Project EU CYBER VAT

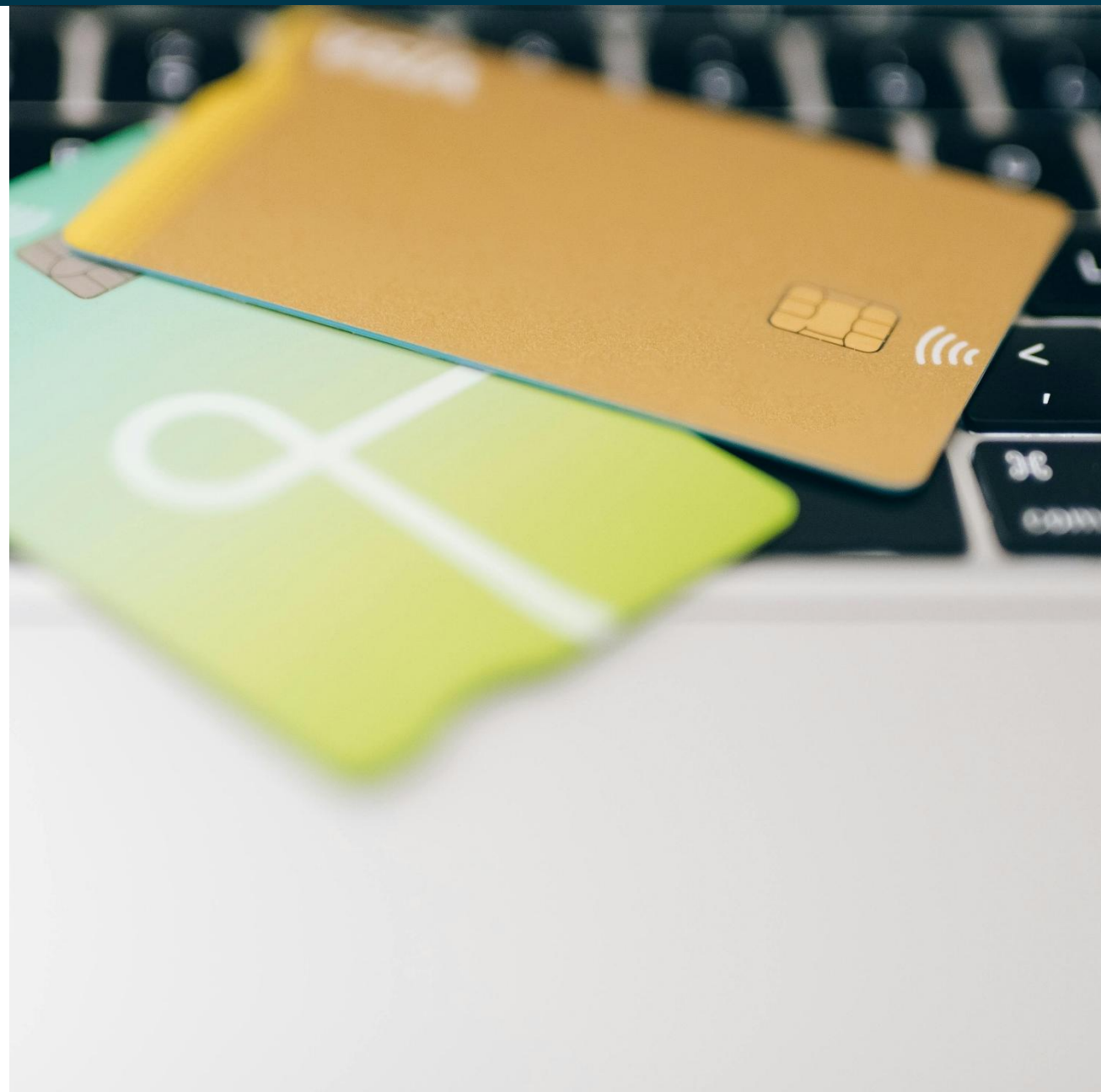
Comparative Study

Co-funded by
the European Union

CSSC
Centro di Scienze della Sicurezza e della Criminalità
Università di Trento
Università di Verona

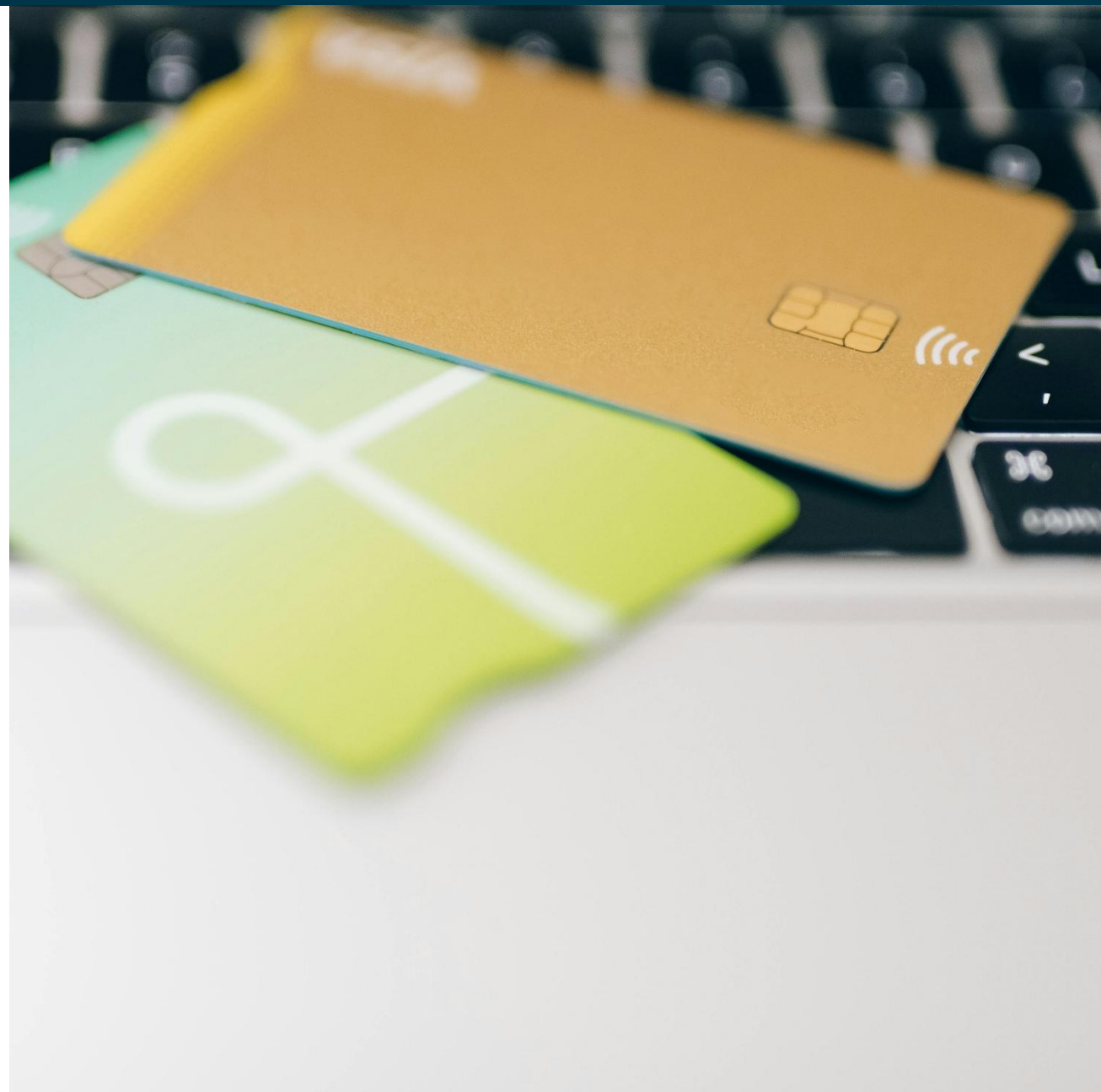
Background and needs

- VAT fraud undermines **national** economies and **EU** financial integrity
- VAT fraud poses a major financial threat, leading to the creation of the **EPPO** in 2020 with jurisdiction over large-scale cross-border cases.
- **Major impact**: 59% of EU budget losses in 2023 (€11.5bn, +71% vs. 2022)
- **Driven by digitalisation & e-commerce**: E-commerce platforms, cryptocurrencies, blockchain, digital invoices
- **Urgent need** for a unified strategy: Enhanced cross-border cooperation; Stronger institutional collaboration



Aim

The **aim** of this analysis was to examinate how EU MSs address VAT and cyber VAT fraud, focusing on the transposition of the PIF Directive and evaluating whether current laws sufficiently cover cyber VAT fraud or if a new offense is needed. It assessed the effectiveness of investigative tools, with particular attention to digital forensics and advanced technologies. It also analyzed protection against VAT fraud in the digital marketplace, including e-commerce rules and the potential liability of online service providers. It compared the implementation of the PIF Directive and Directive 2020/284 across MSs, examining legal frameworks, enforcement practices, sanctions, loopholes exploited by fraudsters, and the effectiveness of cross-border cooperation.



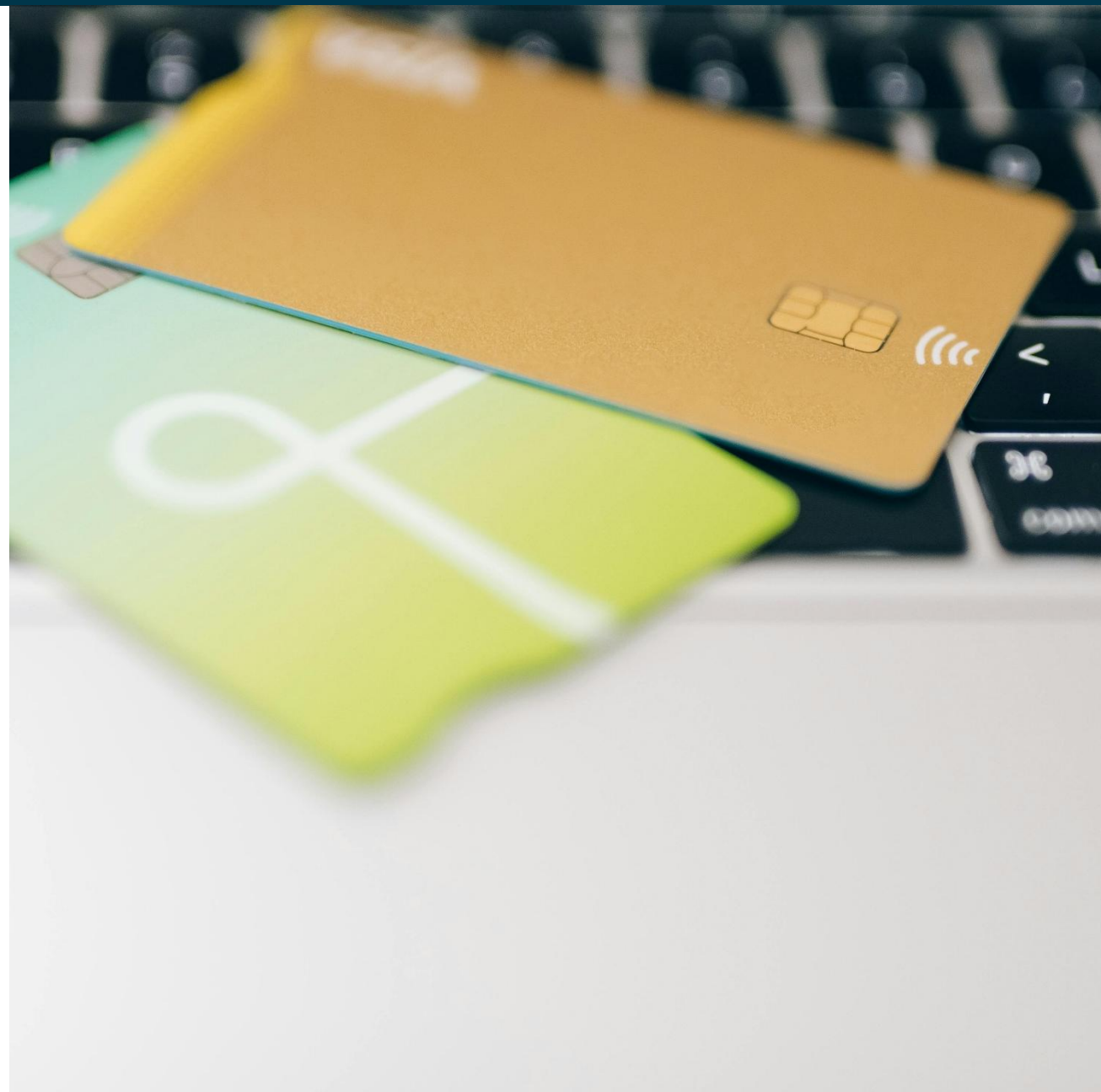
Definition

Cyber VAT fraud refers to both a cyber enabled and a cyber assisted crime that consists of VAT fraud facilitated by new technologies. Such facilitation can take place:

a) at various stages (e.g. the financial transaction stage, where the ability to conceal cash flows can be facilitated);

b) through certain activities (e.g. the creation of false documents or the establishment of fake companies);

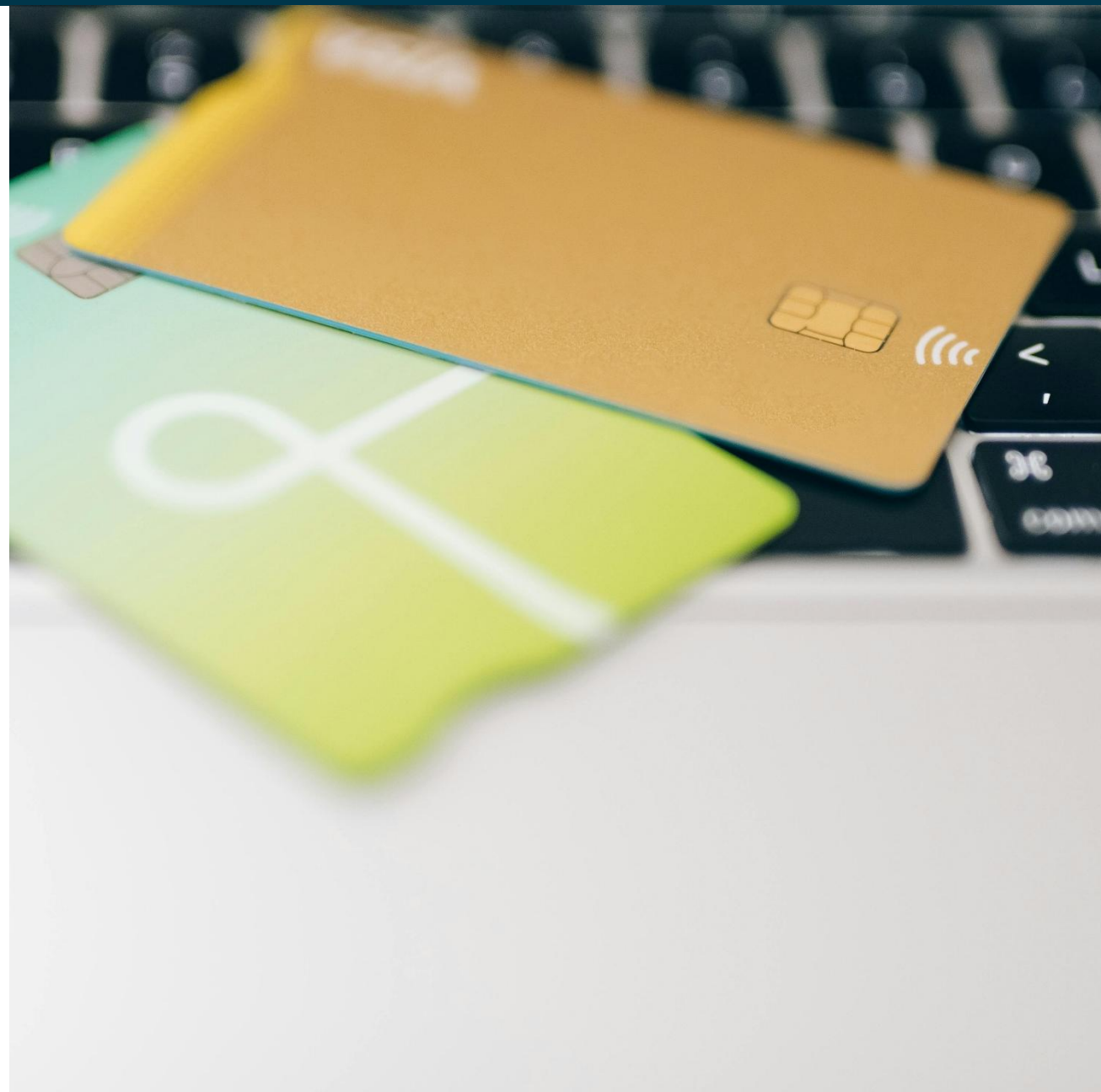
c) through the creation of new intangible goods generated by technology / digital goods (e.g. software, carbon credits).



Methodology

Research **combined**:

- desk research;
- literature review;
- Consultations with national experts from 25 Member States, with Estonia and Slovenia covered through secondary sources, conducted via structured questionnaires and focus groups.



Co-funded by the European Union

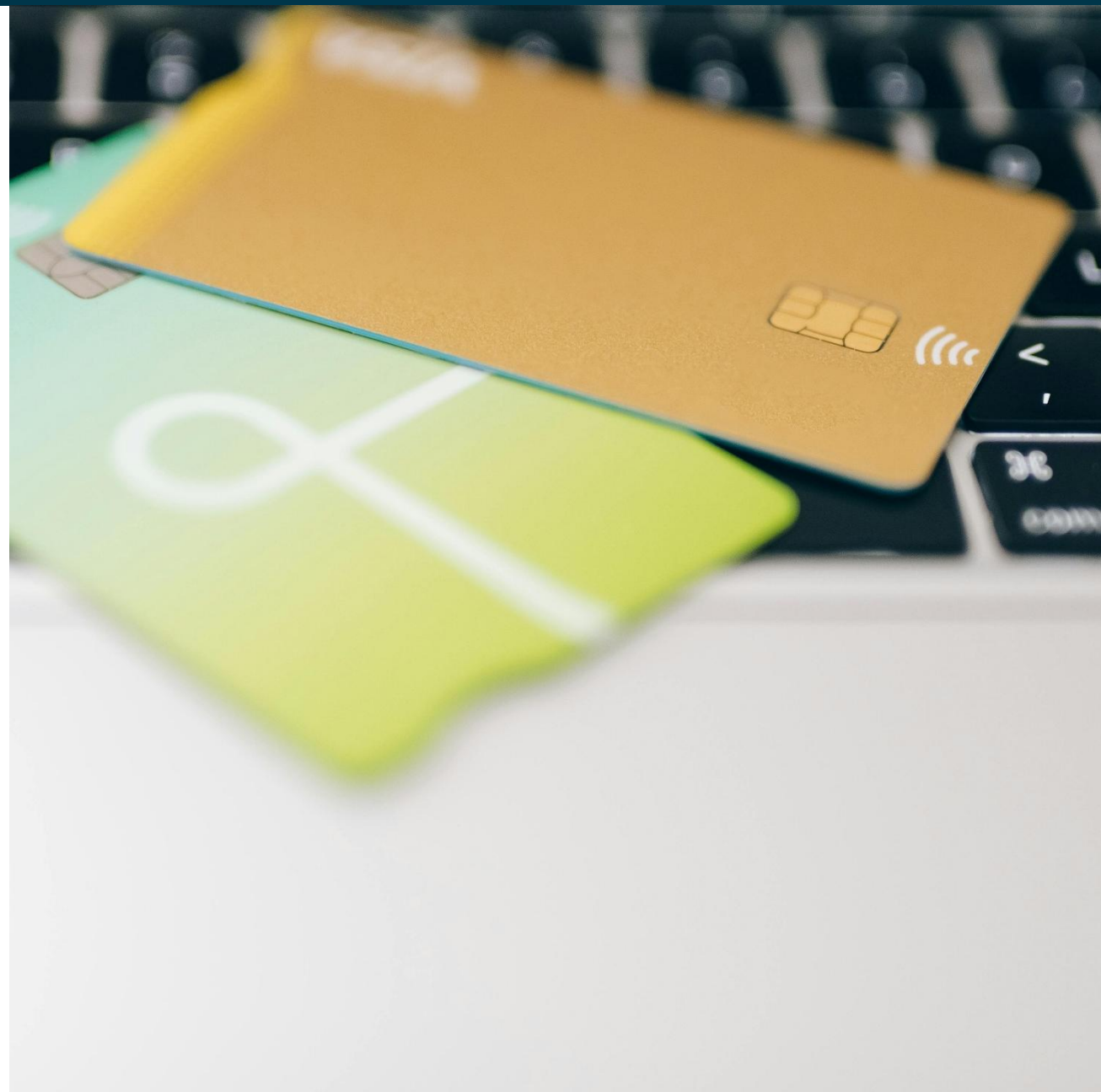
Methodology

Structured **questionnaires** assessed:

- Transposition of the PIF Directive;
- National legislation on VAT and cyber-VAT fraud;
- Investigative tools and ICT strategies;
- Emerging criminal trends.

Focus areas of the questionnaire:

- Criminal law on VAT fraud;
- Criminal law on cyber-VAT fraud;
- Investigation and prosecution;
- Role of ICT in combating cyber-VAT fraud;



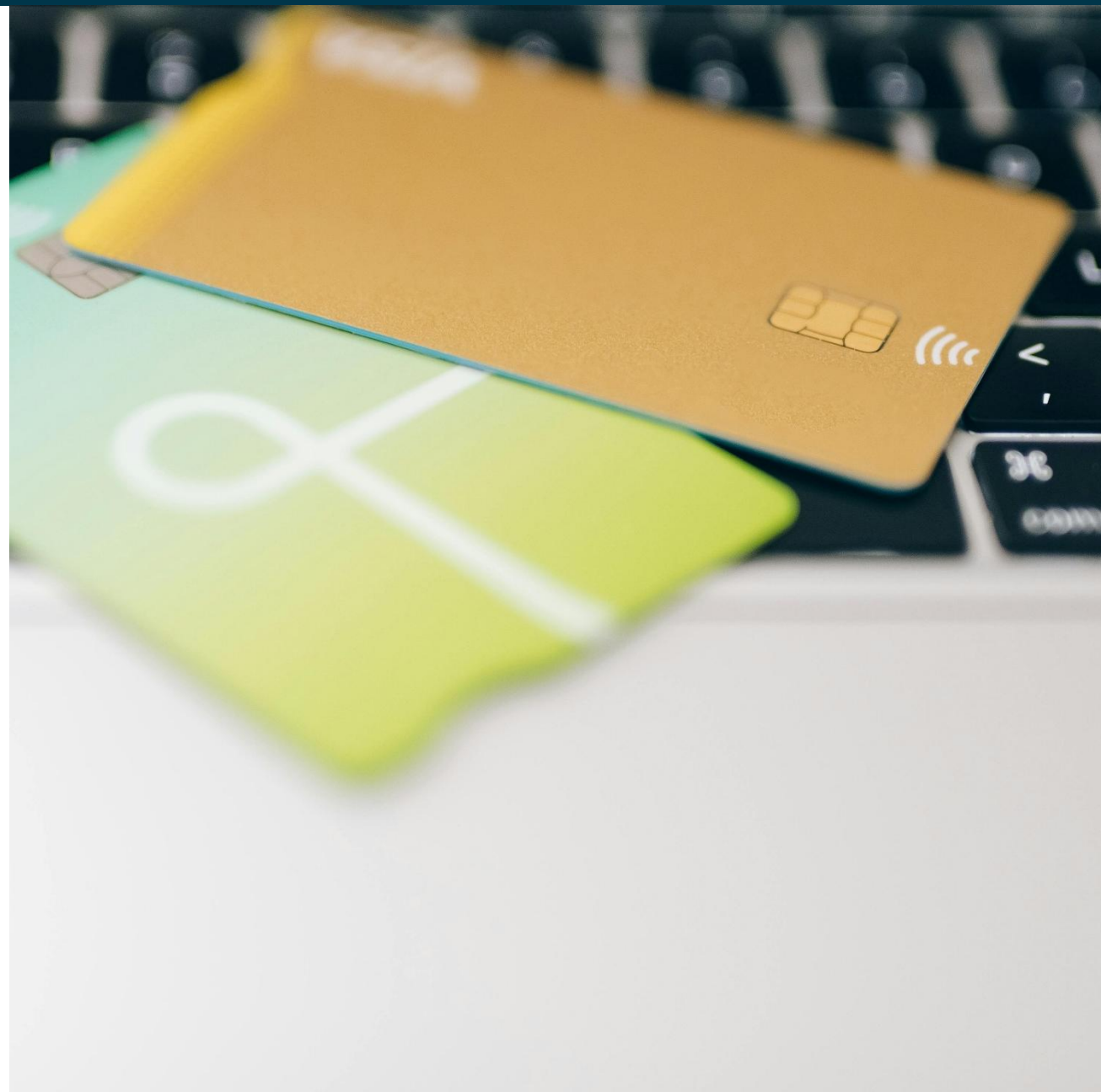
Co-funded by the European Union

Methodology

Two online **focus groups** organized:

- First: legal/procedural strategies for cyber VAT fraud, including potential new offenses and digital investigation tools;
- Second: cyber VAT fraud in e-commerce, covering MTIC fraud, platform responsibilities, MOSS-to-OSS transition, and cross-border harmonization.

Special focus on VAT fraud in the **e-commerce** context.



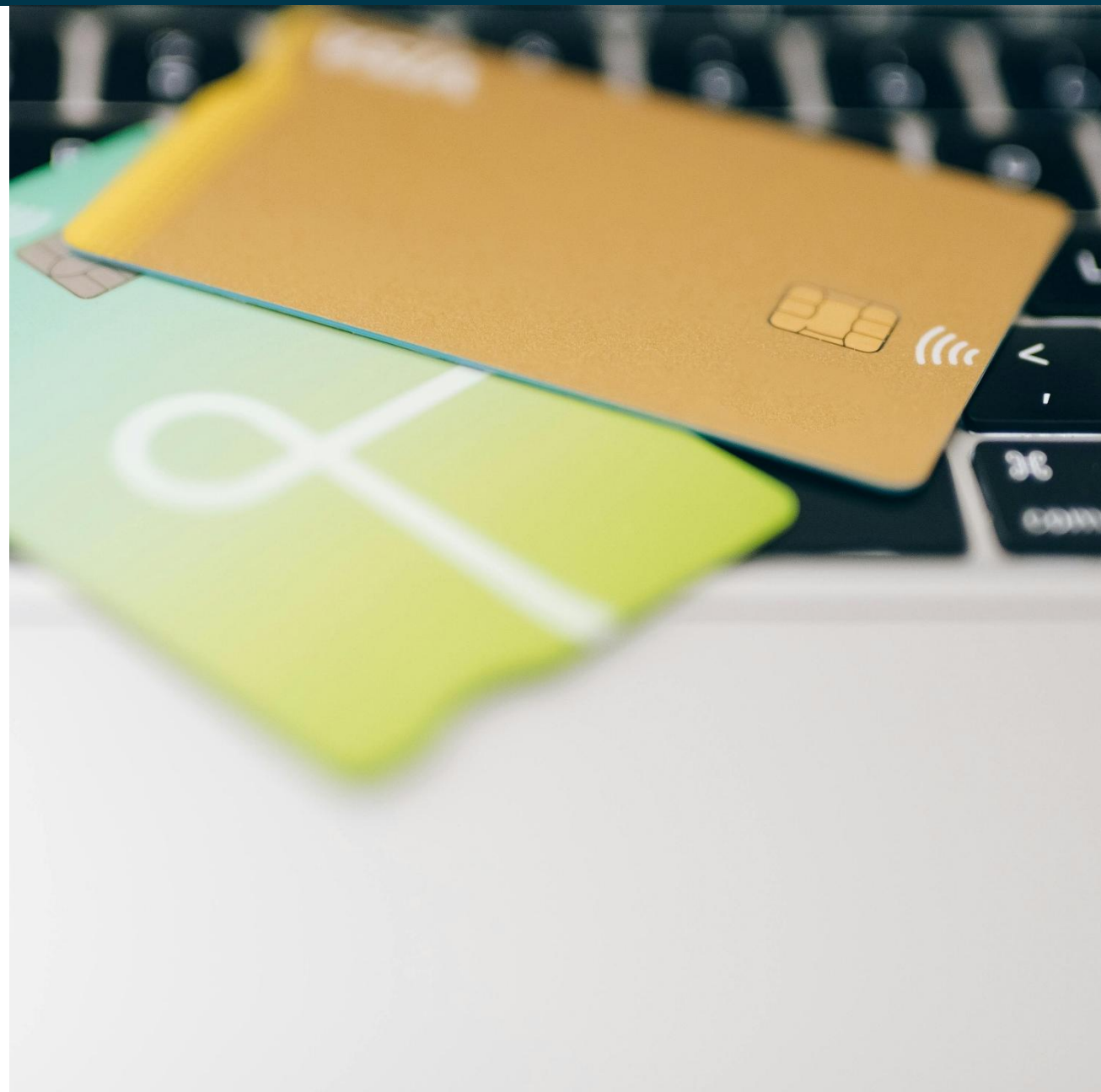
Results

I. The first section reviewed how the PIF Directive (2017/1371) has been transposed into national laws regarding VAT fraud, examining definitions, sanctions, and organized crime aggravating factors, and identified national variations that underscore the need for stronger, coordinated EU-level measures.

Compliance with Article 3 – Definitions of VAT Fraud

21/25 Member States compliant; exceptions: Denmark, France, Croatia, Slovakia.

Compliance achieved via amendments (12), new laws (5), or existing provisions (3).



Co-funded by the European Union

Results

Objective element of VAT-related offenses

In 19 of 25 MSs, VAT fraud is treated as a general offense without specific actions defined in law.

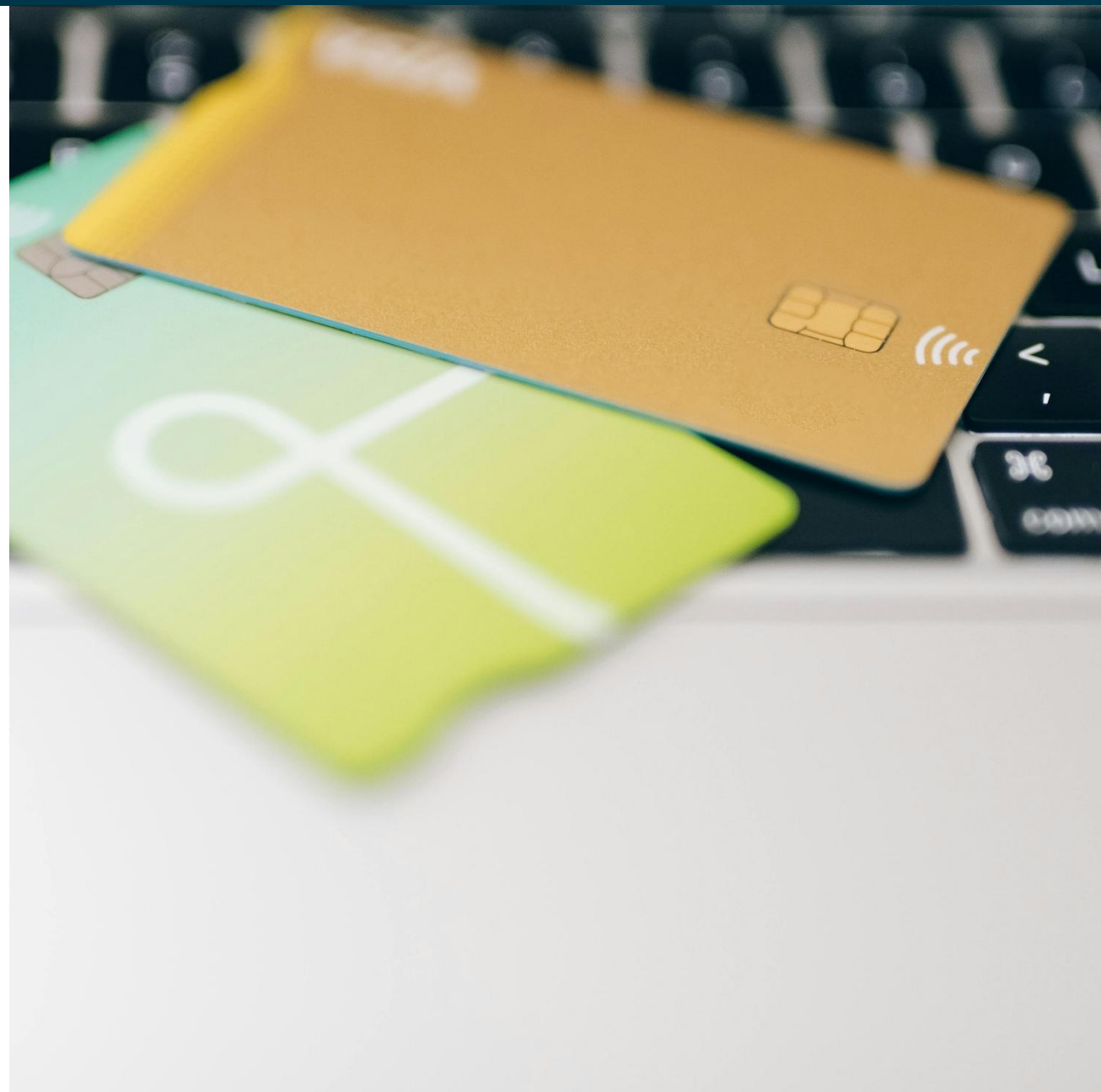
Six countries (Bulgaria, Croatia, France, Greece, Portugal, Italy) list explicit behaviors in their criminal codes.

Subjective element of VAT-related offenses

18 of 25 MSs impose criminal liability only for intentional VAT fraud.

No MS imposes liability solely for negligence.

Seven countries hold offenders liable for both intent and negligence.



Results

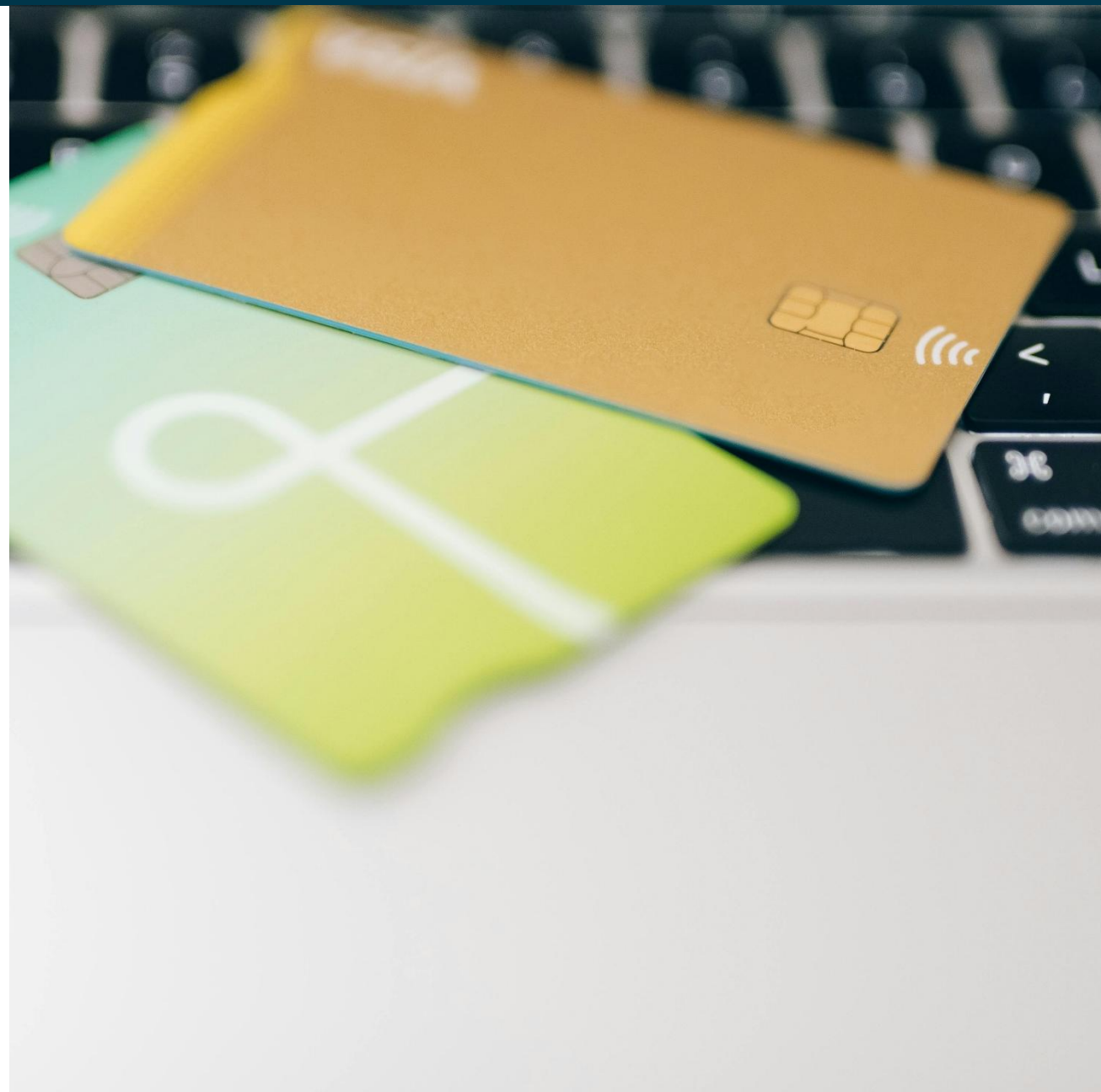
Compliance with Article 7 of the PIF Directive

Article 7 requires a maximum prison sentence of at least 4 years for fraud over €100,000.

Most states comply; exceptions: France and Slovakia impose less than 4 years.

Aggravating circumstances for VAT fraud in organized crime

Only 3 of 25 Member States don't explicitly include VAT fraud in organized crime as an aggravating factor.



Results

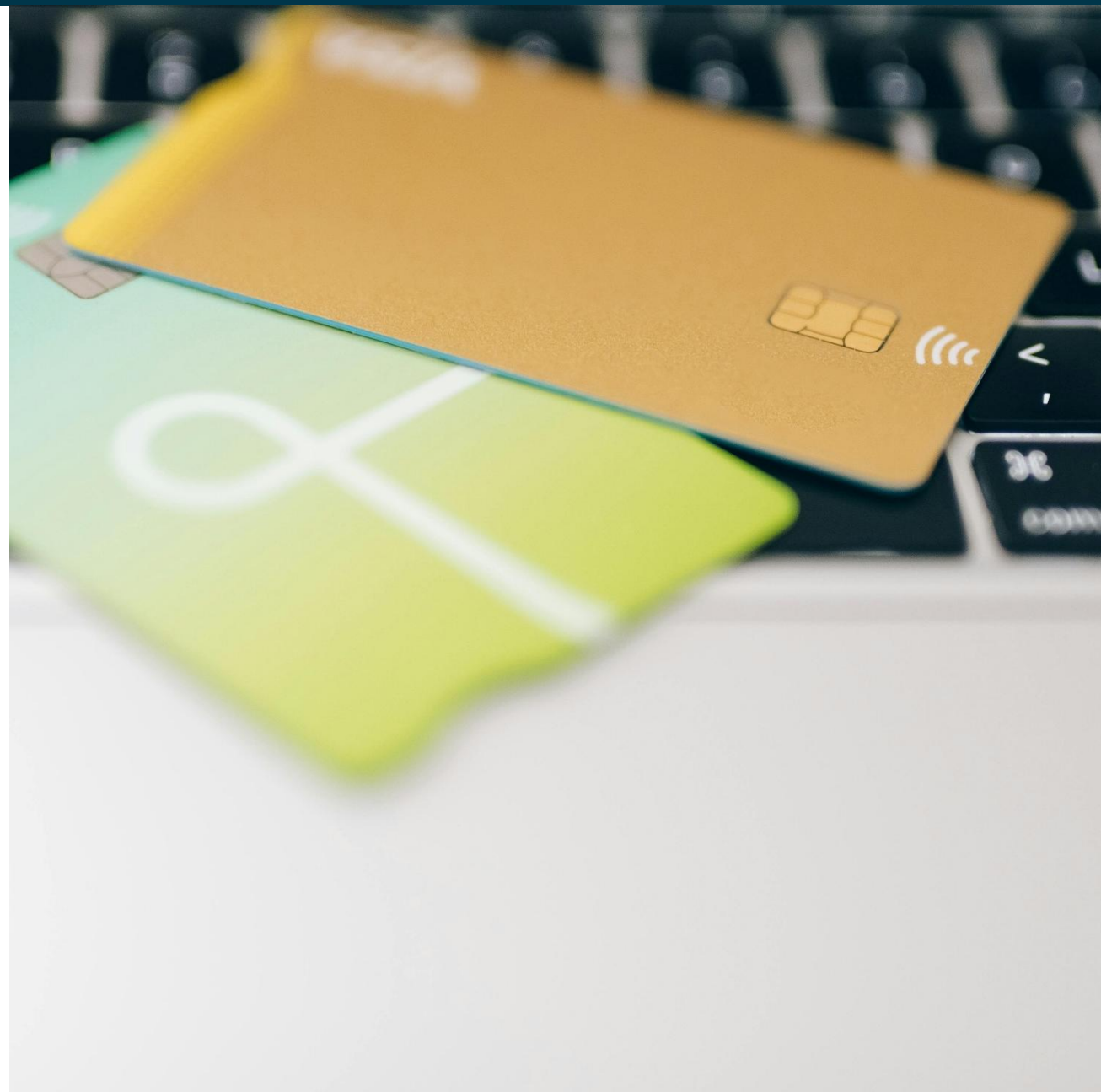
Compliance with Article 6 of the PIF Directive

23 of 25 MS correctly transposed Article 6. Exceptions: Denmark (not required) and France (has not amended legislation, but corporate liability exists).

Sanctions for legal persons

Most MS impose primarily criminal penalties, some also apply administrative or civil measures.

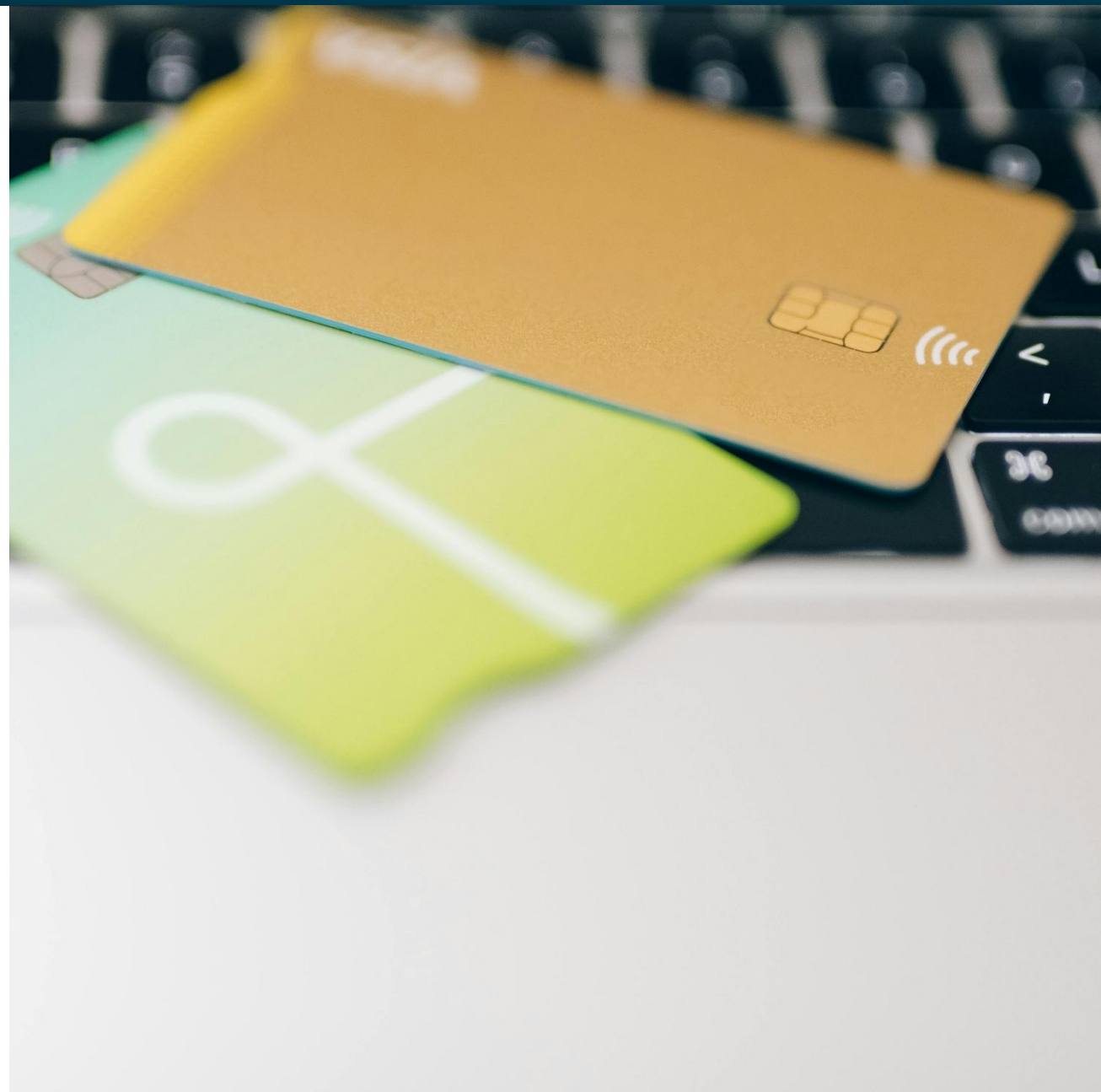
Many states fully or partially align with Article 9 of the PIF Directive regarding sanctions.



Results

II. The second section analyzed how Member States deal with cyber VAT fraud, concluding that existing VAT fraud provisions are generally sufficient.

Experts recommend focusing on stronger investigations, consistent law enforcement, and cross-border cooperation rather than creating new cyber-specific offenses.

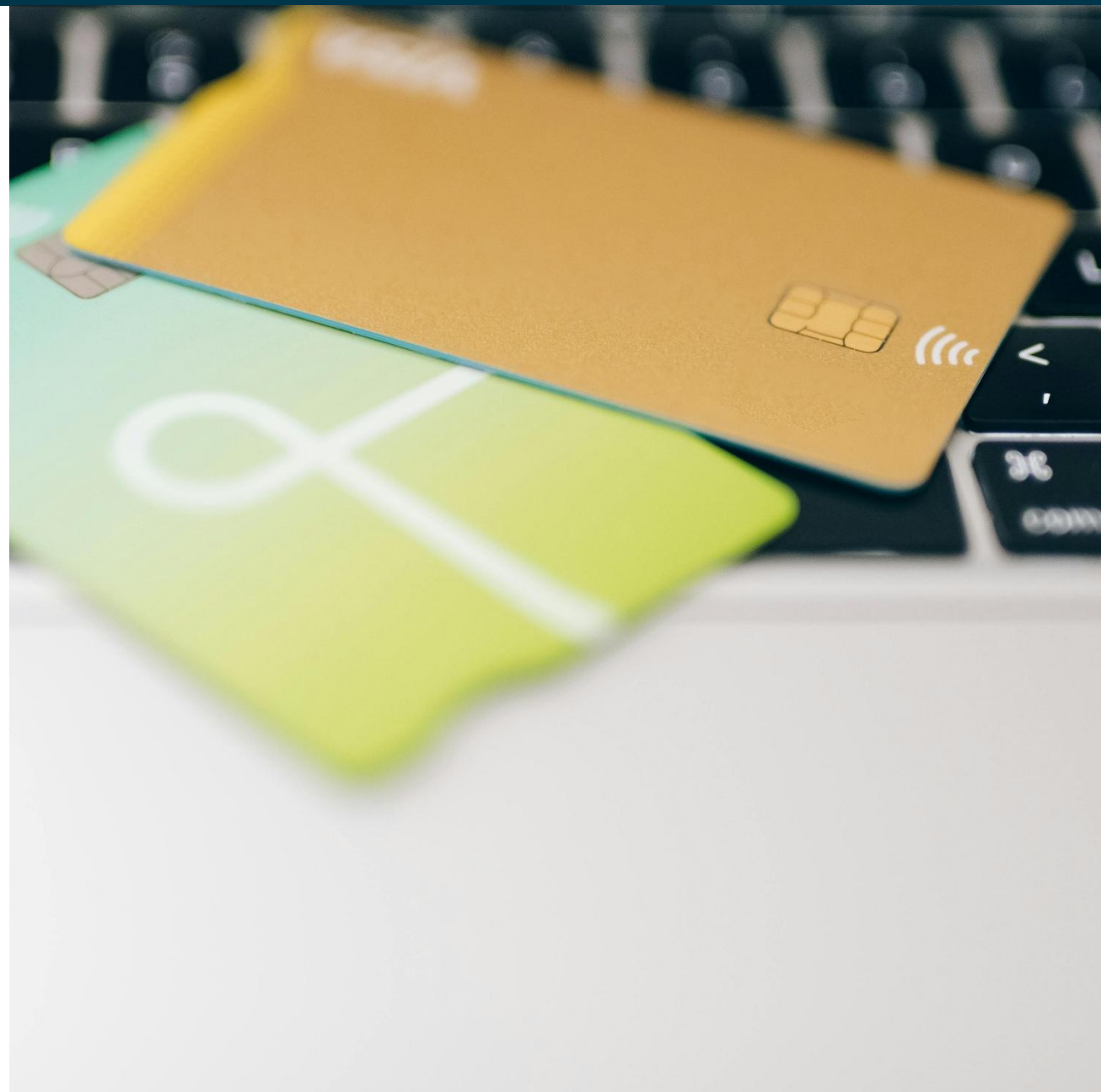


Results

III. The third section examined VAT and cyber VAT fraud procedures, highlighting disparities in investigative tools and measures, the role of EU institutions and international cooperation, and all phases of the anti-fraud cycle, with a focus on digital investigations, forensic tools, jurisdiction, and limitation periods.

Investigative tools and measures against VAT fraud and cyber VAT fraud

VAT fraud tackled via audits, data, surveillance, and cooperation.
Experts call for AI, specialized units, and procedural reforms.
Digital tools and EU-coordinated approach are essential.



Co-funded by the European Union

Results

Jurisdiction (Article 11):

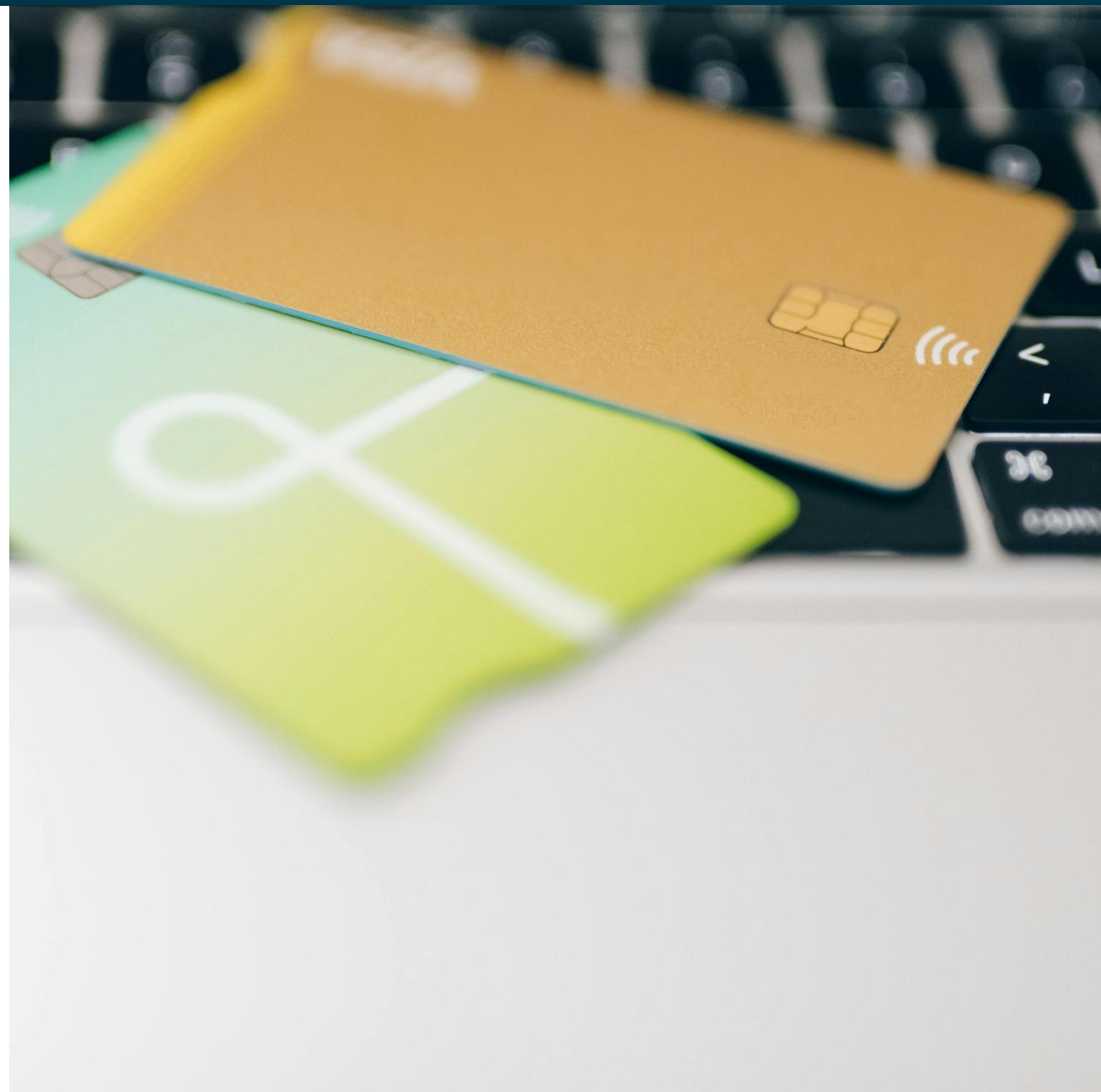
MSs must assert jurisdiction over offenses on their territory or by their nationals.

All states except Cyprus apply territorial jurisdiction; most also use the nationality principle. Exceptions allowed if the Commission is notified.

Limitation period (Article 12):

Sets the timeframe for prosecuting crimes; longer periods needed for complex VAT and cyber VAT fraud.

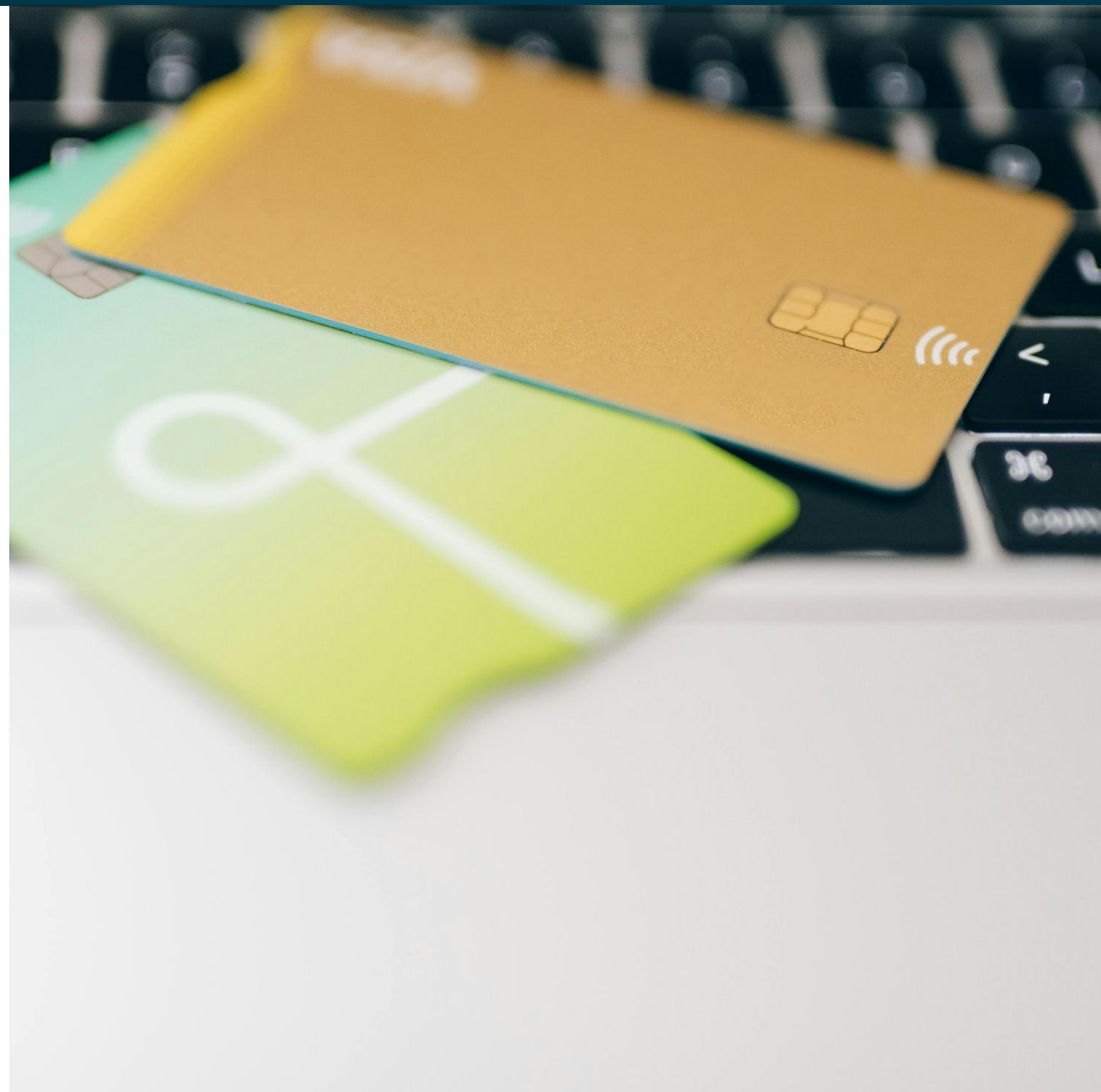
EU law requires at least five years for serious VAT fraud; most states comply, some extend further.



Results

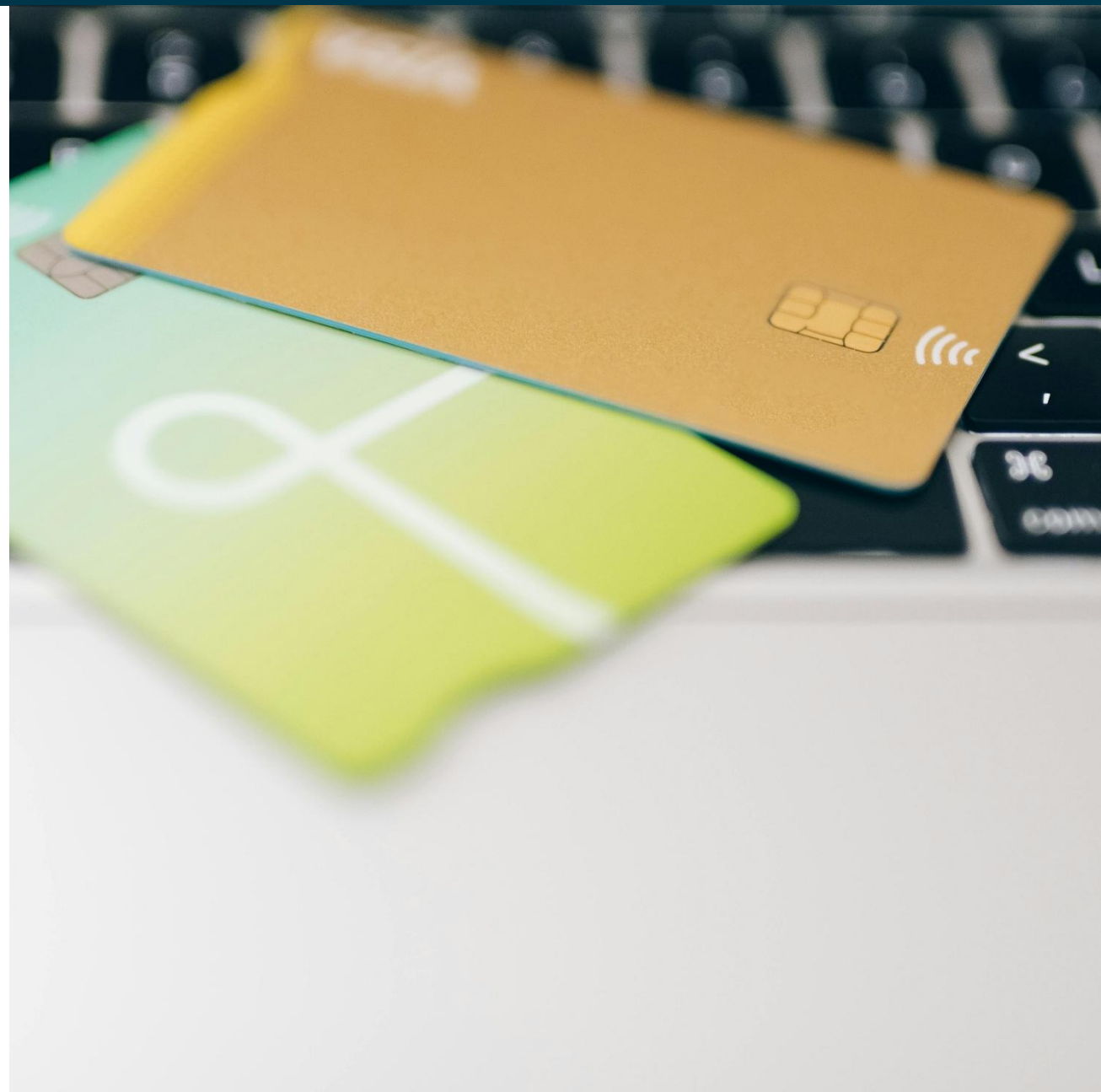
IV. The last section examined the use of information and communication technologies (ICT) in preventing and detecting VAT fraud, including cyber VAT fraud.

Most EU Member States have ICT strategies against crime, but few focus on VAT or cyber VAT fraud. Fragmented systems and diverse e-reporting frameworks limit effectiveness, while standardization, real-time monitoring, AI, and cross-border cooperation could improve detection and prevention.



Results

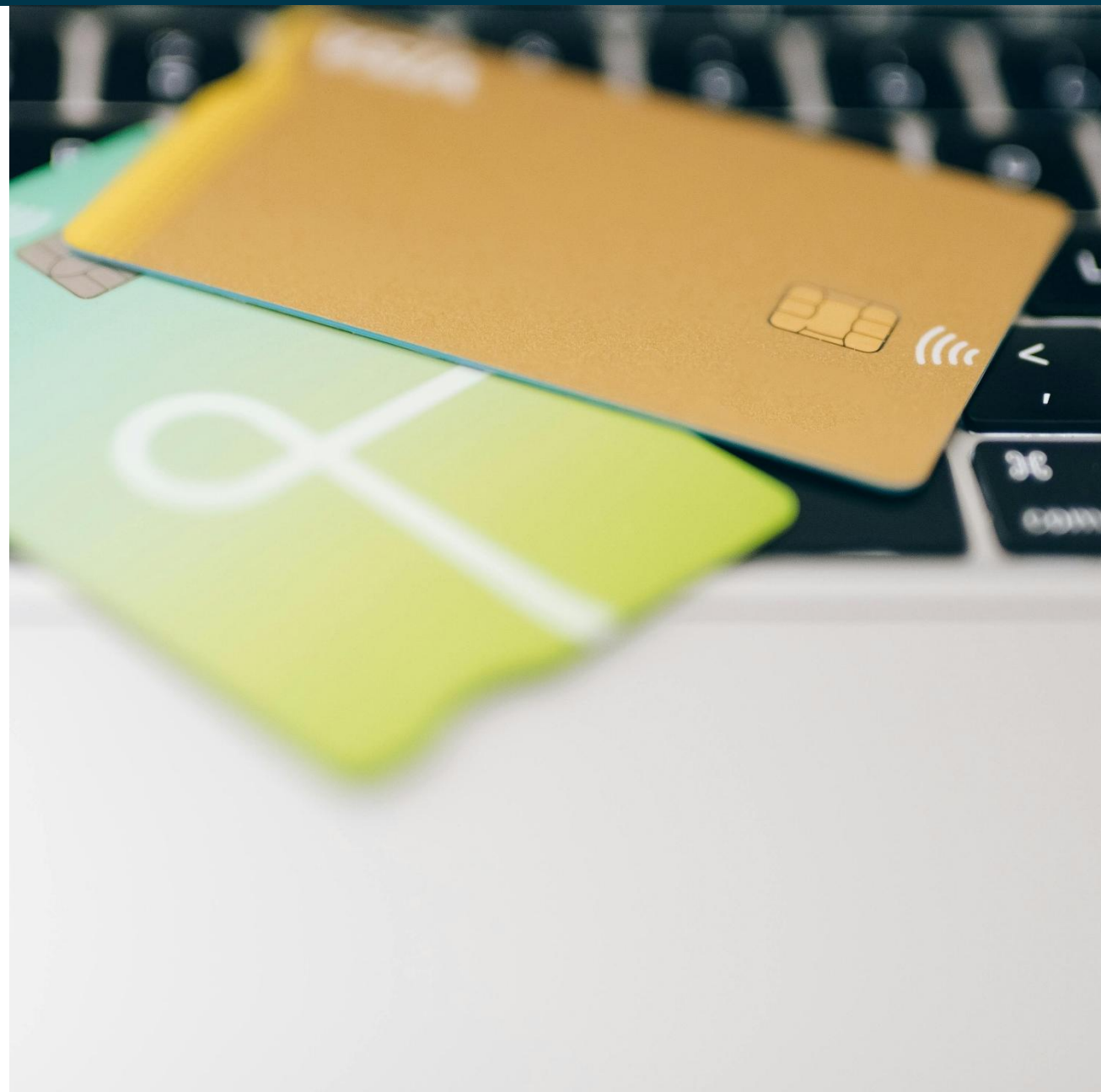
The study examined EU Directive 2020/284 and MOSS/OSS schemes for **e-commerce** VAT fraud, highlighting risks like non-registration, underreporting, and fraudulent VAT numbers. While most Member States comply, challenges remain in processing data, with recommendations including real-time PSP reporting, enhanced fraud detection, staff training, OSS expansion, and stronger collaboration between authorities and service providers to improve VAT compliance and consistency across the EU.



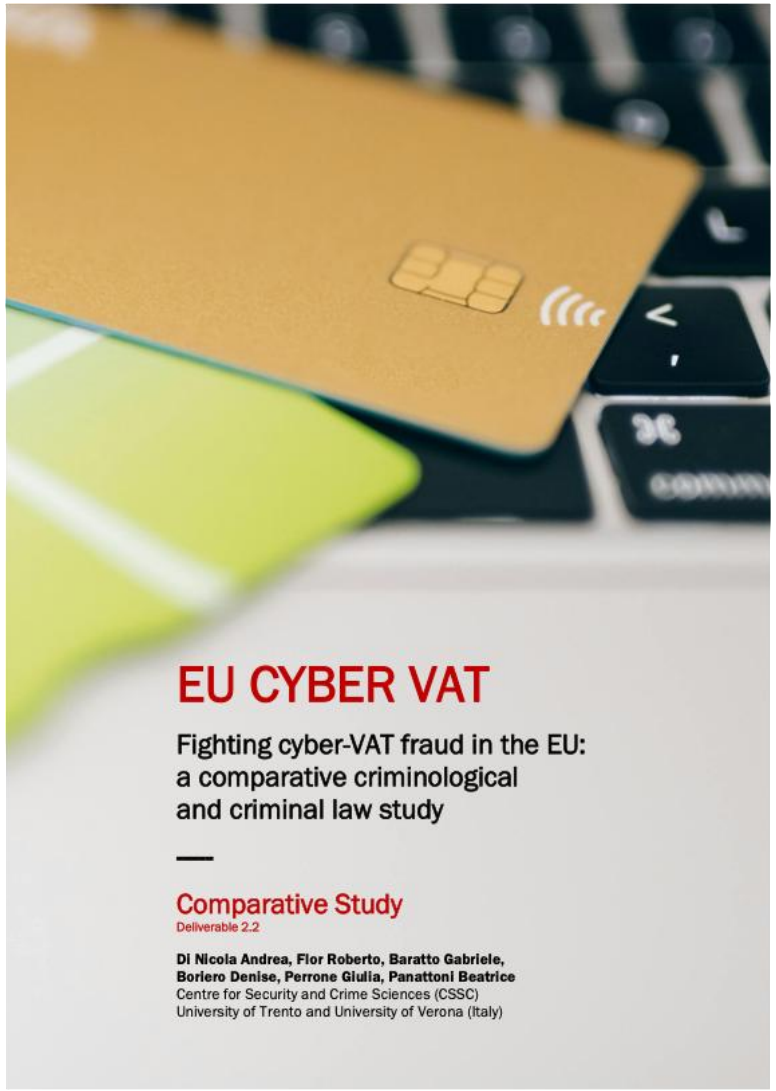
Conclusions

Key finding: Most MSs comply with the PIF Directive and cooperate with the EPPO. Cyber VAT fraud is addressed under traditional VAT or broader fraud/tax evasion laws, and VAT fraud remains a key target for organized crime, highlighting the importance of international cooperation.

Current Priorities: Improving procedural frameworks; Using advanced technologies for detection and investigation; Ensuring consistent enforcement across Member States; Providing specialized training for financial authorities.



Detailed results



MEDWIN PUBLISHERS
Committed to Create Value for Researchers

Open Access Journal of Criminology Investigation & Justice
ISSN: 3064-7940

Combating Cyber VAT Fraud in the EU Member States: A Comparative Study of Criminal and Criminal Procedure Law

Baratto G[1,3], Borlero D[3], Di Nicola A[1,3]*, Flor R[2,3], Panattoni B[2] and Perrone G[1,3]

[1]Faculty of Law, University of Trento, Italy
[2]Department of Law, University of Verona, Italy
[3]Centre of Security and Crime Sciences, University of Trento and University of Verona, Italy

***Corresponding author:** Andrea Di Nicola, Faculty of Law, University of Trento, Centre of Security and Crime Sciences, University of Trento and University of Verona, Italy, Email: andrea.dinicola@unitn.it

Research Article
Volume 3 Issue 1
Received Date: January 15, 2025
Published Date: January 31, 2025
DOI: 10.23880/oajcij-16000130

Abstract

VAT fraud has long posed a major challenge to the economic stability of individual countries and the European Union (EU) as a whole. In recent years, the convergence of VAT fraud and cybercrime has led to a new phenomenon: cyber VAT fraud. Despite its increasing prevalence, this complex issue has not yet been sufficiently researched and a comprehensive framework to combat it effectively has yet to be developed.

This article is an anticipation of the comparative legal analysis on combating cyber VAT fraud in the European Union, which is part of the project "EU CYBER VAT - Fighting cyber-VAT fraud in the EU: a comparative criminological and criminal law study", co-founded by the Union Anti-Fraud Program (EUAF) of the European Anti-Fraud Office (OLAF).

The EU CYBER VAT project aims to fill this gap by assessing the adequacy of the existing legal framework both at EU and Member State level. The comparative analysis examines whether the current rules, including the PIF Directive and its implementation at national level, provide solid and effective protection against the new threats posed by cyber VAT fraud.

Keywords: Value-Added Tax; VAT Fraud; Cybercrime; Cyber VAT Fraud; EPPO; European Union

Abbreviations

VAT: Value Added Tax; EPPO: European Public Prosecutor's Office; EU: European Union; ICT: Information and Communication Technology; CSSC: Centre of Security and Crime Science; OSS: One Stop Shop; PSPs: Payment Service Providers; AI: Artificial Intelligence.

Introduction

It is well known that VAT fraud is a phenomenon that has always seriously affected the economies of individual countries and the European Union. In fact, value added tax (VAT) is one of the most important components of public revenue and represents an essential source of own resources for both the EU budget and national budgets. The importance of VAT goes beyond its role as a mere tax; it is a key element of the financial framework that sustains the European project, finances public services and facilitates cross-border trade in the internal market[1] [1]. The significant impact of fraud

1 Among the various contributions, see for instance: M.C. Fruzza, "Value Added Tax Fraud", Routledge, 2018; S. Pedeli, F. Forte, "EU VAT Fraud", in European Journal of Law and Economics, Vol. 31, n. 2, 145-166, 2009; M. Keen, S. Smith, "VAT Fraud and Evasion: What Do We Know and What Can Be Done?" in National Tax Journal, Vol. 59, n. 4, 861-887, 2006. To better understand the European dimension of this crime, see: M. Griffoen,

cssc.unitn.it

Thank you for your attention!

cssc@unitn.it

Project “EU CYBER VAT. Fighting cyber VAT fraud in the EU:
a comparative criminological and criminal law study”

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission (Directorate General for European Anti-Fraud Office).
Neither the European Union nor the granting authority can be held responsible for them.