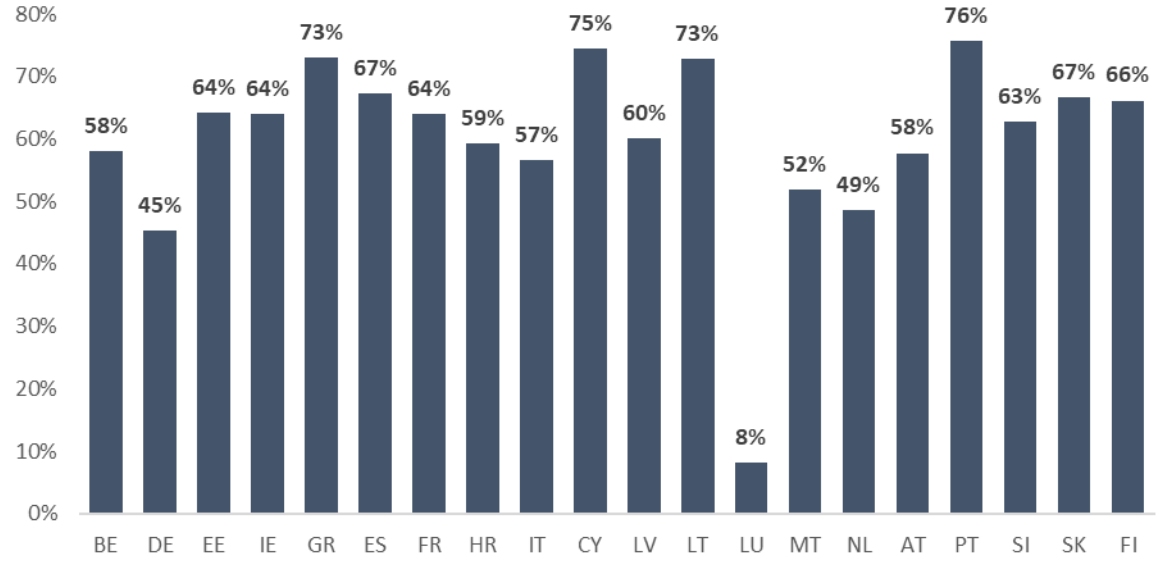
Current State in Card Fraud in Cyprus: Drivers, Impacts and Mitigation Strategies

Irena Prodromou[1]

I. Introduction

Cypriots rely heavily on cards for their day-to-day transactions. The level of card usage in Cyprus is particularly high, a fact that is also reflected at the European comparative level. Notably, during the first half of 2025, Cyprus had the second largest share of card payments (75%) as a percentage of the total number of non-cash payments in the euro area, behind Portugal (Chart 1).

Chart 1: Relative (%) importance of card payments over total non-cash payments in the euro area countries



Source: ECB.

The widespread use of card payments has, however, been accompanied by a persistent increase in card fraud[2], both in Cyprus and in the euro area. It is noteworthy that the largest share of fraudulent non-cash payment transactions comes from card payments. Specifically, during the first half of 2025, card payments accounted for 92% and 81% of the total fraudulent transactions in Cyprus and the euro area, respectively[3].

Fraudulent transactions have become a growing concern in Cyprus but also for the European Union (EU) as a whole. This was also noted in the latest European Banking Authority's edition of the biennial

[1] Comments by Andreas Mylonas, Eleni Nicolaou and George Mardas, Central Bank of Cyprus.
[2] Fraudulent transactions include (a) unauthorised payment transactions and (b) payment transactions made as a result of a manipulation of the payer.
[3] More information on the evolution and analysis of fraudulent transactions can be found in publications of the Central Bank of Cyprus - Payment Fraud Statistics.

Consumer Trends Report 2024/25, which identifies payment fraud as one of the most important issues affecting EU consumers.

In this context, the present article examines the current state of card payment fraud in Cyprus, analyses the main causes and impacts of the phenomenon, and presents key mitigation strategies at the level of consumers, businesses, banks, and the regulatory framework.

II. Drivers

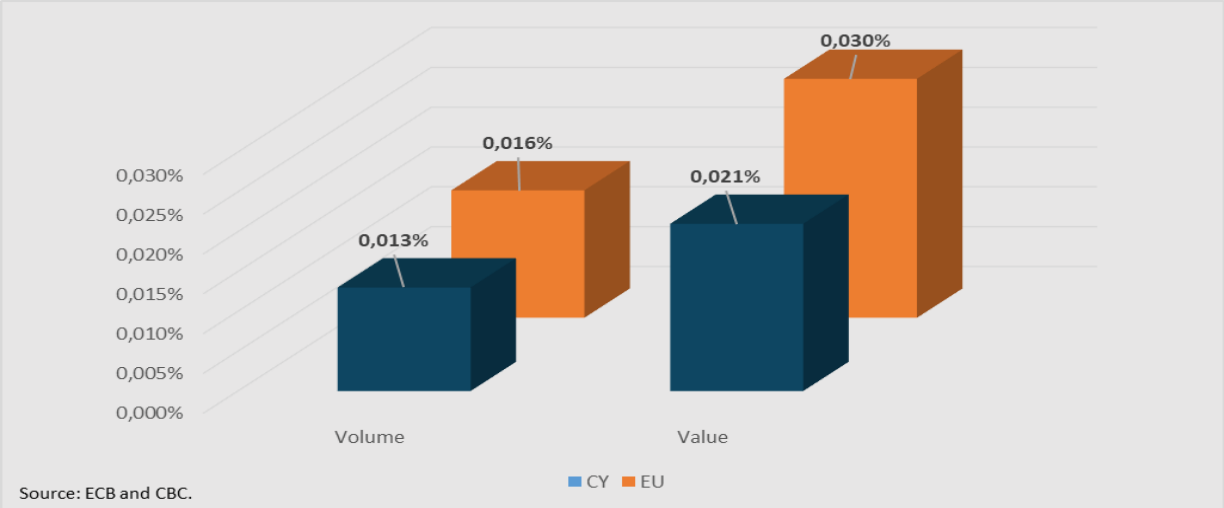
The key drivers of card fraud are deeply rooted in technological and social advancements. Although these key drivers are largely common across EU countries, certain characteristics of the Cypriot economic landscape also contribute to amplifying the phenomenon. The main mechanisms enabling card fraud are described below.

(a) Frequent Use of Cards

Card payments stand out as the most popular method (75%) of non-cash payments in Cyprus, as they are very convenient, fast, and easy to use.

The expansion of card payments goes hand in hand with the rise in card fraud. It is noted that fraud rates[4] for card payments in Cyprus were substantially below the corresponding euro-area averages in both volume and value terms for the first half of 2025 (Chart 2).

Chart 2: Fraud rates for card payments for Cyprus and the euro area



(b) Rise in Online Payments

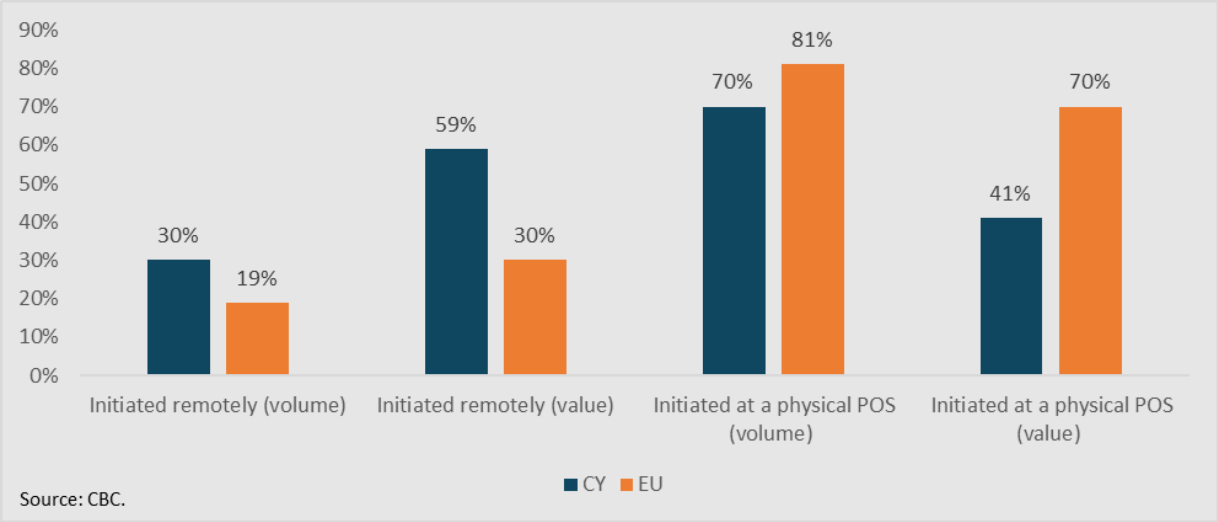
As more businesses transition online, opportunities for card fraud increase. Online card payments are considered riskier than card payments at a physical POS (i.e., in the store) as they are carried out without the physical presence of a card ('card-not-present' transactions), thereby increasing the risk of hacking and theft.

It is noted that Cypriot consumers perform more frequent online card payments of higher average value compared with the euro area average (Chart 3). Indicatively, for the first half of 2025, the split between the volume and value of online card payments in Cyprus was 30% and 59%, respectively.

[4] A fraud rate of 0,001% in volume terms means that 1 transaction per 100.000 of transactions is subject to fraud. A fraud rate of 0,001% means that 1 cent per €1.000 worth of payments is subject to fraud.

Conversely, the split between the volume and value of online card payments in the euro area was 19% and 30%, respectively. It is also highlighted that the average value per card payment initiated online (€125) for Cyprus was one of the highest in the euro area (average value: €60) in the first half of 2025.

Chart 3: Card payments per type of initiation (volume and value in %) for Cyprus and the euro area



(c) Surge in Data Breaches

A rise in data breaches has become one of the strongest drivers of card fraud, as it amplifies fraud opportunities. Data breaches result in the theft of personal and card details, which can be sold to potential fraudsters who may exploit them or use them to automate future fraud attacks.

Over the last few years, Cyprus has experienced a sharp increase in cyber incidents, with data breaches affecting government systems (e.g., Department of Lands and Surveys), postal services, the healthcare sector, and many other businesses and individuals. The most significant breaches were reported at Cyprus Post in October 2025 and at the Bank of Cyprus Oncology Center in December 2025, demonstrating vulnerabilities to fraud attacks.

(d) AI-Driven Fraud Automation

Artificial intelligence (AI) tools have become more widely available, intensifying the speed and complexity of fraudulent activity. New technologies have made it cheaper and easier for fraudsters to operate, reducing the need for specialised skills and enabling even inexperienced individuals to carry out sophisticated schemes. This has resulted in a flood of fraudulent attempts.

Fraudsters apply sophisticated techniques, such as the generation of fake documents, highly advanced deepfakes[5], inexpensive yet realistic fake identities, designed to fool verification systems.

(e) Expansion of Cybercrime

The rise in cybercrime has intensified card fraud, with fraudsters now operating on a larger scale with greater organization and technical capability, making card data theft and card-not-present fraud easier, faster, and more profitable. Moreover, the expansion of cybercrime enables the automation

[5] Deepfakes take the form of images, video, and audio. They are highly realistic and can deceive users by bypassing traditional fraud prevention systems.

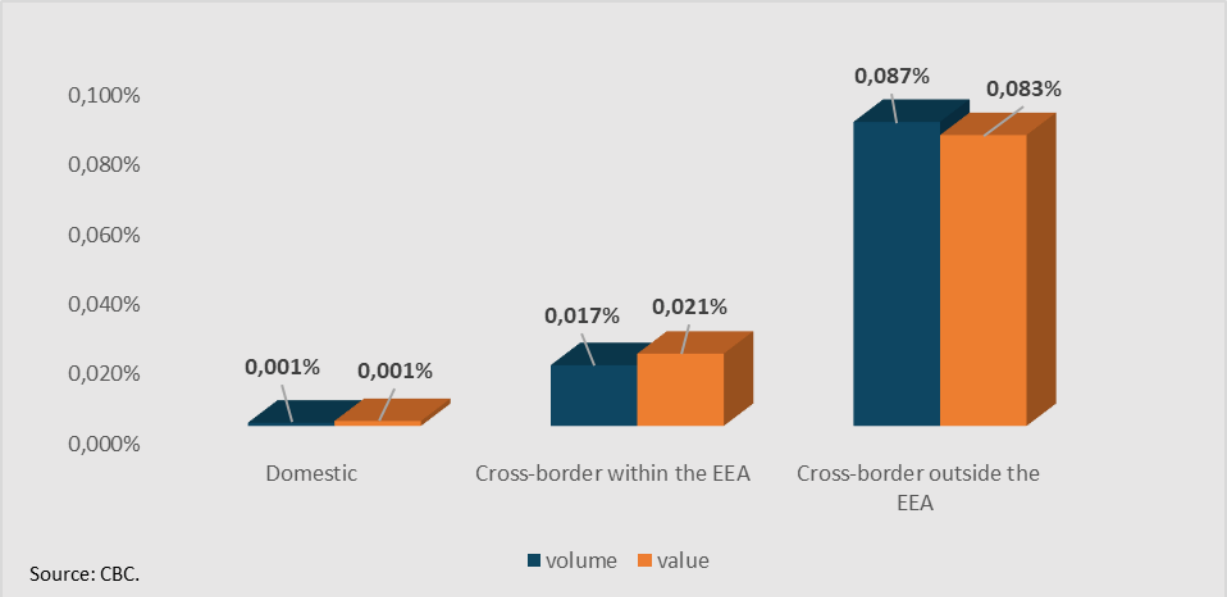
and mass execution of attacks, which are frequently conducted by fraudsters located outside the country.

(f) Weak Verification on Cross-border transactions

Card fraud is significantly higher in cross-border[6] transactions (especially those outside the EEA[7]) than in domestic ones in both absolute and relative (i.e., card fraud as a share of card payments) terms in Cyprus during the first half of 2025 (Chart 4). It is striking that, in absolute terms, card fraud was more than 95% more likely to occur in cross-border payments than in domestic payments.

This can be attributed to the varying regulations across different countries' jurisdictions as well as the insufficient cross-border cooperation among banks and other involved stakeholders to combat fraud.

Chart 4: Fraud rate per counterpart location (volume and value in %)



Source: CBC.

(g) Industries with the Highest Fraud Rates

Unregulated emerging industries continue to be the most common target of fraudsters. This can be attributed to the fact that these industries have generally less stringent anti-fraud measures compared to regulated industries, because there is no regulator to enforce standards.

Indicatively, high card fraud rate in Cyprus was observed in the online subscription services, transfers to payment institutions related to cryptocurrency purchases and transactions in digital banking platforms (e.g. currency-exchange services), as well as online dating applications and advertising services (e.g., payments made through platforms such as Facebook and Google) for the first half of 2025.

(h) Consumer Behavior and Low Awareness Level

Customer behavior and awareness levels are critical factors contributing to the occurrence of fraud. Many fraudulent transactions can be attributed to unsafe practices adopted by consumers, such as

[6] Transactions where the bank of payee is located outside Cyprus.
[7] The European Economic Area, abbreviated as EEA in Chart 4, consists of the Member States (excluding Cyprus which is presented separately under the category 'Domestic') of the EU and three countries of the European Free Trade Association (EFTA) (Iceland, Liechtenstein and Norway).

using unsecured public Wi-Fi networks for sensitive transactions, making online payments to untrusted merchants and clicking on suspicious links in emails or messages. Moreover, weak online security habits related to card payments – such as using weak passwords, not changing passwords regularly, or failing to apply strong customer authentication - create easy entry points that fraudsters can exploit.

III. Impacts

The effects of card fraud can take various forms.

(a) Operational and Financial Strain

Obviously, the main implication of card fraud is the financial losses for consumers, merchants and banks, as well as the higher operational costs incurred by banks to investigate disputes, file reports and close accounts. Furthermore, as banks try to keep pace with increasingly sophisticated fraudsters, they are compelled to invest more in security controls, new technologies and staff training.

These costs are ultimately passed on to consumers through higher transaction fees by the banks and higher fees by the merchants.

(b) Dwindling Confidence in the Banking System

Card fraud implications go beyond immediate financial and operational costs, also undermining customer trust and causing brand damage, making consumers more willing to switch to other banks that appear safer, more modern and responsive to fraud threats.

(c) Psychological Crash

Apparently, fraud can lead to significant psychological and emotional impact on victims causing them frustration, fear, anxiety and embarrassment.

(d) Additional Regulatory Requirements

The rise of card fraud has prompted regulators to impose additional reporting requirements on banks, enabling improved monitoring, data analysis, and the development of timely and targeted policy interventions at both national and euro area levels.

(e) Expansion of Cybercrime

Card fraud fuels the cybercrime economy, as stolen card data is traded on illegal e-commerce platforms (dark-web sales), and used for targeted social-engineering attacks[8], creating demand for fraud tools.

IV. Mitigation Strategies

(a) Fraud Awareness

As businesses and consumers become more exposed to fraud, it is important that the public and companies understand how they are at risk of digital fraud. In this context, the Cyprus Financial

[8] The fraudster tricks the victim into revealing sensitive information like passwords or security answers by posing as trusted entity.

Literacy and Education Committee (CyFLEC)[9], the financial community as well as the society in general should take a step-by-step approach and cater for the empowerment of citizens with the necessary knowledge and skills, increasing awareness and improving the financial literacy. CyFLEC should intensify its efforts to equip individuals with the necessary knowledge to recognize and respond to fraud through awareness and training programs, workshops, online courses, sector-specific training, and targeted advertisements (e.g., social media posts, television spots).

(b) Implementing Advanced Technologies

The changing face of fraud means that businesses will need to quickly adapt and adopt new tactics. In parallel, banks must continue investing in appropriate and advanced security and monitoring technologies. The technology employed must be able to combine preventive and detective controls to achieve the right balance in fraud-risk mitigation.

(c) Data Analytics and Information Sharing

AI is a double-edged sword: it can be used by fraudsters to exploit vulnerabilities in both human behaviour and the payments infrastructure, but it can also serve as a powerful tool for banks and businesses to protect against threats posed by sophisticated fraud techniques.

In this context, banks' adoption of advanced behavioral analytics to detect suspicious or unusual behavior and patterns in real time—based on each consumer's risk profile—combined with information sharing among key stakeholders, enables more accurate real-time identification of fraud patterns, strengthening rapid response, cross-border defense, and consumer protection.

(d) Effective regulatory governance

Regulators need to take steps to level the playing field, closing loopholes that give fraudsters an advantage and creating a fairer and safer environment for everyone.

Governments and regulatory bodies recognize the pivotal need to protect consumers and businesses through effective regulatory governance, as evidenced by a wave of published guidance and legislation in recent months:

- **The EU Artificial Intelligence (AI) Act.**
  Its key aims and mechanisms are to prohibit dangerous AI, regulate high-risk AI, and ensure transparency.
- **The EU Digital Operational Resilience Act (DORA)**.
  It is designed to enhance the digital operational resilience of the financial sector.
- **The European Digital Identity (EUDI) Regulation.**
  This aims to ensure secure digital identification and mitigate fraud in electronic transactions.
- **The forthcoming Payment Services Directive 3 (PSD3) and the Payment Services Regulation (PSR).**
  These measures aim, among other things, to curb fraud and to modernize and transform the payments landscape.

[9] As from December 2023, the Central Bank of Cyprus chairs the CyFLEC.

V. Concluding Remarks

Today, payment card fraud has developed into a complex, cross-border threat that evolves in parallel with the digital payments ecosystem.

As explored in this article, the drivers of card fraud are deeply rooted in technological and social advancements. Although these key drivers are largely consistent across EU countries, certain characteristics of the Cypriot economic landscape also play a role. Specifically, the higher card usage and the larger share of online payments in Cyprus compared to the euro-area average, increase the country's exposure to fraud.

The surge in data breaches, the exploitation of artificial intelligence by fraudsters and the expansion of cyber crime facilitate the large-scale and automated execution of attacks, while cross-border card payments remain particularly vulnerable due to differing regulatory frameworks and limited cooperation among the involved stakeholders.

Sectors exhibiting the highest levels of fraud are typically emerging and largely unregulated industries, characterized by less stringent fraud prevention measures.

The impacts of card fraud extend beyond direct financial losses, eroding customer trust, corporate reputation, and consumers' psychological well-being. At the same time, banks and businesses are required to increase investments in security measures and new technologies in order to keep pace with increasingly sophisticated fraudsters, integrating fraud risk into their overall risk management frameworks.

Effective fraud mitigation requires a combination of technological and regulatory adaptation, the use of advanced behavioral analytics, enhanced information sharing among relevant stakeholders, and continuous consumer education and awareness. In this evolving environment, banks and businesses that remain flexible and adaptive are better equipped to mitigate risk and ensure the smooth functioning of their systems.

The views expressed in the posts belong to the authors and do not necessarily represent the views of the Central Bank of Cyprus.