BANCA D'ITALIA
EUROSISTEMA

Mercati, infrastrutture, sistemi di pagamento

(Markets, Infrastructures, Payment Systems)

The security of retail payment instruments: evidence from supervisory data

by Massimiliano Cologgi

January 2023

Number 30

BANCA D'ITALIA
EUROSISTEMA

Mercati, infrastrutture, sistemi di pagamento
(Markets, Infrastructures, Payment Systems)

Approfondimenti
(Research Papers)

The security of retail payment instruments: evidence from supervisory data

by Massimiliano Cologgi

Number 30 – January 2023

The papers published in the 'Markets, Infrastructures, Payment Systems' series provide information and analysis on aspects regarding the institutional duties of the Bank of Italy in relation to the monitoring of financial markets and payment systems and the development and management of the corresponding infrastructures in order to foster a better understanding of these issues and stimulate discussion among institutions, economic actors and citizens.

The views expressed in the papers are those of the authors and do not necessarily reflect those of the Bank of Italy.

The series is available online at www.bancaditalia.it.

Printed copies can be requested from the Paolo Baffi Library: richieste.pubblicazioni@bancaditalia.it.

ISSN 2724-6418 (online)
ISSN 2724-640X (print)

Banca d'Italia
Via Nazionale, 91 - 00184 Rome - Italy
+39 06 47921

Designed and printing by the Printing and Publishing Division of the Bank of Italy

The security of retail payment instruments: evidence from supervisory data

by Massimiliano Cologgi*

Abstract

This paper provides an overview of retail payments security and assesses the impact of the new strong customer authentication (SCA) requirements introduced by the revised Payment Services Directive (PSD2) on the security of remote payments. For each payment instrument, we construct aggregate risk indicators and compare the security of domestic and cross-border payments, as well as of payments made remotely and at the physical point of sale. Using a model for panel data, we estimate that SCA reduces the risk of fraud by 60 per cent for remote payments made by card and by 80 per cent for e-money payments. We also find that the transactions for which the regulation provides an exemption from SCA requirements are relatively safe.

JEL Classification: E42, G21, G23, G28.

Keywords: payment fraud; remote payments; cross-border payments; strong customer authentication.

Sintesi

Il lavoro affronta il tema della sicurezza dei pagamenti al dettaglio, fornendo una stima dell'impatto dei nuovi requisiti di autenticazione forte del cliente (SCA) introdotti con la PSD2 sulla sicurezza dei pagamenti eseguiti da remoto. Per ciascuno strumento di pagamento si costruiscono indicatori di rischio aggregati e si analizza la sicurezza dei pagamenti domestici e cross-border, e dei pagamenti eseguiti da remoto e al punto vendita fisico. Utilizzando un modello per dati panel, si stima che la SCA riduce il rischio di frode del 60 per cento per i pagamenti eseguiti da remoto con carta e dell'80 per cento per quelli effettuati con moneta elettronica. Si stima inoltre che le transazioni per cui la regolamentazione prevede un'esenzione dall'applicazione della SCA risultano relativamente sicure.

* Bank of Italy, Directorate General for Currency Circulation and Retail Payments.

CONTENTS

1. Introduction[1]

The payment system is a key component of modern financial markets and has a direct impact on our daily lives. The many participants involved in the payment system include financial institutions who provide payment services, payment networks and processors who govern the payment schemes and process payment information, and fintech companies and technology startups developing new payment services, as well as payment service users such as consumers paying for their purchases and bills every day, businesses who accept payments through their point of sale terminals, and the government issuing transfers to families and businesses. Retail payment instruments play the role of access keys to the payment system for millions of people around the world and are therefore subject to regulation and oversight by public authorities,[2] who have the goal to maintain a high level of payments security and efficiency, and to preserve a high level of confidence in the payment system among all participants. On the one hand, the degree of safety and efficiency of payment instruments is regarded by central banks and other authorities with a payment system oversight role as a key element to mitigate financial and operational risks relating to the individual payment schemes, thus contributing to ensuring financial stability. On the other hand, a high level of confidence in the payment system is necessary to avoid drastic changes in payment behaviors that could potentially undermine commerce and overall economic activities, as pointed out in the economic literature (Richardson, 2007; Hayashi, Moore and Sullivan, 2015; Chodorow-Reich *et al.*, 2020). The academic literature has also shown how security can influence consumers' payment habits (Arango and Taylor, 2009; Kosse, 2013a and 2013b; Stavins, 2013; Kahn and Liñares-Zegarra, 2015; Kahn, Liñares-Zegarra and Stavins, 2017) or alternatively hinder the adoption of new technologies, such as mobile and faster payments (Schuh and Stavins, 2015).

Several new trends and payment services that have emerged in recent years posed significant challenges to regulators who formulate policies in a rapidly evolving environment. In particular, the digital development of the retail payments market and the rise of e-commerce have favored the use of electronic payments also for transactions performed remotely, for example for online purchases (Markiewicz and Sullivan, 2017; Hayashi, 2020; OSMP, 2021). This trend has been accompanied by a growing demand and a corresponding increase promoted by regulators of the security requirements aimed at preventing

[1] We thank Guerino Ardizzi, Massimo Doria, Paola Giucca, Michele Lanotte, Andrea Nobili, Laura Painelli, Ravenio Parrini, Francesca Provini, Gabriele Sene and an anonymous reviewer at the Bank of Italy for very helpful comments.

[2] The intervention of public authorities on payments security is justified by the characteristics of modern retail payments systems which make it difficult for markets to reach a socially desirable level of security (Hayashi, Moore and Sullivan, 2015). In particular, the potential coordination challenges that may arise among the many participants require a broad and long-term leadership role to foster the adoption of security improvements. Private entities might not be able to play such role, given the potentially high up-front investments involved and the constraints posed by private shareholders who typically require results in the relatively short term.

fraud and ensuring the safety of consumers' funds and personal data (Gates and Jacob, 2009; Cimiotti and Merschen, 2014; Hayashi, 2019; UK Finance, 2021).[3]

Despite the relevance of the topic from an economic and regulatory perspective, the empirical evidence on the security of retail payment instruments is not abundant due to the lack of publicly available data. The main trends identified in the available studies point to a greater riskiness of remote transactions compared to payments made at the physical point of sale and to a higher riskiness of cross-border payments relative to domestic payments (OSMP, 2021; ECB, 2021; EBA, 2022). Time series evidence has also shown how fraud rates on remote card transactions have been trending down in the last years in advanced countries possibly thanks to the regulatory interventions aimed at strengthening customer authentication in online payments (Hayashi, 2020; ECB, 2021).

In this paper, we contribute to the analysis of retail payments security by developing aggregate risk indicators for each payment instrument using new supervisory data collected from Italian payment service providers in 2019-2021 in the context of the EBA Fraud Reporting. The rich information contained in the dataset allows us to compare domestic and cross-border payments as well as remote payments and payments made at the physical point of sale. The aim of this paper is to offer an overview on the topic of retail payments security by comparing the different payment instruments, and to analyze the efficacy of Strong Customer Authentication, a double factor authentication requirement introduced by the revised Payment Services Directive (PSD2), in reducing the risk of fraud in remote transactions using bank level panel data which, to our knowledge, has no precedents in the literature.

The outline of the paper is the following. In the next section, we describe the data and construct aggregate security indicators for the retail payments market as a whole, before introducing the analysis of the individual payment instruments. In particular, the results presented in sections 3 and 4 concern, respectively, SEPA instruments (credit transfers and direct debits) and cash withdrawals. Section 5 analyzes the security of payments made by card and electronic money (including a discussion of the available evidence on unregulated *closed-loop* instruments). In section 6, we explore the impact of Strong Customer Authentication on the risk of fraud in remote transactions carried out with cards and electronic money using bank level panel data. Finally, section 7 summarizes the policy contributions of the paper and concludes.

[3] For the European market, we refer in particular to the numerous provisions issued by the European legislator over the years, culminating in the Second Directive on Payment Services (PSD2). These measures include the recommendations of the European Commission in the Green Paper - Towards an integrated European market for card, internet and mobile payments in 2012; the Recommendations for the security of internet payments of the ESCB Forum on the Security of Retail Payments (SecuRe Pay) of 2013; the Guidelines on internet payments security of the European Banking Authority of 2014.

2. Data

Pursuant to Article 96(6) of PSD2, payment service providers are required to report statistical data on fraud with payment instruments to their national competent authorities, which must aggregate and transmit them to the EBA and the ECB every six months. To harmonize the data collection, the EBA has issued specific guidelines, available from January 2019, which contain the reporting schemes and validation rules.[4] Recently, the ECB has included payment fraud data in a broader data collection under the Regulation on Payment Statistics.[5] The corresponding amendment was adopted by the Governing Council in December 2020, and the data collection has begun in 2022 for data relating to the first half of 2022 and subsequent semesters. The dataset used in this paper contains information on all Italian payment service providers (over 500 intermediaries) observed from the second half of 2019 through the second half of 2021. The semiannual reports contain the number and amount of total and fraudulent transactions carried out with the following payment instruments: credit transfers; direct debits; cards, both on the issuing side and on the acquiring side; cash withdrawals using cards; electronic money; money remittances; transactions arranged by payment initiation service providers. For both domestic and cross-border payments, the reports include also information on the payment execution mode (non-electronic or electronic, remote or non-remote), and on the authentication technology (Table 1).

Table 1: Data availability by payment instrument and payment characteristics

	Overall	Non Electronic	Electronic	SCA Remote	Non SCA Remote	SCA Non Remote	Non SCA Non Remote
Credit Transfers	✓	✓	✓	✓	✓	✓	✓
Direct Debits	✓	✓	✓	-	-	-	-
Cards (issuing)	✓	✓	✓	✓	✓	✓	✓
Cards (acquiring)	✓	✓	✓	✓	✓	✓	✓
Cash withdrawals	✓	-	-	-	-	-	-
E-money	✓	-	-	✓	✓	✓	✓
Remittances	✓	-	-	-	-	-	-
PISP	✓	-	-	✓	✓	✓	✓

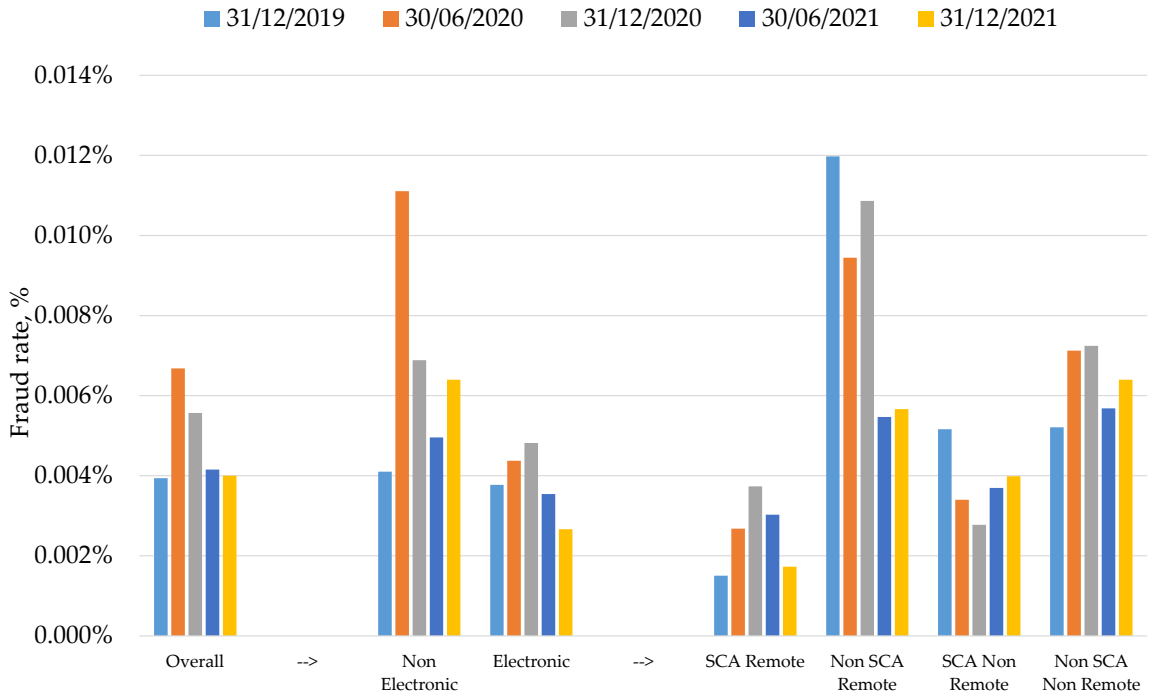
Notes: Summary of the information extracted from EBA Fraud Reporting data by execution mode. Check marks indicate that the information is available. Electronic and Non Electronic are a subset of Overall. SCA Remote, Non SCA Remote, SCA Non Remote, and Non SCA Non Remote are a subset of Electronic.

Before analyzing the individual payment instruments, we first propose an analysis of the security of the retail payments market as a whole. Using the bank level semiannual data on all payment instruments subject to EBA Fraud Reporting, we construct an indicator of the overall security of the retail payments

[4] European Banking Authority (2020), Guidelines on fraud reporting under PSD2. A definition of payment fraud is available in guideline 1 and includes both unauthorized payment transactions and cases of manipulation of the payer (p. 16).

market, as well as aggregate indicators relating to the mode of execution of the transactions (e.g. electronic, remote, with or without SCA). The results are presented in Figure 1.

Figure 1: Fraud rate by execution mode, all instruments



Notes: Calculations based on EBA Fraud Reporting data (see notes to Table 1). Fraud rate calculated as the ratio between the value of fraudulent transactions and the total value of transactions by execution method including all domestic and cross-border payments carried out using all payment instruments subject to EBA Fraud Reporting.

On aggregate, the fraud share on payment transactions in Italy, calculated as the ratio between the value of fraudulent transactions and the total value of transactions carried out with all payment instruments subject to reporting obligations, was 0.005% on average in 2019-2021, which is equivalent to one euro of fraud for every 20,000 euros transacted. The overall fraud rate was at 0.004% in 2019 and 2021 and increased in 2020, when it reached 0.007% in the first semester.

With reference to the execution mode, the fraud rate on electronic payments was mostly below the market average of 0.005% in the years 2019-2021. Among electronic transactions, remote payments executed without SCA (Non SCA Remote) reported the highest fraud rates (more than double the overall market average fraud rate). On the other hand, remote electronic payments executed with SCA recorded a lower than average incidence of fraud in all semesters. For non-electronic transactions, we estimate a higher and more volatile fraud share compared to electronic transactions. The fraud rate was mostly above the market average, including a peak of 0.011% reached in the first half of 2020 due to an increase

[5] Regulation (EU) 2020/2011 of the European Central Bank of 1 December 2020 amending regulation (EU) no. 1409/2013 on payment statistics (ECB/2013/43) (ECB/2020/59).

in fraud with unauthorized direct debits based on non-electronic mandates. As shown in Table 2, the average value of fraud with direct debits is relatively high and explains the impact of this instrument on the overall average fraud share in 2020. Only credit transfers reported a higher average value of fraud. In general, this result is linked to the high average value of transactions carried out with credit transfers and direct debits (Table 3).

Table 2: Average value of fraud by payment instrument

		2019	2020	2021
Credit Transfers	€/transaction	7,946	5,110	4,331
Direct Debits	€/transaction	877	1,137	946
Cards (issuing)	€/transaction	68	83	86
Cards (acquiring)	€/transaction	191	189	175
Cash withdrawals	€/transaction	336	361	430
E-money	€/transaction	56	38	20

Notes: Calculations based on EBA Fraud Reporting data. Average fraud value by instrument, for domestic and cross-border payments (data for 2019 refer to the second semester).

Table 3: Average value of transactions by payment instrument

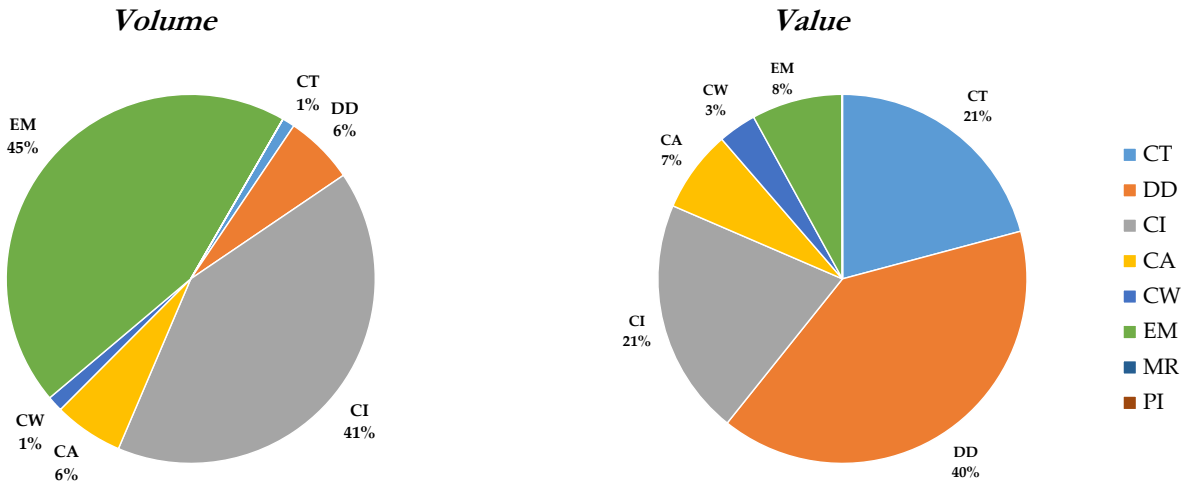
		2019	2020	2021
Credit Transfers	€/transaction	3,916	4,186	5,570
Direct Debits	€/transaction	404	402	411
Cards (issuing)	€/transaction	47	56	52
Cards (acquiring)	€/transaction	59	60	52
Cash withdrawals	€/transaction	231	243	241
E-money	€/transaction	39	38	36

Notes: Calculations based on EBA Fraud Reporting data. Average value of transactions by instrument, for domestic and cross-border payments (data for 2019 refer to the second semester).

It is therefore not surprising that, in comparison with the other payment instruments, credit transfers and direct debits account for a significant share of the overall *value* of fraud in the retail payments market (Figure 2, right panel). On the other hand, cards and electronic money appear to be the most sensitive instruments to fraud from the point of view of the *number* of fraudulent transactions (Figure 2, left panel), even if for small amounts given the relatively low average value of transactions (Table 2 and Table 3). This result is clearly linked to the relative importance of each payment instrument in terms of

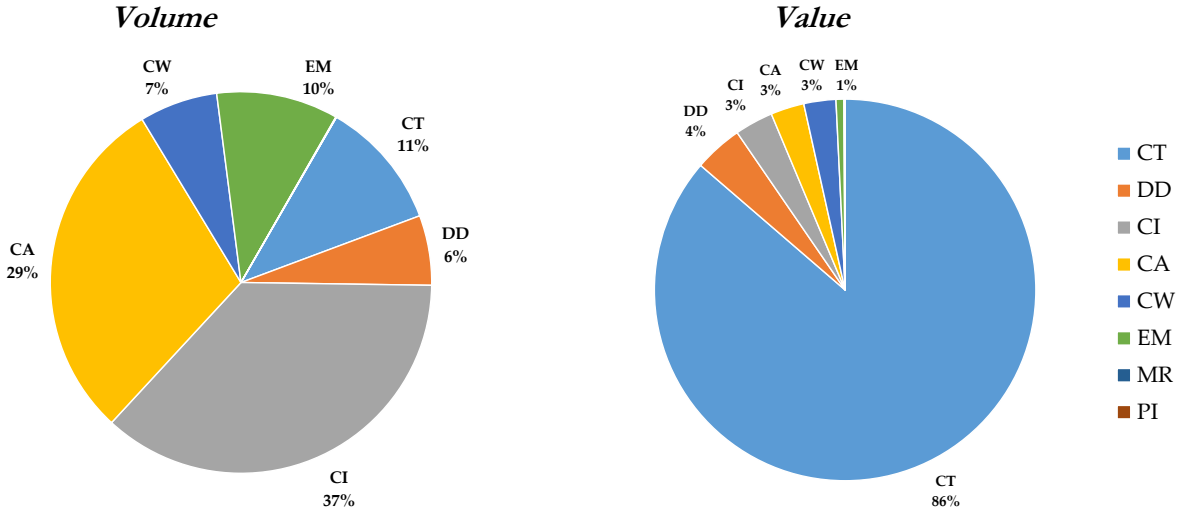
volume and value of transactions in the retail payments market, with credit transfers accounting for most of the value of transactions and cards for most of the volume (Figure 3). Money remittances and transactions arranged by PISP are still relatively less important in the Italian market in terms of both payments and fraud, with market shares well below 1% as shown in Figure 2 and Figure 3, therefore we leave their analysis for future research.

Figure 2: Contribution of payment instruments to the overall volume and value of fraud



Notes: Average values for 2019-2021 calculated using EBA Fraud Reporting data for Italy. CT stands for "Credit Transfers", DD "Direct Debit", CI "Cards Issuer", CA "Cards Acquirer", CW "Cash Withdrawals", EM "E-Money", MR "Money Remittances", PI "Payment Initiation Services". Both domestic and cross-border payments are included in the calculations.

Figure 3: Contribution of payment instruments to the overall volume and value of transactions



Notes: Average values for 2019-2021 calculated using EBA Fraud Reporting data for Italy. See notes to Figure 2.

Finally, with reference to the geo-localization of the transaction (domestic or cross-border within or outside the European Economic Area), on aggregate we estimate a greater incidence of fraud on cross-border transactions, with a fraud share between 0.006% and 0.011% for payments within the European Economic Area and between 0.013% and 0.028% for payments outside the European Economic Area

(Table 10 in the Appendix). For domestic operations instead, we estimate an overall fraud rate between 0.002% and 0.005% on average in 2019-2021. Such higher riskiness of cross-border payments on aggregate, which is in line with the international evidence (OSMP, 2021; EBA, 2022), is also observed within payment instruments and can be ascribed to a number of factors, including the higher attractiveness for fraudsters of jurisdictions outside the European Economic Area with a lower application of e-commerce security, consumer protection standards and cybercrime legislation compared to the European market (UNCTAD, 2021). In the next sections, we turn to the analysis of the individual payment instruments and, within each instrument, we will also consider how the incidence of fraud varies by payment characteristics.

3. SEPA instruments

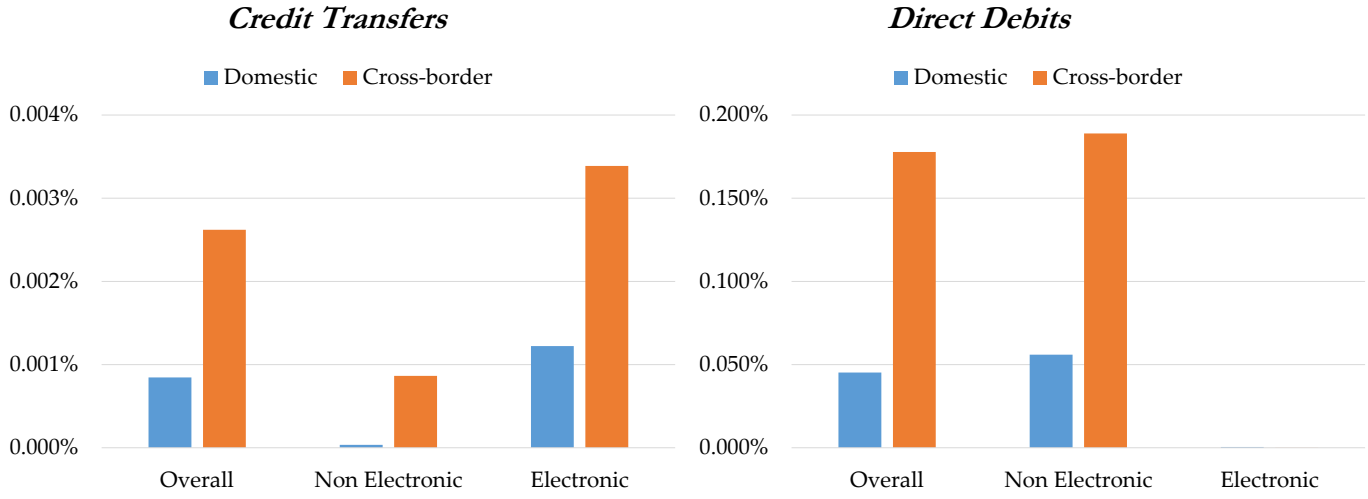
SEPA Credit Transfers (SCT) and Direct Debits (SDD) replaced traditional credit transfers and direct debits following the introduction of the single euro payments area. As described in the previous section, SCT and SDD are used for medium-high value transactions in Italy (respectively around 4,500 and 400 euro on average in 2019-2021, Table 3), and account for around 90% of the overall value of payments in the market (Figure 3). Therefore, the incidence of fraud on payments made using these instruments is an important determinant of the security of the retail payments market in general (Figure 2, right panel), also considering the high average value of fraudulent transactions carried out with SCT and SDD (Table 2).

Based on the data collected within the EBA Fraud Reporting framework, we estimate an aggregate fraud rate on the value of domestic and cross-border transactions carried out with SCT of 0.001% on average in 2019-2021. Thus, the SCT is a very safe instrument with a fraud rate below the average market rate (0.005% on average in the same period, Figure 1). This finding is consistent with the available international evidence (EBA, 2022). There is considerable heterogeneity at the level of both the geo-localization of payments (domestic or cross-border) and the mode of execution (electronic or non-electronic). Specifically, as shown in Figure 4 (left panel), cross-border SCT are on average more risky with a fraud rate equal to three times that of domestic credit transfers while, with reference to the execution mode, electronic transfers (over 90% of SCT) carry a greater risk of fraud compared to SCT arranged at the bank counter. Domestic SCT placed at the bank counter are particularly safe, with a fraud rate close to zero. While a distinction between SCA and non-SCA credit transfers is available in the data (Table 1), the two groups of payments are not really comparable, as non-SCA credit transfers are likely subject to alternative security protocols that may trigger a SCA exemption (as explained in more detail in section 6) while remote SCA transfers are inherently more prone to fraud because of the high attractiveness of such payments for fraudsters also considering the high average amount involved and

the possibility for scammers to circumvent or neutralize the use of SCA in payer manipulation incidents which account for one into ten fraud incidents on domestic electronic SCT and one into three fraud incidents on cross-border electronic SCT on average in 2019-2021.

Other than payment manipulation, we estimate that fraud on domestic payments carried out with electronic SCT is mostly attributable to payment orders issued by fraudsters (around 70% of fraudulent transactions), while the rest is due to the modification of payment orders by fraudsters (20% of fraud incidents). With reference to cross-border electronic SCT, aside from payer manipulation incidents, fraud is mostly attributable to the issuance of payment orders by fraudsters (around 65% of fraudulent transactions), in line with domestic payments.

Figure 4: Fraud rates on the value of SCT and SDD transactions



Notes: Average values for 2019-2021 calculated using EBA Fraud Reporting data for Italy.

The aggregate fraud share on domestic and cross-border transactions carried out with SDD was instead equal to 0.047% on average in the period 2019-2021. The SDD is therefore more prone to fraud on average compared to the SCT. Cross-border transactions present a particularly high risk of fraud (0.178%) relative to domestic transactions (0.045%) but they weigh little on the aggregate fraud rate since almost all payment transactions carried out with SDD are domestic (over 98% of payments). With reference to the execution mode, the fraud share is substantially determined by direct debits based on non-electronic mandates (that account for approximately 80% of total SDD transactions) and is primarily due to unauthorized payments, while direct debits based on electronic mandates present near zero fraud rates (Figure 4, right panel).

4. Cash withdrawals

Despite the growing digitalization of retail payments, the use of cash remains widespread among Italian consumers (ECB, 2020; Baldo *et al.,* 2021; Ardizzi and Cologgi, 2022; Coletti *et al.*, 2022). In Italy, the main access points to cash are bank tellers or post offices and automatic teller machines (ATMs), where cash is withdrawn by means of card transactions. The EBA Fraud Reporting data contain information on cash withdrawal operations carried out with cards for over 500 Italian payment service providers. Despite the relatively high average value of fraudulent transactions (above 300 euros, Table 2), cash withdrawals account for a low share of fraud in the market (1% in terms of volume and around 3% in terms of value, Figure 2). Considering both domestic and cross-border transactions, we estimate an aggregate fraud share on the value of cash withdrawals of 0.006% on average in the period 2019-2021, corresponding to approximately one cent for every 200 euros withdrawn. This fraud rate is consistent with the European average estimated for the second half of 2020 (EBA, 2022) and is very close to the overall market average rate (0.005%, Figure 1). Therefore, cash withdrawals appear to be relatively safe transactions with a fraud rate substantially in line with the overall market average. As shown in Table 4, the fraud rate is determined by domestic transactions which make up 99% of cash withdrawals.

Table 4: Fraud rates on the value of cash withdrawals

			Type of fraud		
	Share of transactions	Fraud rate	Lost or stolen card	Counterfeit card	Other
Domestic	99.0%	0.006%	79%	16%	5%
Cross border within EEA	0.6%	0.016%	73%	20%	7%
Cross border outside EEA	0.4%	0.056%	18%	74%	8%

Notes: Average values for 2019-2021 calculated using EBA Fraud Reporting data for Italy. EEA stands for European Economic Area.

Fraud on domestic or cross-border cash withdrawals within the European Economic Area is mainly due to withdrawal operations with lost or stolen cards (over 70% of fraudulent transactions on average in the period 2019-2021) or counterfeit cards (16-20%). As for fraudulent withdrawals carried out outside the European Economic Area (0.4% of total cash withdrawals), over 70% of fraud occurs due to card counterfeiting (Table 4), consistently with the view that misappropriated or counterfeited payment instruments - even if stolen domestically - can be exploited more easily abroad due to less stringent payment security standards. With regards to the distribution of economic losses, payment service providers reported that on average the economic losses due to cash withdrawal fraud are mainly borne by payment service users (68% of losses).

5. Cards and electronic money

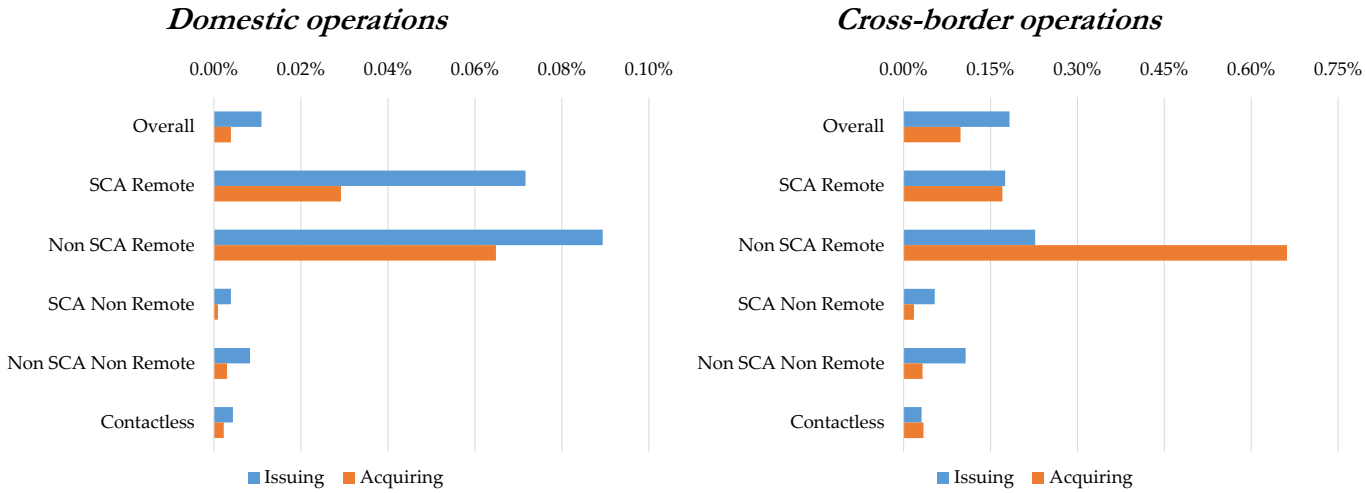
Payments carried out with cards and electronic money (e-money) are the most sensitive to fraud. In section 2, we showed that most of the fraudulent transactions in the years 2019-2021 are attributable to cards or e-money (Figure 2). Despite the high volume of fraudulent transactions we do not find an equally high incidence of these instruments on the total value of fraud, due to the low average value of fraudulent transactions in comparison with other payment instruments (Table 2). We also showed how this result is directly related to the fact that cards and e-money account for most of the volume of payments in the market but for a relatively small share of the value of payments, given the low average value of transactions (around 40-50 euros, Table 3). In paragraphs 5.1 and 5.2, we separately analyze the security of payments made with cards and electronic money using aggregate risk indicators. The two instruments show several similarities. In particular, for both instruments, cross-border operations are more prone to fraud relative to domestic operations while, in terms of execution mode, transactions carried out remotely report the highest incidence of fraud, essentially attributable to payment orders issued by fraudsters with counterfeit cards or stolen card details. It is therefore not surprising that the European regulator has introduced greater security requirements with PSD2, precisely for this type of payments. In this regard, section 6 explores in detail the impact of Strong Customer Authentication (SCA) in lowering the risk of fraud in payments made remotely with cards and e-money using a simple empirical strategy based on bank level panel data.

5.1. Cards

The EBA Fraud Reporting data include information on transactions made with cards with a debit function and transactions made with cards with a credit or delayed debit function. If we consider payments made with cards issued within Italy and acquired worldwide (issuing side), we estimate a fraud share on the value of transactions equal to 0.031% on average in 2019-2021, which is in line with the available estimates for the euro area (ECB, 2021; EBA, 2022). If we look at payments made with cards issued worldwide and acquired within Italy (acquiring side) we estimate a fraud rate equal to 0.012%, which is below the available estimates for the euro area.

With reference to the geo-localization of payments, we estimate that cross-border transactions, about 10% of total card transactions, carry a higher risk of fraud compared to domestic transactions. During 2019-2021 we estimate that, as regards domestic payments (Figure 5, left panel), the fraud rate on the value of transactions was 0.011% if we consider the card issuer side, and equal to 0.004% from a card acquiring perspective. The fraud rate on the value of cross-border transactions was instead equal to 0.183% on the issuing side and 0.098% on the acquiring side (Figure 5, right panel).

Figure 5: Fraud rates on the value of card transactions



Notes: Average values for 2019-2021 calculated using EBA Fraud Reporting data for Italy.

The lower fraud rate on the acquiring side, which compared to the issuing side also includes cards issued by foreign banks (e.g. for transactions carried out by consumers not resident in the national territory), can be explained in part by the heterogeneous application of SCA between issuing and acquiring. From a card issuer perspective, most remote payments were executed without strong authentication in the years 2019 and 2020. In fact, we estimate that transactions carried out with SCA amounted to only 17% of total domestic remote transactions in the period 2019-2020, a percentage which drops to 6% if we consider cross-border transactions. As regards the acquiring side, on the other hand, the share of remote payments carried out with SCA was over 40% regardless of the geo-localization of the transaction. This may have contributed to the lower fraud rates reported by card acquirers relative to card issuers.

The application of SCA affects especially the security of remote transactions which are particularly sensitive to fraud as shown in Figure 5. For remote card payments (issuing side), we estimate aggregate fraud shares between 0.1% and 0.2% in 2019-2021, in line with the international evidence (Hayashi, 2020). We observe significant heterogeneity at the level of the geo-localization and execution mode. In particular, as shown in Figure 5, cross-border payments reported higher fraud rates than domestic payments, while SCA payments reported a lower incidence of fraud compared to non-SCA payments. Similarly, for the acquiring side we estimate that the fraud share on transactions acquired with SCA was less than half the fraud share on non-SCA transactions both domestic and cross-border (Figure 5). For cross-border payments, we estimate a particularly high incidence of fraud (0.662% of the value of transactions) on remote payments acquired without SCA mostly due to incidents of card details theft.

From a card issuer perspective, fraud on remote transactions executed with strong authentication is mostly due to the issuance of payment orders by fraudsters using stolen card details (70% of fraud incidents on average in 2019-2021) or counterfeit cards (around 15% of fraudulent transactions). Instead,

for non-SCA remote payments, over 50% of fraud incidents are due to counterfeit cards while card details theft accounts for around one into three fraudulent transactions.

Payments carried out at the physical point of sale reported markedly lower fraud rates than those carried out remotely, even payments that use the contactless technology (Figure 5). On the issuing side, the fraud rate on domestic transactions carried out at the physical point of sale with SCA is 0.004% (0.054% for cross-border transactions), while for transactions carried out without SCA the fraud rate is 0.008% (0.107% for cross-border transactions). Contactless payments, which are included among payments performed at the physical point of sale without strong authentication (Non SCA Non Remote), reported a fraud share of 0.004% in domestic operations and 0.031% in cross-border operations on average during 2019-2021. In terms of burden sharing, i.e. the distribution of economic losses deriving from fraud in card payments, payment service users have borne a share of losses due to fraud equal to approximately 30% of total losses on the issuing side, and over 80% on the acquiring side consistently with the higher application of SCA from a card acquiring perspective.

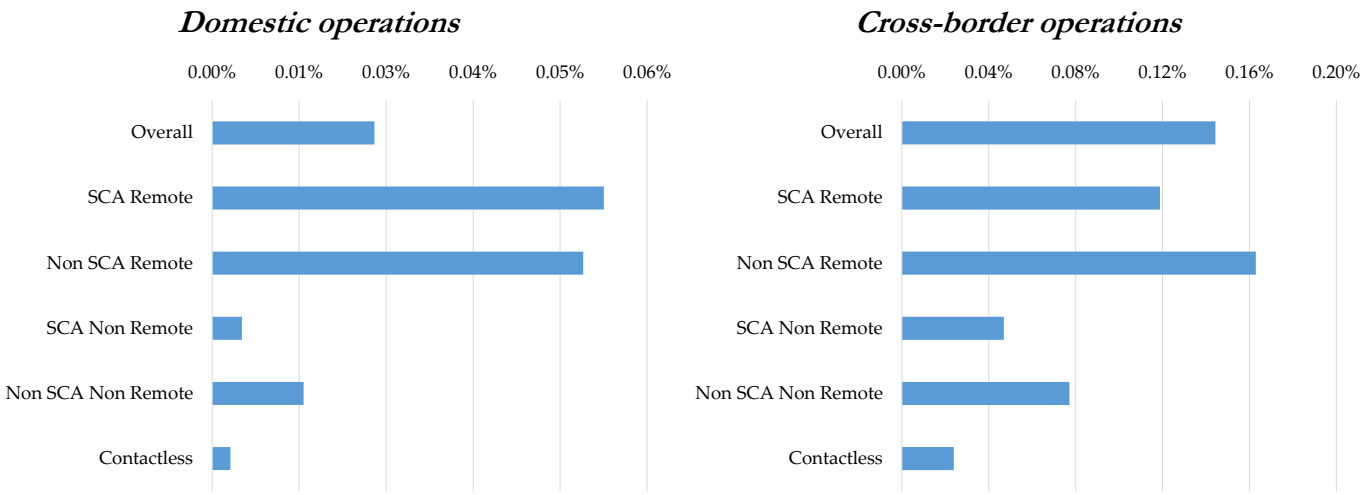
5.2. Electronic money

Electronic money instruments include prepaid credit and debit cards, and *open-loop* and *closed-loop* cards subject to *Know-Your-Customer* (KYC) anti-money laundering requirements that ensure high standards of transparency regarding the identity of users and the lawful origin of consumers' funds. These instruments are subject to the European regulation on payments (PSD2, E-money directive and the fifth directive on anti-money laundering, AML5). Included in the category are also other *closed-loop* cards which are not formally identified as electronic money instruments and therefore are not subject to KYC requirements[6] and are outside the scope of European regulation. These cards can only be used for purchases from the merchants that issue them (e.g. *gift cards*, *store cards*, *petrol cards* or *casino cards*).

In the case of e-money instruments issued by payment service providers and subject to regulation, it is possible to construct aggregate security indicators based on the EBA Fraud Reporting data.

[6] Therefore they are anonymous payment instruments. Under the AML5 Directive, only customers who purchase *closed-loop* cards for amounts over 10,000 euro need to be audited.

Figure 6: Fraud rates on the value of e-money transactions



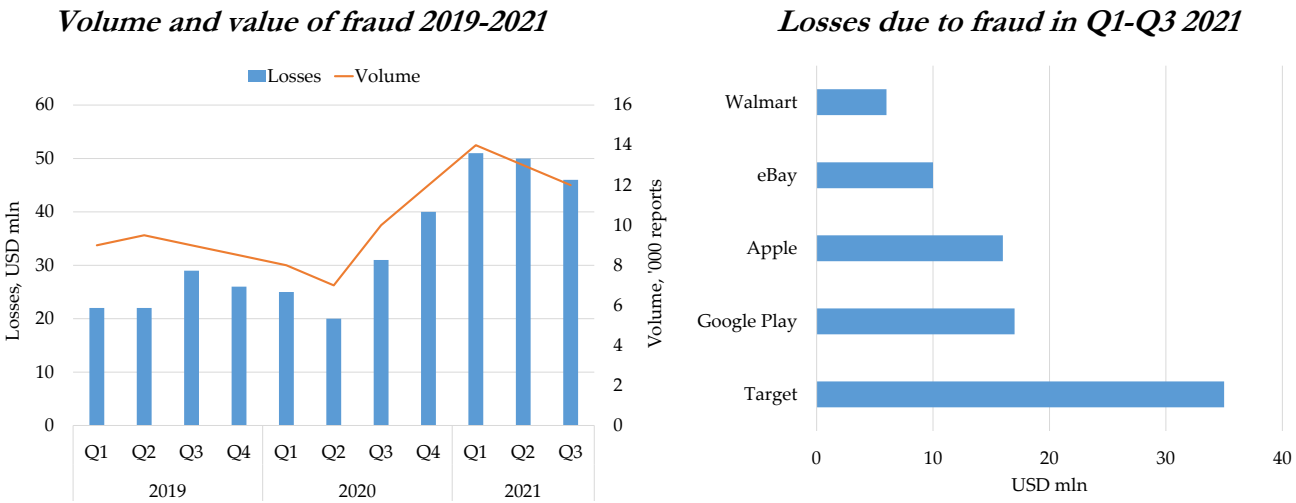
Notes: Average values for 2019-2021 calculated using EBA Fraud Reporting data for Italy.

With reference to the geo-localization of the transactions, in line with the evidence presented in the previous section on card payments, cross-border payments were on average more subject to fraud compared to domestic payments in 2019-2021. On aggregate, for cross-border payments we estimate a fraud rate on the value of transactions equal to 0.144%, while for domestic transactions we estimate a fraud rate of 0.023% (Figure 6). In comparison with credit and debit cards, e-money payments are more risky if we consider domestic transactions (with a fraud rate equal to about double that of card transactions), and less risky if we consider cross-border transactions. As in the case of card payments, there is considerable heterogeneity with respect to the payment execution method. In particular, remote payments present a greater risk of fraud compared to payments made at the physical point of sale (Figure 6) because of a higher incidence of payment orders issued by fraudsters, in line with the evidence presented in the previous section on card payments. For remotely executed domestic transactions, the fraud rate on non-SCA payments was 0.053% on average over the period 2019-2021, broadly in line with the fraud rate on the value of payments made with SCA (0.056% on average over the same period). Instead, for cross-border remote payments carried out with SCA we estimate a fraud rate of 0.119% (0.163% for payments made without SCA). The impact of SCA on the security of e-money remote payments will be further analyzed in section 6.

Payments made at the physical point of sale experienced much lower fraud rates than remote payments. The fraud rate was 0.004% for domestic SCA transactions (0.047% for cross-border transactions), and 0.013% for domestic transactions carried out without SCA (0.077% for cross-border transactions). Contactless payments reported fraud rates in line with those observed for cards, specifically 0.003% for domestic transactions and 0.024% for cross-border transactions. In terms of burden sharing, in line with what we observe in the case of cards (issuing side), payment service users have borne a share of losses due to fraud equal to about 30% of total losses on average in the period 2019-2021.

With reference to unregulated e-money products, on the other hand, based on the available evidence there is a significant exposure to the risk of fraud for consumers who use *closed-loop* instruments such as *gift cards*. These instruments are particularly sensitive to fraud due to the anonymity and irreversibility of the transactions to which consumers could be induced by scammers. In Europe and the USA this phenomenon has attracted the attention of trade associations and consumer protection authorities, in particular the Euro Banking Association and the Federal Trade Commission (FTC).[7] Data on fraud in the European market are not yet available, while for the American market the FTC has collected over 30,000 reports of fraud with *gift cards* per year since 2019, for an increasing value of economic losses on average around 120 million dollars per year in 2019-2021 (Figure 7, left panel). According to the data collected by the FTC, the *gift cards* most prone to fraud are those of large distribution chains such as Target and Walmart, online retailers such as eBay and cards for purchases on *big-tech* platforms such as Apple and Google Play (Figure 7, right panel).

Figure 7: Gift card fraud in the US



Notes: Federal Trade Commission (2021).

[7] For a review of the risks and regulation regarding *closed-loop* instruments in Europe and the United States see Euro Banking Association (2020) and Federal Trade Commission (2021).

6. The impact of SCA on security

The regulation on SCA requires that electronic payments must be authenticated with at least two of three factors[8] with the addition, for online payments, of a complex dynamic code specifically associated with the online payment. In order to ensure a balance between safety rules, speed and ease of use of the instruments subject to regulation, the legislation provided for exempting intermediaries from the generalized application of SCA in online payments according to a specific analysis of the risks connected to the transaction (so-called transaction risk analysis), as well as additional exemptions specific to particular types of transactions. Given the complexity of the adjustments required, the migration to SCA entailed a certain cost for payment service providers and also in terms of user experience during the remote payment process. According to recent evidence, SCA has also caused a decrease in online cart conversion rates and put pressure on the profitability of e-commerce retailers.[9] This dynamic raised concerns about the benefits of SCA among stakeholders, who also highlighted the lack of evidence on its effectiveness in reducing the risk of fraud in e-commerce transactions.[10]

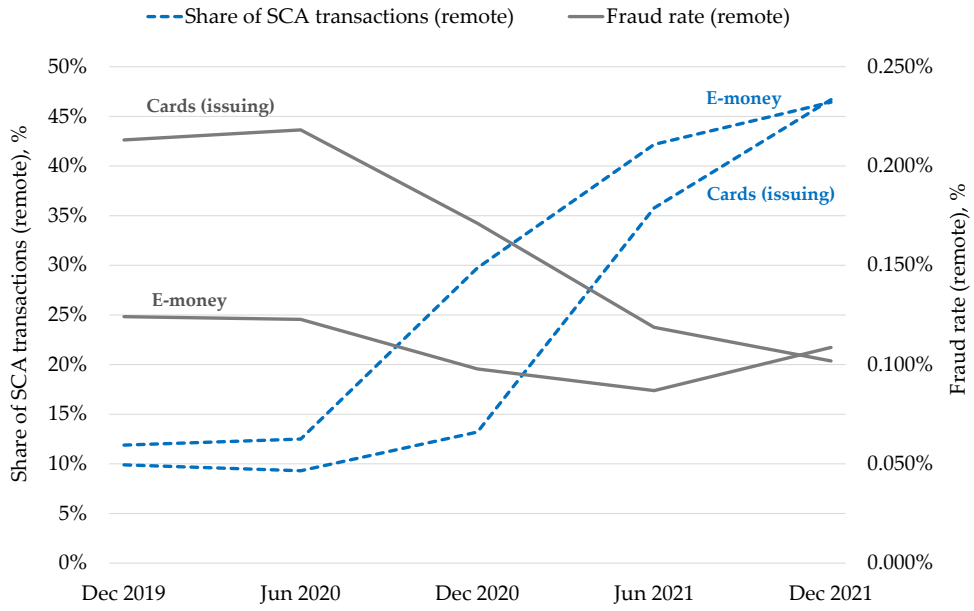
At first glance, from the analyses presented in the previous paragraphs on cards and e-money, the security measures introduced by PSD2 may seem to have a relatively low impact on the risk of fraud in transactions carried out remotely (Figure 5 and Figure 6). The aggregate fraud rates of SCA payments are in fact very similar to those of non-SCA payments. However, it should be noted that aggregate fraud rates do not take into account the variation in the use of SCA over time within and across payment service providers. As mentioned in section 5, most online card transactions were performed without SCA until the end of 2020, and it is only from the following year that the percentage of SCA transactions began to rise in correspondence with the completion of the migration to SCA by Italian payment service providers. In Figure 8, we analyze more in detail the evolution of fraud rates in relation to the use of SCA in payments made remotely by card and e-money.

[8] The three categories are: 1) knowledge (something only the payer knows) such as a password, PIN, passphrase or secret answer; 2) possession (something that only the payer owns) such as a mobile phone, smartwatch, smart card or token; 3) inherence (something the payer is) e.g. a fingerprint, facial recognition, voice patterns, iris format.

[9] See for example the Joint Letter on measuring the impact of SCA addressed to the European Commission and the European Banking Authority by online retailers associations EuroCommerce and Ecommerce Europe in 2021. The costs associated with increased security requirements in online payments are in principle due to the greater difficulty for users to finalize the payment process. An Italian bank computed that 22% of online purchases in the first semester of 2021 did not complete because of problems with the application of SCA (Distante *et al.*, 2022). Ardizzi (2017) also provides empirical support for this view and finds a significant negative impact of security innovation on user experience measured by online card turnover.

[10] Among the available studies, EBA (2022) uses country level data on payment fraud for the second half of 2020 in the Eurozone and finds lower fraud rates for SCA authenticated card transactions compared to non-SCA transactions. Earlier studies on the trends of fraud rates in online transactions suggest an improvement in the security of remote payments in recent years (Ardizzi, Bonifacio and Painelli, 2020; Hayashi, 2020; EBA, 2021; ECB, 2021). However, these studies do not offer a quantitative assessment of the impact of SCA on the risk of fraud, due to the lack of data on the distribution of payments and fraud by customer authentication mode.

Figure 8: Use of SCA and fraud in remote transactions



Notes: Calculations based on the value of domestic and cross-border transactions from EBA Fraud Reporting.

Specifically, for both instruments, we report the share of remote payments carried out with SCA and the fraud rate on the value of remote payments from 2019 to 2021. The results suggest a significant impact of SCA on the security of remote transactions. With the completion of the migration to the new customer authentication standards, the use of SCA in Italy has progressively increased reaching almost 50% of payments made remotely by card and e-money in 2021. Together with the increase in the share of transactions performed with SCA, we observe a clear decrease in the fraud rate on the value of remote transactions, as large as 52% for cards and 30% for e-money.

To further investigate the role of SCA in reducing the risk of fraud in remote payments, we use a simple empirical strategy based on a regression framework, exploiting the panel dimension of the EBA Fraud Reporting data at the bank level. The objective is to obtain an estimate of the average impact of SCA on the risk profile of remote payments made with cards and e-money, by exploiting the within bank variation in the use of SCA and taking into account bank specific unobservable characteristics that are constant over time and potentially correlated with the use of SCA in remote payments (e.g. the degree of technological evolution of the services offered, the use of other internal security protocols, or customer preferences with respect to remote payments), as well as generic fluctuations in the incidence of fraud common to the entire retail payments market (such as the impact of the restrictions put in place to contrast the covid-19 pandemic on the use of remote payments).

Using an econometric model for panel data with bank and time fixed effects, for each payment instrument we estimate the elasticity of the total value of fraud to the value of payments made remotely

with SCA and without SCA. Specifically, for each payment instrument and execution mode j, we estimate the model:

$$Fraud_{it} = \alpha + x_j Payments_{it}^{j} + u_i + h_t + \varepsilon_{it} \quad (1)$$

where all variables are expressed in logarithm, u_i is a bank fixed effect, h_t is a time effect and ε_{it} is a residual term. The elasticity x_j is a measure of the fraud risk associated with the two execution methods. This measure of fraud risk, that is related but different from the fraud rate, can be interpreted as a more 'dynamic' security indicator. For example, for a given instrument, a 1% increase in payments executed with or without SCA is associated with an increase in fraud equal to x%, where x is the elasticity estimated by the panel regressions. The impact of SCA on the risk of fraud is then calculated as the difference between the two estimated elasticities, in the vein of a difference-in-differences type analysis. More explicitly, on the basis of the parameters x_j estimated for each execution mode j (1 = remote SCA, 2 = remote non-SCA), we calculate the SCA risk premium of each payment instrument as:

$$SCA\ premium = x_1 - x_2 \quad (2)$$

The results are presented in Table 5. Alongside the coefficients we report the t-statistics calculated with robust standard errors. In the last two columns of Table 5, we consider the difference between the elasticities of payments made remotely with SCA and without SCA and its statistical significance, calculated using the methodology outlined in Clogg, Petkova and Haritou (1995).[11]

Looking at domestic card payments, the results show that the risk of fraud in remote payments is mainly due to non-SCA payments (the elasticity being equal to 0.31, against 0.13 for payments executed with SCA). Payments made with SCA have a better risk profile than non-SCA payments, quantifiable in 18 basis points and statistically significant. To put it differently, based on the percentage variation between the two elasticities (that is, $SCA\ premium/x_2$), remote card payments made with strong authentication have on average a 58% lower risk of fraud than payments made without SCA. Similarly, for e-money payments carried out remotely, we estimate a lower risk of fraud due to the use of SCA quantifiable in 21 basis points, or alternatively an 81% lower risk of fraud compared to payments carried out without SCA. Therefore, as regards card payments, we obtain an estimate of the impact of SCA in line with the results of the aggregate fraud rates analysis presented in Figure 8, which showed that as the share of transactions carried out with SCA increases between 2019 and 2021, the fraud share has halved. As for e-money payments, on the other hand, the result is very different. On aggregate, we observe a decrease

[11] Specifically, we calculate a z-score as $Z = \frac{x_1 - x_2}{\sqrt{(\hat{\sigma}x_1)^2 + (\hat{\sigma}x_2)^2}}$, where $\hat{\sigma}x_j$ is the robust standard error of the coefficients x_j estimated by the panel regressions.

in the fraud rate of around one third. By exploiting the within bank variation in the use of SCA and controlling for bank specific unobservable factors, we obtain a much larger estimate of the impact of SCA on the security of remote payments carried out with e-money (81% lower risk of fraud), which signals the presence of significant heterogeneity across payment service providers not captured by the analysis of aggregate risk indicators. As shown in Table 5, the results are similar if we analyze the perimeter of cross-border payments, which are confirmed to be more risky than domestic payments in line with the analyses presented in paragraphs 5.1 and 5.2, and with the international evidence (ECB, 2021; EBA, 2022).

Table 5: Risk of fraud in remote payments with and without SCA

	Remote SCA	t-statistic	Remote Non SCA	t-statistic	SCA premium	z-score
Domestic						
Cards Issuer	0.127***	(3.834)	0.305***	(4.966)	-0.178**	(-2.551)
E-Money	0.051**	(2.497)	0.262***	(6.281)	-0.211***	(-4.543)
Cross-border (within EEA)						
Cards Issuer	0.125***	(3.445)	0.322***	(5.545)	-0.197***	(-2.877)
E-Money	0.082***	(3.295)	0.356***	(6.377)	-0.274***	(-4.483)
Cross-border (outside EEA)						
Cards Issuer	0.154***	(3.797)	0.324***	(5.109)	-0.170**	(-2.258)
E-Money	0.153***	(6.433)	0.354***	(6.077)	-0.201***	(-3.195)
Intermediaries	554		554			
Observations	2,421		2,421			

Notes: *** p <0.01, ** p <0.05, * p <0.1. For each payment instrument, each coefficient is obtained from a regression of the logarithm of the total fraud value on the logarithm of the value of remote payments made with or without SCA using EBA Fraud Reporting semiannual data for 2019-2021. All regressions include bank and time fixed effects. The SCA risk premium is estimated as the difference between the elasticities of payments made with SCA and the elasticities of payments made without SCA. Its significance is calculated according to the method described in Clogg, Petkova and Haritou (1995), see also footnote 11.

The impact of SCA on the security of cross-border payments within the European Economic Area is similar in magnitude to that estimated for domestic payments (around 60% lower risk of fraud for cards and 80% for e-money), while for cross-border payments made outside the European Economic Area we estimate that SCA reduces the risk of fraud by half for both cards and e-money, consistently with the view that jurisdictions outside the European Economic Area are more attractive for fraudsters.

Using the same analytical framework, we can also look into the impact of SCA exemptions in specific types of remote payments on the risk of fraud as previously defined. As already mentioned, the

legislation provided for exempting intermediaries from the generalized application of SCA in online payments, and in particular it has allowed the exemptions of low value payments, payments directed to a trusted beneficiary (including payments to self), recurring transactions, payments processed through secure corporate payment protocols, and payments subjected to transaction risk analysis.[12] These types of payments account for a significant and growing share of the value of remote card and e-money payments executed without SCA in our sample. Considering both domestic and cross-border card payments, we estimate that this share went from 3% in the second half of 2019 to 24% at the end of 2021, while for e-money the share of SCA exempted transactions went from 5% to 15%. By comparing the estimated elasticities of SCA-exempted payments to the elasticities of SCA payments, we can assess whether SCA exemptions expose consumers to a relatively higher risk of fraud. Our analysis shows that these types of transactions do not report a higher risk of fraud compared to SCA transactions (Table 6).

Table 6: Risk of fraud in remote payments exempted from the application of SCA

	Remote SCA	t-statistic	Remote Non SCA (exempted)	t-statistic
Domestic				
Cards Issuer	0.127***	(3.834)	0.066*	(1.743)
E-Money	0.051**	(2.497)	0.034	(1.142)
Cross-border (within EEA)				
Cards Issuer	0.125***	(3.445)	0.101***	(2.721)
E-Money	0.082***	(3.295)	0.069**	(2.233)
Cross-border (outside EEA)				
Cards Issuer	0.154***	(3.797)	0.048	(0.595)
E-Money	0.153***	(6.433)	0.046	(0.655)
Intermediaries	554		554	
Observations	2,421		2,421	

Notes: *** p <0.01, ** p <0.05, * p <0.1. See notes to Table 5.

The estimated elasticities of fraud to SCA exempted payments are not statistically significant in the case of domestic and cross-border payments outside the European Economic Area. The elasticities are only significant in the case of cross-border transactions within the European Economic Area but the

[12] The exemptions are specified in the Regulatory Technical Standards on strong customer authentication and common and secure open standards of communication (European Commission, 2017. See in particular articles 13-18). In addition to SCA exempted payments, merchant initiated transactions, which are not subject to art. 97 of PSD2, do not require the application of SCA. A flag for merchant initiated transactions has been made available in the EBA Guidelines since 2020 together with a flag for other types of non-SCA remote payments. We do not include these types of payments in our computations of the independent variable used in the regression analysis presented in Table 6.

coefficients are smaller than the elasticities of SCA payments, indicating that remote transactions exempted from the application of SCA are relatively safe.

In conclusion, the evidence presented in this section points to the important role that SCA plays in reducing the risk of fraud in remote payments. The gains from SCA are estimated at 60% lower risk of fraud in the case of cards, and 80% lower risk of fraud in the case of e-money for domestic and cross-border payments within the European Economic Area, and around 50% lower risk of fraud for both instruments in cross-border payments outside the European Economic Area. The results presented in this section are confirmed also if we use data on the volume rather than on the value of transactions (Appendix). We have also analyzed the role of specific types of SCA exemptions and found that they do not increase the risk of fraud in remote payments. This result is relevant for the discussion regarding the development of new security protocols alternative to SCA, in view of the concerns raised by stakeholders about the costs of a double-factor authentication requirement especially in terms of user experience.

In this regard, we leave for future research the assessment of a potential shift of consumers towards instruments issued by payment service providers not subject to SCA regulation, or the impact on online carts abandonment which are important determinants of the net economic benefits of SCA in the retail payments market. In general, an analysis of the net economic impact of SCA would need to take into account the costs and benefits for all payment system participants including consumers, businesses, and the public sector. Such a cost-benefit analysis would have to consider not only the costs borne by payment service providers to adapt to the new regulatory standards, the savings in terms of less fraud or the costs in terms of user experience, but also the benefits induced by greater trust in electronic payment instruments over a long term horizon, which we view as a public good. In fact, the regulatory intervention on the security standards applied to electronic payments was also aimed at increasing confidence in modern payment instruments and in e-commerce, which has grown by more than 50 percent in terms of volumes processed during the last three years in Italy.

However, based on the available data we can provide useful insights on some of the key parameters mentioned above. With regards to the savings in terms of less fraud on online payments due to the use of SCA, it is possible to construct a simplified counterfactual policy exercise using the EBA Fraud Reporting data. According to a back of the envelope calculation, on the basis of fraud and transactions carried out remotely with cards and e-money in the period 2019-2021, and assuming a fraud rate fixed at 2019 levels (when SCA was applied only to 11% of remote transactions), we estimate a saving in terms of less fraud of approximately 60 million euros overall in the five semesters considered in the analysis, or alternatively a saving of around 25 million euros per year on remote payments made by card and e-money (Table 11 in the Appendix).

With reference to the costs for businesses and consumers, we currently lack the data to quantify the economic loss for e-commerce retailers deriving from a hypothetical decrease in online cart conversion rates attributable to the higher failure rates of SCA transactions. Furthermore, we do not have data on the "social cost" for consumers associated with a worsening of the user experience in remote SCA payments. In this regard, however, the available evidence has shown that the difficulties for consumers and operators might be limited to the first months after the migration to the new standards, and might be substantially overcome as users increase the take-up of the new authentication solutions (OSMP, 2021; Figure 9 in the Appendix).

7. Conclusion

This paper offers an overview on the topic of retail payments security using new supervisory data reported by Italian payment service providers in 2019-2021 in compliance with EBA Fraud Reporting obligations. We construct aggregate risk indicators for cash withdrawals, credit transfers, direct debits, cards and electronic money, and compare domestic and cross-border payments as well as remote and non-remote payments.

In summary, cash withdrawal operations performed with payment cards are relatively safe transactions with a low incidence of fraud, mainly due to lost or stolen cards. With regard to SEPA instruments, payments made with Credit Transfers (SCT) are associated with very low fraud rates. Fraud is mostly due to payment orders issued by fraudsters and payer manipulation incidents on electronic SCT. Direct Debits (SDD) present higher risks of fraud compared to SCT due to the incidence of unauthorized payment transactions especially on SDD based on non-electronic mandates. In comparison with the other payment instruments, SCT and SDD report the highest average value of fraud also because of the high average value of transactions carried out with these instruments, and therefore account for a significant share of the overall value of fraud in the retail payments market.

Cards and electronic money appear to be the most sensitive instruments to fraud from the point of view of the number of fraudulent transactions, even if for small amounts given the relatively low average value of transactions. Fraud is mostly due to payment orders issued by fraudsters with counterfeit cards or using stolen card details. Among electronic money instruments, we described how some unregulated *closed-loop* products (such as *gift cards*) carry potentially high risks for consumers due to the non-traceability and irreversibility of transactions and how these instruments have come under the scrutiny of private sector associations and consumer protection authorities in Europe and the United States. For both electronic money and card based transactions, cross-border payments are on average more risky than domestic payments, just as payments carried out without Strong Customer

Authentication (SCA) present a greater risk of fraud, in particular in the case of remote transactions (for example for online purchases).

In this paper, we documented the important role of SCA in mitigating the risk of fraud in remote payments with cards and electronic money. The gains from SCA are estimated at 60% lower risk of fraud in the case of cards, and 80% lower risk of fraud in the case of e-money for domestic and cross-border payments within the European Economic Area, and around 50% lower risk of fraud for both instruments in cross-border payments outside the European Economic Area. According to a simple back of the envelope calculation, we estimate that SCA saved on average 25 million euros per year in terms of less fraud on online card and e-money payments in 2019-2021. We also estimate that SCA exemptions provided for in articles 13-18 of the Regulatory Technical Standards on SCA do not increase the risk of fraud in remote transactions, which is relevant for the discussion regarding the development of new security protocols alternative to SCA that might protect consumers from the vulnerabilities of remote payments and avoid the burden of a double-factor authentication requirement that has been associated with online carts abandonment and the exclusion of consumers less accustomed to technology.

References

Arango, C. and V. Taylor (2009), "The role of convenience and risk in consumers' means of payment", Discussion Papers, Bank of Canada.

Ardizzi, G. (2017), "Innovation in Customer Authentication Methods, Card-Based Internet Payments and User Experience: Empirical Evidence from Italy", Joint ECB-Bank of Italy Conference, Rome, 30 November-1 December.

Ardizzi, G., E. Bonifacio and L. Painelli (2020), "Payment card fraud: global trends and empirical evidence on online fraud in Italy", Bank of Italy, Occasional Papers, n. 562.

Ardizzi, G. and M. Cologgi (2022), "Business Models and Pricing Strategies in the Market for ATM Withdrawals", Bank of Italy, Markets, Infrastructures and Payment Systems, n. 23.

Baldo, L., E. Bonifacio, M. Brandi, M. Lo Russo, G. Maddaloni, A. Nobili, G. Rocco, G. Sene and M. Valentini (2021), "Inside the black box: tools for understanding cash circulation", Bank of Italy, Markets, Infrastructures and Payment Systems, n. 7.

Chodorow-Reich, G., G. Gopinath, P. Mishra, A. Narayanan (2020), "Cash and the Economy: Evidence from India's Demonetization", The Quarterly Journal of Economics, vol. 135, 1: 57-103.

Cimiotti, G. and T. Merschen (2014), "Trends in consumer payment fraud: A call for consistent strong authentication across all consumer payments", Journal of Payments Strategy & Systems 8.1 (2014): 43-63.

Clogg, C., E. Petkova and A. Haritou (1995), "Statistical methods for comparing regression coefficients between models", American Journal of Sociology, 100 (5), 1261-1293.

Coletti, G., A. Di Iorio, E. Pimpini and G. Rocco (2022), "Report on the payment attitudes of consumers in Italy: results from ECB surveys", Bank of Italy, Markets, Infrastructures and Payment Systems, n. 21.

Distante, C., L. Fineo, L. Mainetti, L. Manco, B. Taccardi and R. Vergallo (2022), "HF-SCA: Hands-Free Strong Customer Authentication Based on a Memory-Guided Attention Mechanisms", Journal of Risk and Financial Management, 15, 342.

Ecommerce Europe and EuroCommerce (2021), "Joint letter on measuring the impact on Strong Customer Authentication in Europe", 30 April 2021.

Euro Banking Association (2020), "Gift cards: a gift for fraudsters? A SMART2 paper on the abuse potential of closed-loop cards".

European Banking Authority (2014), "Guidelines on internet payments security".

European Banking Authority (2020), "Guidelines on fraud reporting under PSD2".

European Banking Authority (2021), "Report on the data provided by Payment Service Providers on their readiness to apply Strong Customer Authentication for e-commerce card based payment transactions".

European Banking Authority (2022), "Discussion Paper on the EBA's preliminary observations on selected payment fraud data under PSD2, as reported by the industry".

European Central Bank (2013), "Recommendations for the security of internet payments. Final version after public consultation".

European Central Bank (2020), "Study on the payment attitudes of consumers in the euro area (SPACE)".

European Central Bank (2021), "Seventh report on card fraud".

European Commission (2012), "Green Paper - Towards an integrated European market for card, internet and mobile payments".

European Commission (2017), Regulation (EU) 2018/389 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication.

European Parliament (2015), Directive 2015/2366 - Payment services in the internal market (PSD2).

European Parliament (2018), Directive 2018/843 - On the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (AML5).

Federal Trade Commission (2021), "Scammers prefer gift cards, but not just any card will do".

Gates, T. and K. Jacob (2009), "Payments fraud: Perception versus reality - a conference summary", Economic Perspectives 33.1: 7-15.

Hayashi, F. (2019), "Payment Card Fraud Rates in the United States Relative to Other Countries since Migrating to Chip Cards", Federal Reserve Bank of Kansas City, Economic Review, vol. 104, n. 4: 23-40.

Hayashi, F. (2020), "Remote Card Payment Fraud: Trends and Measures Taken in Australia, France, and the United Kingdom", Federal Reserve Bank of Kansas City, Payments System Research Briefing.

Hayashi, F., T. Moore and R. Sullivan (2015), "The Economics of Retail Payments Security." Proceedings from the Federal Reserve Bank of Kansas City 2015 International Payments Conference, The Puzzle of Payments Security: Fitting the Pieces Together to Protect the Retail Payments System, Kansas City, MO, June 25-26.

Kahn, C., J. Liñares-Zegarra and J. Stavins (2017), "Are there Social Spillovers in Consumers' Security Assessments of Payment Instruments?", Journal of Financial Services Research 52, 5-34.

Kahn, C. and J. Liñares-Zegarra (2015), "Identity theft and consumer payment choice: Does security really matter?", Journal of Financial Services Research 50.1: 121-159.

Kosse, A. (2013a), "Do newspaper articles on card fraud affect debit card usage?", Journal of Banking & Finance, Elsevier, vol. 37(12), 5382-5391.

Kosse, A. (2013b), "The Safety of Cash and Debit Cards: A Study on the Perception and Behavior of Dutch Consumers", International Journal of Central Banking, vol. 9(4), 77-98, December.

Markiewicz, Z. and R. Sullivan (2017), "Managing Fraud in Remote Payments", Federal Reserve Bank of Kansas City, Payments System Research Briefing: 1-6.

Observatory for the Security of Payment Means (OSMP) of the Bank of France (2021), "Annual Report 2020".

Richardson, G. (2007). "Categories and Causes of Bank Distress During the Great Depression, 1929-1933: The Illiquidity versus Insolvency Debate Revisited," Explorations in Economic History, 44, 588-607.

Schuh, S. and J. Stavins (2015), "How Do Speed and Security Influence Consumers' Payment Behavior?", ECB Working Paper n. 1871.

Stavins, J. (2013), "Security of retail payments: The new strategic objective", Federal Reserve Bank of Boston, Public Policy Discussion Papers, n. 13-9.

UK Finance (2021), "Fraud - The Facts 2021".

United Nations Conference on Trade and Development (UNCTAD) (2021), Global Cyberlaw Tracker.

Appendix

Table 7: Risk of fraud in remote payments with and without SCA (volume)

	Remote SCA	t-statistic	Remote Non SCA	t-statistic	SCA premium	z-score
Domestic						
Cards Issuer	0.074**	(2.571)	0.239***	(5.049)	-0.165***	(-2.978)
E-Money	0.009	(0.606)	0.184***	(5.976)	-0.175***	(-5.119)
Cross-border (within EEA)						
Cards Issuer	0.084**	(2.443)	0.256***	(4.885)	-0.172***	(-2.744)
E-Money	0.054**	(2.355)	0.272***	(5.538)	-0.218***	(-4.022)
Cross-border (outside EEA)						
Cards Issuer	0.119***	(3.069)	0.266***	(4.417)	-0.147**	(-2.052)
E-Money	0.183***	(8.659)	0.321***	(7.239)	-0.138***	(-2.809)
Intermediaries	554		554			
Observations	2,421		2,421			

Notes: *** p <0.01, ** p <0.05, * p <0.1. Estimates based on the number of transactions rather than the value. See notes to Table 5.

Table 8: Impact of SCA on the risk of fraud

	Value	Volume
Domestic		
Cards Issuer	-58%	-69%
E-Money	-81%	-95%
Cross-border (within EEA)		
Cards Issuer	-61%	-67%
E-Money	-77%	-80%
Cross-border (outside EEA)		
Cards Issuer	-52%	-47%
E-Money	-57%	-43%

Notes: Impact of SCA estimated as the percentage change in the elasticity coefficients of SCA and non-SCA remote payments reported in Table 5 and Table 7.

.

Table 9: Risk of fraud in remote payments exempted from the application of SCA (volume)

	Remote SCA	t-statistic	Remote Non SCA (exempted)	t-statistic
Domestic				
Cards Issuer	0.074**	(2.571)	0.059*	(1.926)
E-Money	0.009	(0.606)	0.024	(1.185)
Cross-border (within EEA)				
Cards Issuer	0.084**	(2.443)	0.072**	(2.173)
E-Money	0.054**	(2.355)	0.041	(1.582)
Cross-border (outside EEA)				
Cards Issuer	0.119***	(3.069)	0.077	(0.965)
E-Money	0.183***	(8.659)	0.074	(1.108)
Intermediaries	554		554	
Observations	2,421		2,421	

Notes: *** p <0.01, ** p <0.05, * p <0.1. Estimates based on the number of transactions rather than the value. See notes to Table 5.

Table 10: Fraud rates on domestic and cross-border payments

	2019			2020			2021		
	Domestic	Within EEA	Outside EEA	Domestic	Within EEA	Outside EEA	Domestic	Within EEA	Outside EEA
Overall	0.002%	0.010%	0.028%	0.005%	0.011%	0.021%	0.003%	0.006%	0.013%
Non Electronic	0.003%	0.007%	0.028%	0.009%	0.005%	0.018%	0.007%	0.001%	0.006%
Electronic	0.002%	0.012%	0.028%	0.002%	0.014%	0.022%	0.002%	0.008%	0.015%
SCA Remote	0.001%	0.003%	0.007%	0.002%	0.007%	0.006%	0.002%	0.005%	0.005%
Non SCA Remote	0.004%	0.058%	0.110%	0.003%	0.030%	0.090%	0.001%	0.023%	0.084%
SCA Non Remote	0.002%	0.018%	0.065%	0.002%	0.030%	0.025%	0.003%	0.018%	0.034%
Non SCA Non Remote	0.003%	0.005%	0.045%	0.005%	0.008%	0.059%	0.005%	0.005%	0.025%

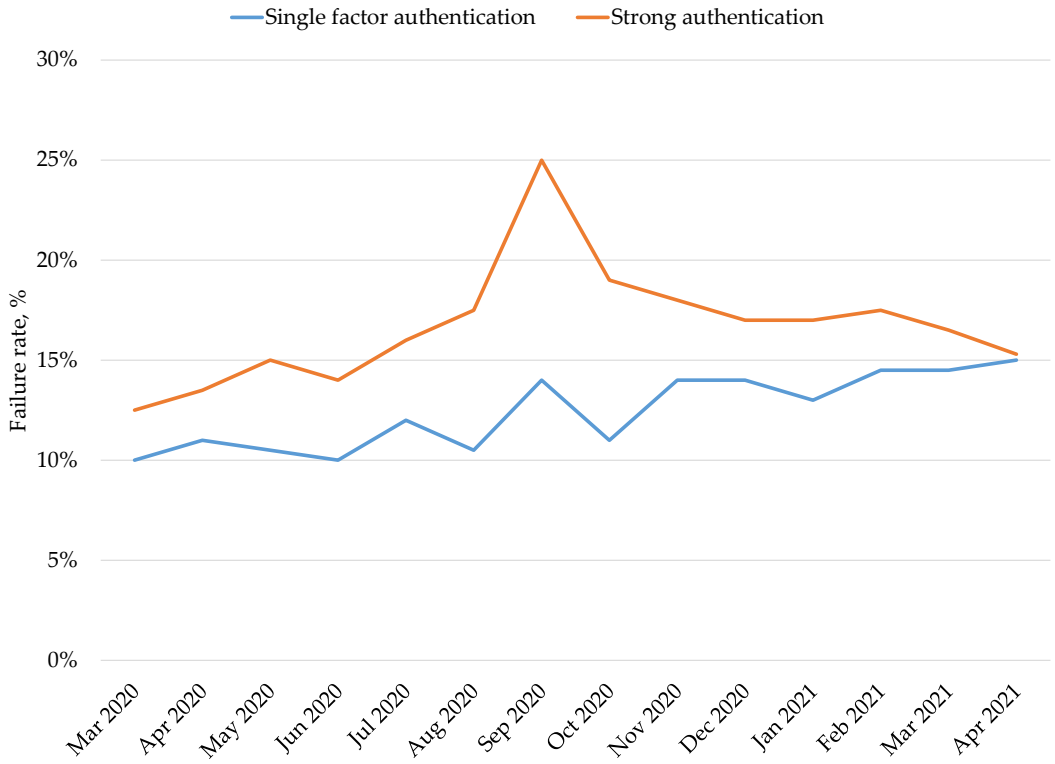
Notes: calculations based on EBA Fraud Reporting data (see notes to Table 1). Fraud rate calculated as the ratio between the value of fraudulent transactions and the total value of transactions carried out using all instruments subject to EBA Fraud Reporting (data for 2019 refer to the second semester). EEA stands for European Economic Area.

Table 11: Counterfactual policy exercise on the savings from SCA in terms of less fraud

				31/12/2019 [A]	30/06/2020 [B]	31/12/2020 [C]	30/06/2021 [D]	31/12/2021 [E]	Overall [F]
[1]	Remote transactions	See note	€ mln	24,146	25,369	30,141	31,792	35,559	147,008
[2]	*SCA Remote*	See note	€ mln	2,572	2,698	6,121	12,266	16,563	40,219
[3]	*Non SCA Remote*	See note	€ mln	21,575	22,672	24,020	19,527	18,996	106,789
[4]	Share SCA	[2]/[1]	%	11%	11%	20%	39%	47%	27%
	Frauds								
[5]	Fraud on remote transactions	See note	€ mln	43	45	42	33	37	201
[6]	Fraud rate	[5]/[1]	%	0.179%	0.178%	0.140%	0.105%	0.105%	0.137%
	Counterfactual analysis								
[7]	Fraud rate	[6][A]	%	0.179%	0.179%	0.179%	0.179%	0.179%	0.179%
[8]	Fraud on remote transactions	[7]x[1]	€ mln	43	46	54	57	64	264
[9]	Benefits from SCA	[8][F]-[5][F]	€ mln						63

Notes: calculations based on EBA Fraud Reporting data on remote transactions carried out with cards (issuing) and e-money. See section 6.

Figure 9: Failure rate of transactions by authentication mode



Source: OSMP (2021).

Papers published in the 'Markets, Infrastructures, Payment Systems' series

n. 1 TIPS - TARGET Instant Payment Settlement – The Pan-European Infrastructure for the Settlement of Instant Paymentsi, *by Massimiliano Renzetti, Serena Bernardini, Giuseppe Marino, Luca Mibelli, Laura Ricciardi and Giovanni M. Sabelli* (Institutional Issues)

n. 2 Real-Time Gross Settlement systems: breaking the wall of scalability and high availability, *by Mauro Arcese, Domenico Di Giulio and Vitangelo Lasorella* (Research Papers)

n. 3 Green Bonds: the Sovereign Issuers' Perspective, *by Raffaele Doronzo, Vittorio Siracusa and Stefano Antonelli* (Research Papers)

n. 4 T2S - TARGET2-Securities – The pan-European platform for the settlement of securities in central bank money, *by Cristina Mastropasqua, Alessandro Intonti, Michael Jennings, Clara Mandolini, Massimo Maniero, Stefano Vespucci and Diego Toma* (Institutional Issues)

n. 5 The carbon footprint of the Target Instant Payment Settlement (TIPS) system: a comparative analysis with Bitcoin and other infrastructures, *by Pietro Tiberi* (Research Papers)

n. 6 Proposal for a common categorisation of IT incidents, *by Autorité de Contrôle Prudentiel et de Résolution, Banca d'Italia, Commissione Nazionale per le Società e la Borsa, Deutsche Bundesbank, European Central Bank, Federal Reserve Board, Financial Conduct Authority, Ministero dell'Economia e delle Finanze, Prudential Regulation Authority, U.S. Treasury* (Institutional Issues)

n. 7 Inside the black box: tools for understanding cash circulation, *by Luca Baldo, Elisa Bonifacio, Marco Brandi, Michelina Lo Russo, Gianluca Maddaloni, Andrea Nobili, Giorgia Rocco, Gabriele Sene and Massimo Valentini* (Research Papers)

n. 8 The impact of the pandemic on the use of payment instruments in Italy, *by Guerino Ardizzi, Alessandro Gambini, Andrea Nobili, Emanuele Pimpini and Giorgia Rocco* (Research Papers) (in Italian)

n. 9 TARGET2 – The European system for large-value payments settlement, *by Paolo Bramini, Matteo Coletti, Francesco Di Stasio, Pierfrancesco Molina, Vittorio Schina and Massimo Valentini* (Institutional Issues) (in Italian)

n. 10 A digital euro: a contribution to the discussion on technical design choices, *by Emanuele Urbinati, Alessia Belsito, Daniele Cani, Angela Caporrini, Marco Capotosto, Simone Folino, Giuseppe Galano, Giancarlo Goretti, Gabriele Marcelli, Pietro Tiberi and Alessia Vita* (Institutional Issues)

n. 11 From SMP to PEPP: a further look at the risk endogeneity of the Central Bank, *by Marco Fruzzetti, Giulio Gariano, Gerardo Palazzo and Antonio Scalia* (Research Papers)

n. 12 TLTROs and collateral availability in Italy, *by Annino Agnes, Paola Antilici and Gianluca Mosconi* (Research Papers) (in Italian)

n. 13 Overview of central banks' in-house credit assessment systems in the euro area, by L*aura Auria, Markus Bingmer, Carlos Mateo Caicedo Graciano, Clémence Charavel, Sergio Gavilá, Alessandra Iannamorelli, Aviram Levy, Alfredo Maldonado, Florian Resch, Anna Maria Rossi and Stephan Sauer* (Institutional Issues)

n. 14 The strategic allocation and sustainability of central banks' investment, by *Davide Di Zio, Marco Fanari, Simone Letta, Tommaso Perez and Giovanni Secondin* (Research Papers) (in Italian)

n. 15 Climate and environmental risks: measuring the exposure of investments, by *Ivan Faiella*, *Enrico Bernardini*, *Johnny Di Giampaolo*, *Marco Fruzzetti*, *Simone Letta, Raffaele Loffredo and Davide Nasti* (Research Papers)

n. 16 Cross-Currency Settlement of Instant Payments in a Multi-Currency Clearing and Settlement Mechanism, by *Massimiliano Renzetti*, *Fabrizio Dinacci and Ann Börestam* (Research Papers)

n. 17 What's ahead for euro money market benchmarks?, by *Daniela Della Gatta* (Institutional Issues) (in Italian)

n. 18 Cyber resilience per la continuità di servizio del sistema finanziario, by Boris Giannetto and Antonino Fazio (Institutional Issues) (in Italian)

n. 19 Cross-Currency Settlement of Instant Payments in a Cross-Platform Context: a Proof of Concept, *by Massimiliano Renzetti, Andrea Dimartina, Riccardo Mancini, Giovanni Sabelli, Francesco Di Stasio, Carlo Palmers, Faisal Alhijawi, Erol Kaya, Christophe Piccarelle, Stuart Butler, Jwallant Vasani, Giancarlo Esposito, Alberto Tiberino and Manfredi Caracausi* (Research Papers)

n. 20 Flash crashes on sovereign bond markets – EU evidence, *by Antoine Bouveret, Martin Haferkorn, Gaetano Marseglia and Onofrio Panzarino* (Research Papers)

n. 21 Report on the payment attitudes of consumers in Italy: results from ECB surveys, *by Gabriele Coletti, Alberto Di Iorio, Emanuele Pimpini and Giorgia Rocco* (Institutional Issues)

n. 22 When financial innovation and sustainable finance meet: Sustainability-Linked Bonds, *by Paola Antilici, Gianluca Mosconi and Luigi Russo* (Institutional Issues) (in Italian)

n. 23 Business models and pricing strategies in the market for ATM withdrawals, *by Guerino Ardizzi and Massimiliano Cologgi* (Research Papers)

n. 24 Press news and social media in credit risk assessment: the experience of Banca d'Italia's In-house Credit Assessment System, *by Giulio Gariano and Gianluca Viggiano* (Research Papers)

n. 25 The bonfire of banknotes, *by Michele Manna* (Research Papers)

n. 26 Integrating DLTs with market infrastructures: analysis and proof-of-concept for secure DvP between TIPS and DLT platforms, *by Rosario La Rocca, Riccardo Mancini, Marco Benedetti, Matteo Caruso, Stefano Cossu, Giuseppe Galano, Simone Mancini, Gabriele Marcelli, Piero Martella, Matteo Nardelli and Ciro Oliviero* (Research Papers)

n. 27 Statistical and forecasting use of electronic payment transactions: collaboration between Bank of Italy and Istat, *by Guerino Ardizzi and Alessandra Righi* (Institutional Issues) (in Italian)

n. 28 TIPS: a zero-downtime platform powered by automation, by *Gianluca Caricato, Marco Capotosto, Silvio Orsini and Pietro Tiberi* (Research Papers)

n. 29 TARGET2 analytical tools for regulatory compliance, by *Marc Glowka, Alexander Müller, Livia Polo Friz, Sara Testi, Massimo Valentini and Stefano Vespucci* (Institutional Issues)