Joint ECB-BI conference, Roma, 30 November and 1 December 2017

INNOVATION IN CUSTOMER AUTHENTICATION METHODS, CARD-BASED INTERNET PAYMENTS AND USER EXPERIENCE: EMPIRICAL EVIDENCE FROM ITALY

by Guerino Ardizzi*

Abstract

The present study moves from the consideration that every payment innovation should strike the right balance between security and a positive user-experience. However very few empirical studies assess the impact of innovative authentication methods on the e-commerce turnover. This paper constitutes the first attempt to provide an econometric assessment of the impact of a security innovation (such as 3D Secure) to card-based internet payments by relying on semi-annual Italian banking panel data over the period 2012-2016. Econometric results show that multiple-factor authentication methods may have negative effects on user-experience (expressed in terms of card turnover). Such outcome could implicitly suggest to preserve a flexible approach in security innovation and to combine the launch of new authentication methods with adequate educational programs, as acknowledged also by regulators.

JEL Classification: C23, C33, D04, D12, E21, K23

Keywords: Internet payments, credit cards, SCA, user experience, security, e-commerce, two-factor authentication, banking panel data.

Contents

This version, December 1, 2017

* Banca d'Italia, Market and Payment System Oversight. The authors would like to thank, for their useful remarks, Paola Giucca, Monika Hartmann, Costanza Iacomini, Michael Salmony, Ravenio Parrini and Michele Savini Zangrandi. The views expressed in the article are those of the author and do not involve the responsibility of the Bank.

1. Introduction

The way we pay is changing with the digital transformation of the retail payments ecosystem and the increasing authentication possibilities that allow payment service providers (PSP) to verify a customer's identity. The present study moves from the consideration that every payment innovation is to strike the right balance between security and a positive user-experience and that very few empirical studies assess the impact of innovative authentication methods[1] on the e-commerce turnover.

In this field, one of the main objectives of the PSD2 – entered into force in January 2016 - consists of a general enhancement of the levels of security for electronic payment services, in order to increase consumer protection and foster innovation in the retail payments market. To achieve this goal, the Directive confers on the EBA the mandate to deliver, in close cooperation with the ECB, regulatory technical standards (RTS) on "strong customer authentication" (SCA). These RTS will apply from 18 months after their entry into force (approximately end-2018). These security measures should ensure that payment services offered electronically be carried out in a secure manner, adopting technologies able to guarantee the safe authentication of the user and reduce, to the maximum extent possible, the risk of fraud, in particular, through the application of SCA to payments as a rule. In developing the RTS, the EBA had to manage trade-offs between competing demands, in particular between ensuring a high degree of security and fostering innovation and the easy use of electronic payment instruments.

To this purpose, while PSD2 introduces the obligation for payment services providers to apply strong customer authentication for remote electronic payments (including card-based internet payments), it also acknowledges the benefit of allowing the development of user-friendly and accessible means of payment. The idea of providing exemptions from the requirement of strong customer authentication, is to ensure the possibility of making payment initiation easier for users (positive user-experience). The underlying assumption being that strong customer authentication could create a slower payment initiation.

[1] "Authentication" is a procedure that allows the PSP to verify a customer's identity. The procedure is considered "strong" if it requires the user to provide more than one authentication factor to improve security.

This issue has been already tackled by the EBA Guidelines on the security of internet payments requiring strong customer authentication for internet payments[2]. These guidelines also apply to card issuing and acquiring PSPs via their adoption in the EU members from 2016 and provide for the implementation of a transaction risk analysis as an alternative authentication method to evaluate the risks related to a specific transaction, taking into account criteria such as, for example, customer payment patterns (behaviour).

Having said that, the aim of this paper is to contribute to the lack of empirical analysis on the relationship between the innovation in authentication methods and the user adoption of digital payment instruments and to address an important issue in terms of policy implications: if the massive adoption of strong customer authentication (SCA) has a negative impact on user experience, the new legal framework should allow for alternative authentication methods or exemptions based on transaction risk analysis (i.e. below a specific monetary threshold for e-commerce transactions).

In Section 2 a brief review of the available literature on the subject is exposed. In Sections 3 and 4 we show in more detail the market trend of card-based internet payments in Italy and the database used in this work. Section 5 illustrates the model of analysis and the econometric approach, aimed to verifying the relationship between user-experience and security innovation in Internet payments. The results are discussed in Section 6, while the conclusions and some policy indications are reported in Section 7.

2. Literature

The theoretical and empirical literature has addressed the issue of the security innovation and consumer behaviours in economic and financial sectors. In the field of payment systems some researchers find that consumers' payment preferences are strongly affected by their perceptions of safety when using payment instruments (see Kosse 2013;

[2] ECB (2013), page. 3: "Strong customer authentication is a procedure based on the use of two or more of the following elements – categorised as knowledge, ownership and inherence: i) something only the user knows, e.g. static password, code, personal identification number; ii) something only the user possesses, e.g. token, smart card, mobile phone; iii) something the user is, e.g. biometric characteristic, such as a fingerprint. In addition, the elements selected must be mutually independent, i.e. the breach of one does not compromise the other(s). At least one of the elements should be non-reusable and non-replicable (except for inherence), and not capable of being surreptitiously stolen via the internet".

Hayashi et al. 2015) or mobile technologies to access financial services (Fed 2015). Such studies note that security concerns are a main impediment to the confidence and adoption of digital services and confirm the need for promoting security technologies for customer authentication. However, even though payment security is important to customers, some other researchers find that improving security of payments is unlikely to change customers' payment behaviour significantly (Schuh and Stavins 2015).

At the same time, user experience can suffer as digital products become more secure. Nevertheless, the empirical analyses of the usability of security technologies in payment systems are scarce.

Braz and Robert (2006) were among the first to investigate the usability of safety innovations, showing from a qualitative point of view that multiple-factor authentication[3] methods strengthens security but reduces usability of electronic applications. More recently, Krol et al (2015) conducted a diary survey by recruiting 21 actual customers that had been using 2FA in the context of UK online banking. The outcome shows that participants' satisfaction is negatively correlated with the use of hardware tokens as well as with the need to provide multiple credentials. Key targets for improvements are (i) the reduction in the number of authentication steps, and (ii) removing features that do not add any security but negatively affect the user experience. However, such investigations are based on small samples and self-reported data, with a selection bias that may strongly reduce the statistical significance of the results.

Other studies conducted by consulting firms remark the issue of consumer experience and safety of technology in the field of payment networks. For instance, a report conducted by Adyen (2014) shows how applying 3D Secure to all card transactions over the Internet can positively or negatively impact conversion rates on a per-country basis, and that a more flexible implementation of the 2FA methods may increase sales for merchants and at the same time mitigate fraud risks. More recently, a PayPal investigation on the application of 3DS on e- and m-commerce transactions in 2016 demonstrates that, on average, an additional 40% of transactions were abandoned following the introduction of 3DS in

[3] Multi-factor authentication has emerged as an alternative way to improve security bu requiring the user to provide more than one authentication factor, as opposed to only a password (De Cristofaro et. Al 2014).

Europe[4]. However, it is not possible to assess the methodology adopted in such investigations, which reflect the specific point of view of the stakeholder and have not been published in detail on scientific journals.

****

As far as we are aware, our paper constitutes the first attempt to provide an econometric assessment of the impact of a (multi-factor) security payment innovation (such as 3D Secure) to e-commerce by relying on representative macro-banking data. This reduces the sample selection bias problems, typical of the micro-data surveys. Moreover, our approach considers actual payment systems' data, which show suitable features to track economic activity and consumer behaviours in the digital ecosystem (Kosse 2013, Aprigliano et al. 2017).

3. Card-based Internet payments

The use of payment cards for Internet payments has increased significantly in Italy, as elsewhere in the world, over the years, in parallel to the structural trend in the e-commerce[5]. E-commerce diffusion is part of the Digital Single Market strategy in Europe, ensuring better access for consumers and businesses to goods and services across the EU, increasing price transparency and price competition, having positive impacts on companies' distribution strategies, consumer behaviours, economic activities.

Card based products are the most frequently used electronic payment instruments over the Internet, also thanks to the popularity of mobile technologies (such as tablets and smartphones) and the versatile manner to expand the possibility of card payments for online shopping by means of digital applications or software solutions.

[4] See Paypal reply to the written consultation on the EBA regulatory technical standards on SCA (https://www.eba.europa.eu/councilregulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2). EBA (2016)

[5] E-commerce in the EU has grown steadily in recent years. EU is one of the largest e-commerce markets in the world. The percentage of people aged between 16 and 74 that have ordered goods or services over the internet has grown year-on-year from 30 % in 2007 to 55 % in 2016 (See EC, Sector Inquiry 2016).

The number of e-commerce transactions in Italy using prepaid or credit cards[6] has grown yearly by [20] per cent in the period 2011-2016 and last year around 400 million card transactions have been made over the Internet. The rate of "remote" transactions growth is four times higher than that of "face-to-face" transactions. Figure 1 reports the evolution of the percentage composition of card-based internet payments in Italy with respect to credit and prepaid cards. Credit cards are more mature products than prepaid ones, and have experimented first the development of new security technology for card-not-present payments[7] (such as 3D Secure or 3DS). So we can derive interesting information from evaluating credit card performances over the last years[8].

Figure 2 reports the more recent dynamics of online credit card transactions in Italy and the 3DS adoption rate, calculated as a percentage of "secure electronic commerce transactions", which designates a transaction between a cardholder and a merchant performed via the Internet where the transaction was successfully authenticated through the 3D secure protocols (statistics are recorded on the issuing side). With regards to the e-commerce turnover, data on the total number of online credit card transactions (and transactions per card) confirm a positive trend over the last five years. Moreover, at the end of 2016 over 60 percent of online credit card transactions were authenticated via the 3DS Secure protocol in Italy[9] but we can see a steady increasing trend after 2014, in line with the international recommendations promoting the adoption of two-factor authentication methods for remote payments.

However, although 3D Secure is adopted throughout the world, it is more widely-used in some countries than others. In 2014, an ad hoc survey (Ingenico PS, 2014) released the results of a study of 3DS usage across a number of European countries[10]. The rates of

[6] Internet payments with debit cards remain embryonic in Italy.

[7] Although pre-paid card solutions have rapidly grown over the years, around 41 percent of online purchases are still made with traditional credit cards in Italy.

[8] As regards prepaid cards in Italy, the 3D Secure protocol has been actually adopted after 2014. However, we have no statistics on the "3-D" rate of adoption for prepaid payments over the internet.

[9] This statistics seems to be in line with the only one available from other countries (See Adyen (2014).

[10] Moreover, 3-D Secure can rely on different options for generating the OTP (one-time password) for authentication purpose, such as hardware tokens, sms or mobile phone applications. In some countries 3DS functionality isn't reliable on mobile devices and conversion rates are likely to suffer significantly if a large share of transactions are made on mobile phones.

successfully authenticated transactions within these countries vary from 17% up to 82%. To this purpose, in the past, merchant participation in 3DS was usually not mandatory, but merchants that implemented the program could benefit from a significant liability shift, as they were no longer responsible for fraud-related chargebacks; instead these would become the responsibility of the issuing bank (and not of the cardholder who is usually protected by the payment service legislation). Despite this strong incentive for end-users, adoption of 3DS services since its inceptions in the early 2000's has been much slower than expected (Ecommerce Europe, 2015). However, after the entry into force of the EBA-ECB Recommendations on security for internet payments (2016) and, especially in the near future with the implementation of the mandatory EBA rules on strong customer authentication methods in 2018, it is expected that the adoption of a compatible version[11] of 3DS protocol will significantly increase across all European countries.

Lastly, with regards to providing a complete picture of the card-based internet payments, it should be noted that the value of card-not-present (CNP)[12] frauds on cards issued inside Europe significantly increased over the years and that such frauds still account for the majority of the total fraud losses on cards (ECB Card Fraud Report). Also in Italy (see Figure 3), after chip-EMV diffusion, the card present fraud rate[13] (at POS and ATM) has been declining, while the CNP fraud rate has grown over the years. However, in this paper we do not conduct an exercise to evaluate the impact of security technology on the level of frauds, which is a relevant topic for further researches.

By using the available information contained in the panel dataset described below, we are more interested here in evaluating the impact of the massive diffusion of stronger authentication methods on the e-commerce turnover

4. Dataset

[11] A compatible version with PSD2-EBA requirements means that the PSP must apply strong (multi-factor) customer authentication that includes "elements which dynamically link the transaction to a specific amount and specific payee" .

[12] Remote payments via the internet, post or telephone order.

[13] We consider the amount of the frauds related to a specific payment instrument???, divided by the gross amount of the total card transactions (the so-called card fraud loss rate) as a synthetic indicator of riskiness of that instrument.

In this work we use semi-annual data drawn from the reports of the credit card institutions (banks and other payment service providers) collected by the Bank of Italy from each reporting body on cumulative and anonymous basis. The available information allows us to construct an unbalanced panel data over the period 2011H1 – 2016H2, which includes around 50 payment service providers representative of 80 percent of the credit card-based Internet payments sector ranging from 221 to 376 observations[14]. The data encompass information about: number of credit cards in circulation, share of cards used over the Internet, total volume of credit card transaction (of which: Internet transactions), volume of "3D-Secure" based transactions, other 'control variables' (such as bank size and type of business model[15]). See Table 1 and 1B for definitions, descriptive statistics, and information about the data sources for the whole sample. Individual data on "3D-Secure" are not balanced for all types of payment service providers during the period: bank statistics are reported from 2014, while other payment service providers (credit card companies) report the volume of "secured" transactions from 2011. Figure 4 and 5 show the empirical distribution of the 3-D Secure rate and credit card Internet turnover, respectively.

5. Model of analysis

As a case study, we assess the impact of the so called "3D Secure" protocol (which involves a two-factor authentication method[16]) on the use of card-based payment instruments over the Internet (e- and m-commerce). 3D Secure is already adopted by the industry as communication protocol linking the e-merchant, the acquiring PSP and the issuing PSP. Following a request by the e-merchant's server, the cardholder's PSP is contacted in order to authenticate the cardholder, approve the terms of the transaction,

[14] In some case, we can have gaps in the panel depending on the availability of the data. However we have excluded the banks that have missing values as well as those who do not report all the relevant data (e.g transactions, number of cards issued) in both reference periods.

[15] Business models are mainly detected by institutional dummy variables (i.e. bank or credit institutions), by the individual share of cross-border payments, and by the share of prepaid payments.

[16] The two-factor approach allows for stronger authentication and aims to enhance resilience of the cardholder identification by requiring users to provide an additional authentication factor , e.g. a code generated by a security token or sms or other technologies, in addition to the typical credit card number o CVV code. In general, multi-factor authentication methods are usually of three kinds: 1) knowledge (something the user knows, e.g., a password; 2) possession (something the user has, e.g. a security token (also known as hardware token); 3) inherence (something the user is, e.g., a biometric characteristic. See ECB (2013), Recommendations for the security of internet payments.

notably the amount, and prepare a record or certificate as evidence of the transaction. Where the e-merchant is 3-D Secure compliant – i.e. the issuer provides a solution for additional customer authentication – the customer will be directed, via the 3-D Secure Directory, to the issuer's authentication server. Note that the customer must have been enrolled by the issuer (enrolment verification) and informed about the authentication procedure prior to the first authenticated payment transaction. A separate window will open where the customer is asked to enter his password, which is subsequently verified by the issuer. The level of security offered by the password depends on the nature of the password required by the service, i.e. static or dynamic. Dynamic passwords provide stronger authentication. In this case, 3-D Secure will generate a "one-time password" (OTP) for authentication purposes with different options (such as hardware tokens, SMS or mobile phone applications). Once the cardholder has been authenticated, the e-merchant is informed via its acquirer. The e-merchant then sends the issuer an authorization request, incorporating the digital proof of successful cardholder authentication, after which the issuer finally authorizes the transaction. Once the e-merchant has received the final authorization message, the transaction can be finalized. This authentication solution provides additional security, and the use of the service results in a shift of liability in the event of fraud. However, 3D Secure authentication methods introduce additional steps in the payment workflows which can impact the user experience, as discussed previously. Whilst 3D Secure payments have been around for a while it is only recently that the card payment schemes are enforcing the implementation of this technology, taking into account also the new regulatory framework enhancing customer authentication methods which rely on the multi-factor approach.

By relying on an the panel dataset described in par. 4, we estimate the impact on card-based internet turnover caused by the 3D Secure adoption on the use of payment card over the internet. The exercise is carried out regardless of the option used to initiate the payment (via mobile phone, PC, Tablet etc.), to generate the password (i.e. token based or SMS-based) and the type of authentication (i.e. dynamic or static). The respective information is not available. However, we have determined that the collective data allow us to assess the customer experience in general.

We adopt a simple equation model to test the effect on the turnover per card (dependent variable) of the share of transaction between a cardholder and a merchant via the

Internet where the transaction was successfully authenticated via 3D Secure (explanatory variable). Thus it is determined that the turnover per card represents a proxy of the user-experience.

One can then assume a relationship between the Internet card turnover, the 3D Secure adoption and other control variables *Z*, with conditionally independent errors $E(\varepsilon_{it}|Z_{it}, 3DSecure_{it}) = 0$, *i* banks and *t* periods, and run a regression model like the following Equation:

$$TURNOVER_{it} = \alpha_0 + a_1 Secure_{it} + \sum_h \alpha_h Z_{it} + u_{it} \qquad [5.1]$$

The dependent variable (TURNOVER) is equal to the value of transactions per card that are completed over the Internet. The first variable in the right-hand side of equation *Secure* is equal to the percentage of the 3DS transaction. Its coefficient aims to capture the effect of the two-factor authentication method to the internet purchases of the same cards issued by the bank. In other words, we verify whether an increase in the level of 3DS adoption gives less rise – on average – to the Internet payments.

The summation term among the covariates in the Equation above indicates the set of h environmental variables (Z), and that of the relative coefficients, which can influence the use of card-based internet payments. Control variables identifies size, share of internet payments, alternative payment methods, network size (i.e. number of card active over Internet), PSP type (market share, business model, non-bank operators) which may affect the choice of using Internet payments.

An alternative specification considers as dependent variable the share of credit cards on total cards which has been activated online for Internet payments, as follows:

$$CARDONL_{it} = \alpha_0 + a_1 Secure_{it} + \sum_h \alpha_h Z_{it} + u_{it} \qquad [5.2]$$

Such alternative model allows us to evaluate the impact of two-factor 3D Secure technology to the propensity to use the card at least once in the reference period[17].

6. Estimation of the model

The parameters of Equation [5.1]-[5.2] were estimated using the panel data described in par. 4.

Several methods have been proposed for the estimation of panel data models with a large number of cross-sectional units observed over a rather long period of time (in our case, N = 58 payment service providers and T = 9 semesters). The estimated values of the static coefficients in equation (1) can be obtained by classic panel model estimators with fixed, random, between effects and by the standard (pooled) least squares (OLS) estimator.

Our baseline model is a standard panel model with “fixed effects” as the Hausman test strongly rejects the hypothesis of “random effects”, while the Breusch-Pagan test refuses that of "poolability" (cross-sectional model instead of panel model). First of all we estimate the base model, which considers only the percentage “3D-secure transactions” (Secure) and the time dummy variable among the covariates[18]. Then we include the other control variables in the full model[19] and test the stability of the results with respect to the disturbances affecting the base model. As a further specification, we also added a lagged dependent variable among covariates[20], to incorporate a temporal dependency of the y-

[17] Such specification consider a panel data with several gaps (around 40 banks and 200 observations), as such data are not always available for the entire period and for all the reporting institutions.

[18] A time dummy variable may be useful to take into account the effect of the business cycle influences or technological changes. We consider year dummies, which are preferred to six-monthly dummies to maintain the specification parsimonious, and a semester dummy in order to capture seasonality in the data, and a number of variables that attempt to capture broader market trends.

[19] The full model includes a set of institutional (1. commercial banks, 2. Credit card companies); size dimension and business specific variables (market share, percentage of online active credit cards, percentage of internet card-based payments, share of cross-border transactions).

[20] As Greene (2012) asserts, adding dynamics creates a major change in the interpretation of the equation. Without the lagged variable, the “independent variables” represent the full set of information that produce observed outcome y-variable. With the lagged variable, we now have in the equation the entire history of the right-hand-side variables, so that any measured influence is conditional on this history; in this case, any impact of the independent variables represents the effect of new information. Thus, in a dynamic panel model, the ‘independent variables’ only reflect new or contemporaneous information conditional both on the other controls and the lagged dependent variable, which itself represents the history of the model (i.e. the past).

variable, even if the unobserved panel-level effects are correlated with the lagged dependent variables, making standard estimators less consistent (see below par. 6.2 for appropriate dynamic panel data estimations).

6.1. Results

The results of the estimates are shown in Table 2. As expected, the coefficient of the degree of migration to 3D Secure (3DS) shows a negative and significant sign. This is true also after controlling for environmental variables Z, whose coefficients are not reported for the sake of brevity[21]. The magnitude of the effect, however, is significant: on average, an increase of 100 basis points of the number of "secure" internet payments is associated with a reduction in the card turnover in the order of 0.3 percent[22].

This is true even if we replicate the regression exercise considering the alternative dependent variable to measure the use of card over Internet as in Eq. 5.2[23]. In this case the magnitude of the effect is in the order of -0.1 percent.

Table 3 follows the structure set out in Eq. 5.2 and estimation results confirm the negative impact, on average, of the 3DS secure rate on the level of adoption of credit cards over the Internet.

---

[21] The full model shows a positive and significant correlation between credit card turnover and market power (expressed in terms of individual concentration index); moreover, as expected, there is a negative (and significant) correlation between credit card turnover and the share of prepaid cards ("substitution good") issued by the same institutions. With regards to the other control variables, the institutional factor dummies (bank vs. non-bank institution) as well as the share of cross-border card transactions, are not always significant across the different methods; hence we do not report specific comments here. Moreover, main results are robust calculating the collective information of the intermediaries who belong to the same banking group, in order to control for possible "group" specific effects. For the sake of brevity, we do not present the results of these tests, but they are available on request from the author.

[22] Since the dependent variable is logarithmic, the regression coefficients beta must be interpreted as a one unit change in the regressor X (expressed as a percentage) and associated with a percentage change in Y according to this formula: $\%\Delta y=(e^{\beta} - 1)$. Our results seem to be in line with other studies (see Adyen 2015) focused on assessing the impact of 3DS authentication on conversion reports, which state that in many of the countries assessed abandonment rates are well over 25%, with the USA at 44%, China at 47% and Brazil at 55%.

6.2. Robustness

The specification may suffer from issues of serial correlation in the errors, omitted variables and endogeneity problem. Dynamic panel estimators are purpose-designed to deal with this issues (Bond, 2002). We therefore adopt also a GMM approach including lags of the dependent variable as well as the fixed effect approach to address the GMM-style instrumentation. We always include time dummies to make the assumption of no correlation across individuals in the idiosyncratic disturbances more likely to hold (Roodman 2009). GMM-style instrumentation can quickly generate a large number of instrument, causing problems of invertibility in the instrument matrix. In the case of Eq. 5.2, with a smaller database (complete statistics on active cards are recorded only by 2014), we are more careful to avoid the use of a generalized inverse (and its related issues) by considering the GMM-diff [24] (first difference equations), limiting the number of lags included and collapsing the instruments (Roodman, 2009). The size dimension of the panel data (number of observations) varies across different models depending on the availability of data for each covariate and instrumental variable included in the estimation. To this purpose we use orthogonal deviations in panels with caps to maximizes sample size as suggested by Roodman in "How to use xtabond2" (2009).

The estimation checks in Table 4 and 5 seem to be more than satisfactory. Columns (1) to (2) report the two-step GMM results in order to control for potential serial correlation in the errors. Column (3) reports the fixed-effects estimation with the lagged y-variable among covariates.

The GMM specifications include lagged y-variable, 3D-S rates and other lagged control variables as GMM-style (Table 5) and GMM-diff (Table 6) instruments[25]. GMM instruments are collapsed in order to avoid too-many-instruments-type problems. Dummy

---

[23] We remark that such estimation considers a panel data with more gaps (around 42 banks and 220 observations) as data on active cards are not always available for the entire period and for all the reporting institutions.

[24]Moreover, the GMM-diff model does not require the assumption that - in a panel with fixed effects including the equation in levels - the first-differenced instruments used for the variables in levels should note be correlated with the unobserved country effects.

[25] As already remarked, in case of "CARDONL" model estimation we use a smaller dataset; hence, we adopt the diff-GMM estimator, as the GMM-style instrumentation generate a larger number of instruments causing problems of invertibility in the instrument matrix and may be inappropriate (Roodman, 2005).

variables (time and institutional ones) are considered exogenous. Variables measuring market power and overall market trend, conversely, are also considered exogenous as no intermediary is sufficiently large to single-handedly affect market-wide outcomes. The Hansen and Sargan test shows instrument validity for both GMM specifications.

Across all of the methods adopted, the significance and the intensity (negative) of the 3D-Secure effect on the use of card for Internet payments (*TURNOVER*; *CARDONL*) are confirmed. As an additional check we also replicate all the estimations by using the strongly balanced panel dataset[26].

Finally we perform an indirect test of robustness, by changing the dependent variable in the eq. 5.1- (credit card turnover) with its direct substitute (prepaid cards turnover over the Internet). Although statistical data about the 3D Secure adoption on prepaid cards in Italy are not available, we can presume that prepaid cards networks started to migrate to the 3D-Secure protocol after 2015 (in accordance with the new international recommendation on security of internet payments). This was not the case of credit cards, for which 2FA methods started to be promoted and widely adopted in the market before 2015 in Italy (see par. 6). So we estimated the "modified" version of Eq. 5.2 for the panel database in the period 2011 to 2014, with "prepaid card turnover" as dependent variable and maintaining all other explanatory variables already considered in the previous estimations. The related hypothesis to be tested is the following: the higher the 3DS rate implementation on the credit card market, the higher the use of more user-friendly prepaid cards. Table 6 reports the estimates of equation model for the prepaid turnover, through both static and dynamic estimators, which show a positive effect of the "Secure" (credit card) variable on the prepaid turnover (value of prepaid card transaction over the internet per card), which seem to be consistent with the underlying hypothesis even if such effect is significant[27] in the FE specification only (standard and lagged version).

[26] For the sake of brevity, we do not present the results of these tests, but they are available on request from the author

[27] As regard the GMM estimation, the high p value on the Hansen test suggest that this method (and the instrument set) is not valid in this application to test our hypothesis.

7. Conclusion

The issue of the potential trade-off between new security technologies and positive usability of digital payment methods is the focus of growing attention.

Our results from estimating an equation model support the hypothesis of negative effects of a certain two-factor authentication method (such as the 3-D Secure protocol) on the user-experience in the 2012.H1-2016.H2 period. Such outcomes are robust both in static panel data specifications (fixed effect-FE models) and those of dynamic (GMM estimator à la Arellano-Bond).

However, we interpret these results in a dynamic way as well: they just confirm that that user-experience should not be underestimated by the policy maker. This issue has been already tackled by the recent EBA Guidelines on the security of internet payments requiring strong customer authentication for internet payments and, more recently, it is under discussion within the works for the new regulatory framework implementing the PSD2. The idea of allowing exemptions from the requirement on "strong customer authentication" is consistent with the possibility to make payment initiation more user-friendly. To this purpose EBA Guidelines already provide for the implementation of transaction risk analysis as an alternative authentication method to evaluate the risks related to a specific transaction taking into account criteria such as customer payment patterns (behaviours). This approach seems to be also confirmed in the new regulatory framework for internet payments after the PSD2 implementation.

Moreover, there is no one-size-fits-all security technology and service providers can implement different kinds of two-factor authentication methods for e-banking with different levels of usability. For instance, some seminal studies[28] remark that the adoption of biometric techniques (so called "implicit authentication") is considered a more user-friendly way to implement strong customer authentication and to ensure at the same time a high level of security.

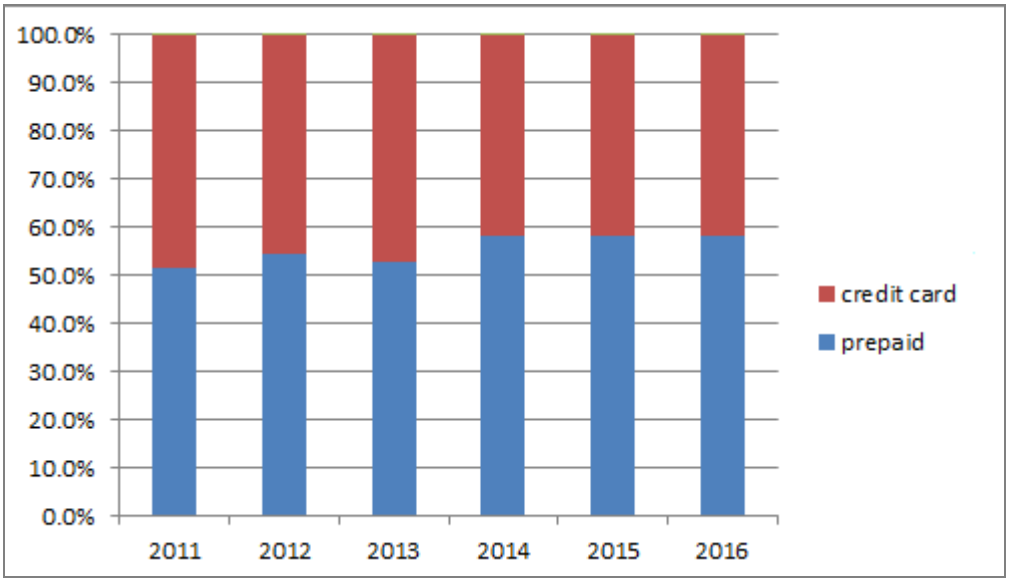
Finally, adequate educational programs for users should also be considered before launching new authentication methods, as acknowledged by regulators. This topic, in the

[28] See Svilar A.- Zupancic J. (2016); Krol et al. (2015).

past, seems to have been overlooked by market operators and probably usability issues related to previous multifactor-factor authentication schemes should have been more carefully evaluated. To this purpose, “customer awareness, education, and communication” is a specific topic also tackled by the EBA Guidelines on the security of internet payments. It appears beneficial to confirm this approach in the new regulatory framework for internet payments after the PSD2 implementation.

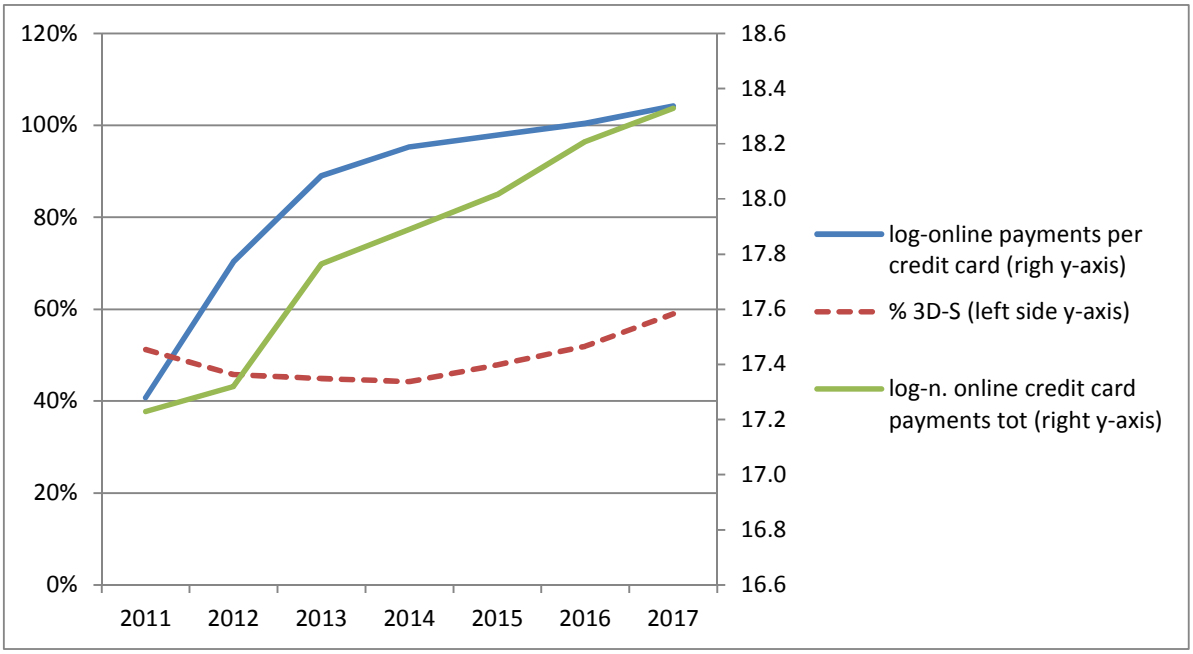
Tables and Figures

Figure 1: Card-based Internet payments, credit vs prepaid: % composition



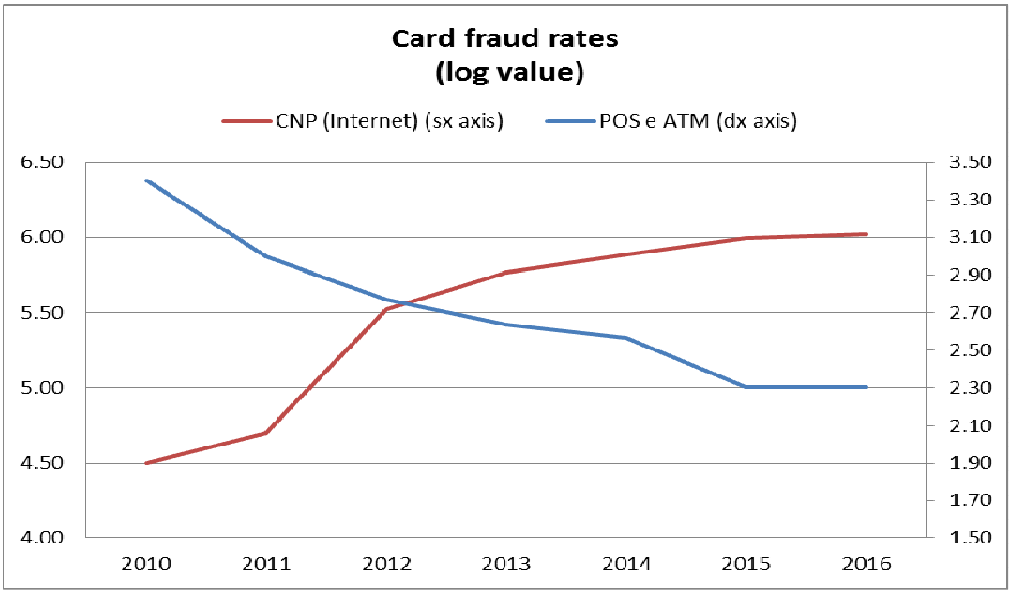
Source: Bank of Italy, banking statistics.

Figure 2: Pattern of the 3D Secure rate (issuing side) and credit card payments in Italy



Source: Bank of Italy, banking statistics

Figure 3: Card fraud rates: CNP vs. CP (ATM & POS):



Source: Bank of Italy, banking statistics

Table 1A: Panel dataset - descriptive statistics of main variables

Variable		mean	Std. Dev.	Min	Max	Observations		
ln TURNOVER (value)	overall	5.47	2.16	-1.08	11.86	N	=	383.00
	between		2.08	-0.71	11.76	N	=	58.00
	within		0.56	3.40	8.67	N	=	6.60
ln TURNOVER (volume)	overall	1.42	1.41	-4.65	6.46	N	=	383.00
	between		1.52	-4.65	6.35	n	=	58.00
	within		0.36	-0.77	2.98	T	=	7.20
CARTONL	overall	0.12	0.20	0.00	0.89	N	=	244.00
	between		0.14	0.00	0.87	n	=	42.00
	within		0.14	-0.11	0.51	T-bar	=	4.16
Secure	overall	0.41	0.47	0.00	1.00	N	=	383.00
	between		0.32	0.00	1.00	n	=	58.00
	within		0.37	-0.14	1.24	T-bar	=	6.60
Internet_share	overall	0.22	0.17	0.00	1.00	N	=	415.00
	between		0.18	0.00	1.00	n	=	58.00
	within		0.04	-0.08	0.55	T-bar	=	7.16
market power	overall	0.02	0.04	0.00	0.30	N	=	444.00
	between		0.04	0.00	0.25	n	=	62.00
	within		0.01	-0.02	0.07	T-bar	=	7.16
prepaid_share	overall	0.32	0.32	0.00	1.00	N	=	469.00
	between		0.30	0.00	1.00	n	=	63.00
	within		0.13	-0.36	1.04	T-bar	=	7.44

Table 1B: Data definitions

DESCRIPTION OF MAIN VARIABLES (at bank level)

Variable	Description	Source
CARTONL	Percentage of number credit cards used over the internet at least once in the reference period	Banca d'Italia
INTERNET_SHARE	Share of Internet payments	Banca d'Italia
PREPAID_card	Log-Number of prepaid cards	Banca d'Italia
RETAIL_PAY	Log-number (or value) of total retail payments	Banca d'Italia
SECURE	Percentage of 3DS transactions on total credit card transactions	Banca d'Italia
MARKET_SHARE	PSP market share in retail payments (percentage of total retail payments)	Banca d'Italia
TURNOVER	Log-number (or value) of credit card based Internet transaction divided the number of credit card	Banca d'Italia

Figure 4: Empirical distribution (number of banks) rate of 3D-Secure adoption

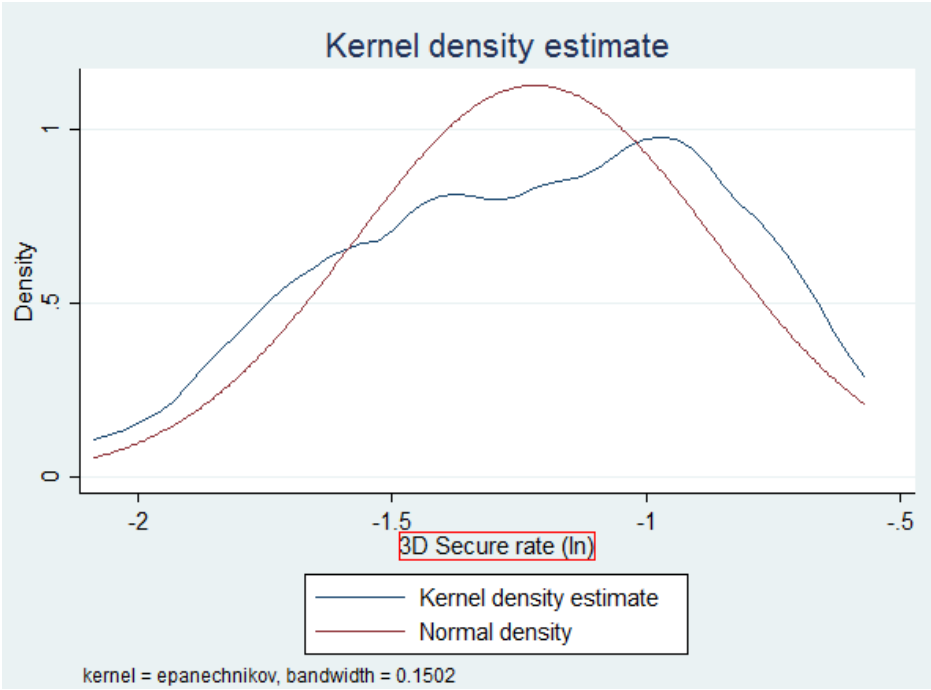


Figure 5: Empirical distribution (number of banks) of the log-turnover per card

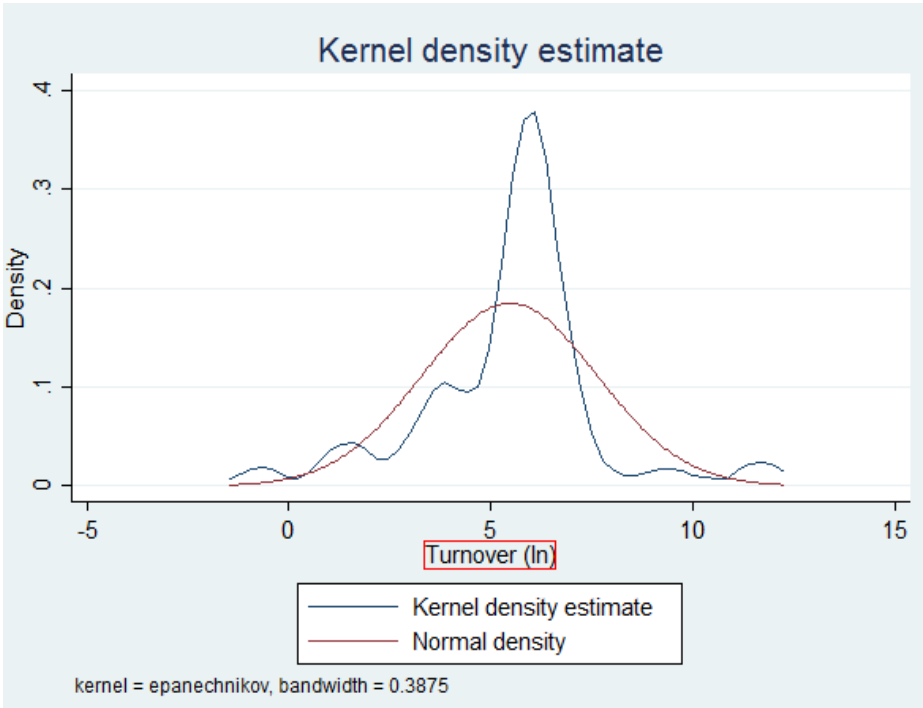


Table 2 : Estimation of the equation model 5.1 "TURNOVER"; fixed effect (unbalanced panel)

Regressor (a)	Fixed Effect Base	Fixed Effect Full
Secure	-.340**	-.346**
	(.1053)	(.1433)
$\sum_h Z$	.	*yes*
Time dummy	yes	yes
Constant	yes	yes
Observations	376	376
Groups	58	58
R^2(within)	0.29	0.30

[a] Dependent variable: *TURNOVER* = log-value of credit card based Internet transaction divided number of issued credit card; robust standard errors in round brackets. The summation term among the regressors indicates the set of h environmental variables (Z) which can influence the use of card-based internet payments. Control variables identifies size, share of internet payments, alternative payment methods, network size (i.e. number of card active over Internet), PSP type (market share, business model, non-bank operators) which may affect the choice of paying over the Internet.

***, **, * : statistically significant at 1%, 5%, 10%.

Table 3: Estimation of the equation model 5.2 "CARD_ONLINE"; fixed effect (unbalanced panel)

Regressor (a)	FE Base	FE Full	FE-lagged Full
Secure	-0.097**	-0.096**	-0.106*
	(.0407)	(.0324)	(.0531)
$\sum_h Z$	.	*yes*	*yes*
Time dummy	yes	yes	yes
Constant	yes	yes	yes
Observations	234	222	221
Groups	44	42	42
R^2(within)	0.30	0.36	0.49

[a] Dependent variable: *CARD_ONLINE* = percentage share of credit cards active at least once for Internet payments during the reference period (semester); robust standard errors in round brackets. The summation term among the regressors indicates the set of h environmental variables (Z) which can influence the use of card-based internet payments. Control variables identifies size, share of internet payments, alternative payment methods, network size (i.e. number of card active over Internet), PSP type (market share, business model, non-bank operators) which may affect the choice of paying over the Internet.

***, **, * : statistically significant at 1%, 5%, 10%.

Table 4: Estimation of the equation model 5.1 "TURNOVER"; Arellano-Bond GMM-style estimator (unbalanced panel)

Regressori	1-AB		2-FE_lag
	Base	Full	Full
Turnover(t-1)	0.671***	0.523***	0.362***
	(-0.211)	(-0.123)	(-0.073)
Secure	-0.339**	-0.457**	-0.389**
	(0.148)	(0.191)	(0.146)
$\sum_h Z$	.	yes	yes
Time dummy	yes	yes	yes
Constant	yes	yes	yes
Observations	376	367	375
Groups	58	58	57
R2	.	.	0.57
AR1(p-value)	0.02	0.01	.
AR2(p-value)	0.86	0.78	.
Hansen test (p-value)	0.10	0.17	.

[a] Dependent variable: *TURNOVER* = log-value of credit card based Internet transaction divided number of issued credit card; robust standard errors in round brackets. The summation term among the regressors indicates the set of h environmental variables (Z) which can influence the use of card-based internet payments. Control variables identifies size, share of internet payments, alternative payment methods, network size (i.e. number of card active over Internet), PSP type (market share, business model, non-bank operators) which may affect the choice of paying over the Internet.

[b] Coefficients and p-values in parentheses from Arellano-Bond two-step GMM estimation (xtabond2 in Stata). All covariates – with the exception of dummies - are treated as endogenous and instrumented through their lagged values. For the system-GMM estimator instruments are specified as applying both to the differenced equations and to the level equation. The number of instruments is always kept below the number of groups. AR1 and AR2 are the Arellano-Bond tests for first and second order autocorrelation of the residuals (one should reject the null hypothesis of zero first order serial correlation and not reject the null hypothesis of zero second order serial correlation of the residuals.) The Hansen test of overidentifying restrictions suggests that the instruments are appropriate.

Table 5: Estimation of the equation model 5.2 "CARD_ONLINE"; Arellano-Bond diff-GMM estimator (unbalanced panel)

Regressori		2-AB		2-FE_lag
	Base	Full-1lag	Full-2lags	Full
Card_online(t-1)	-0.490***	-0.523***	-0.473***	0.385***
	(-0.120)	(-0.123)	(-0.076)	(-0.073)
Card_online(t-2)	.	.	-0.270***	.
			(-0.06)	
Secure	-0.059**	-0.076*	-0.075*	-0.106*
	(0.022)	(0.039)	(0.047)	(0.053)
$\sum_h Z$	.	yes	yes	yes
Time dummy	yes	yes	yes	yes
Constant	yes	yes	yes	yes
Observations	206	206	195	221
Groups	58	37	37	42
R2	.	.	.	0.48
AR1(p-value)	0.12	0.13	0.13	.
AR2(p-value)	0.01	0.01	0.43	.
Hansen test (p-value)	0.93	0.83	0.45	.

[a] Dependent variable: *TURNOVER* = log-value of credit card based Internet transaction divided number of issued credit card; robust standard errors in round brackets. The summation term among the regressors indicates the set of h environmental variables (Z) which can influence the use of card-based internet payments. Control variables identifies size, share of internet payments, alternative payment methods, network size (i.e. number of card active over Internet), PSP type (market share, business model, non-bank operators) which may affect the choice of paying over the Internet.

[b] Coefficients and p-values in parentheses from Arellano-Bond two-step difference GMM estimation (xtabond2 in Stata). All covariates – with the exception of dummies - are treated as endogenous and instrumented through their lagged values. For the diff-GMM estimator instruments are specified as applying the differenced equations. The number of instruments is always kept below the number of groups. AR1 and AR2 are the Arellano-Bond tests for first and second order autocorrelation of the residuals (one should reject the null hypothesis of zero first order serial correlation and not reject the null hypothesis of zero second order serial correlation of the residuals.) The Hansen test of overidentifying restrictions suggests that the instruments are appropriate.

Table 6: Further robustness checks: Alternative equation model 5.1 "TURNOVER" with PREPAID; FE vs Arellano-Bond GMM-style estimator (unbalanced panel < year 2015)

Regressori	1-FE		2-AB
	Full	Full-lagged	Full
Turnover(t-1) (Prepaid)	.	0.525*	0.897**
		(0.062)	(-0.073)
Secure (credit)	0.326**	0.273**	0.075
	(0.148)	(0.088)	(0.027)
$\sum_h Z$	yes	yes	yes
Time dummy	yes	yes	yes
Constant	yes	yes	yes
Observations	225	188	188
Groups	38	35	35
R2	0.30	0.62	.
AR1(p-value)	.	.	0.23
AR2(p-value)	.	.	0.32
Hansen test (p-value)	.	.	0.04

[a] Dependent variable: *TURNOVER with prepaid* = log-value of prepaid based Internet transaction divided number of issued prepaid cards; robust standard errors in round brackets. The summation term among the regressors indicates the set of h environmental variables (Z) which can influence the use of card-based internet payments. Control variables identifies size, share of internet payments, alternative payment methods, network size (i.e. number of card active over Internet), PSP type (market share, business model, non-bank operators) which may affect the choice of paying over the Internet.

[b] Coefficients and p-values in parentheses from Arellano-Bond two-step GMM estimation (xtabond2 in Stata). All covariates – with the exception of dummies - are treated as endogenous and instrumented through their lagged values. For the system-GMM estimator instruments are specified as applying both to the differenced equations and to the level equation. The number of instruments is always kept below the number of groups. AR1 and AR2 are the Arellano-Bond tests for first and second order autocorrelation of the residuals (one should reject the null hypothesis of zero first order serial correlation and not reject the null hypothesis of zero second order serial correlation of the residuals.) The Hansen test of overidentifying restrictions suggests that the instruments are appropriate.

References

- Adyen (2014), “Analysis Reveals Worldwide Impact of 3D Secure on Transaction Conversion Rates. Report. Amsterdam.

- Aprigliano V., Ardizzi G., and Monteforte L. (2017), “Using payment system data to forecast GDP”, Bank of Italy, Temi di Discussione (Working Paper) No. 1098.

- Braz C. and Robert J.M. (2006). “Security and usability: the case of the user authentication methods”. In International Conference of the Association Francophone d’Interaction Homme-Machine.

- Carbo-Valverde S., Chakravorti S. and Fernandes F.R. (2009), “Regulating two-sided market: an empirical investigation”, ECB, Working Paper Series, n. 1137/2009.

- De Cristofaro E., Parc H.D., Park J.F., Norcie G. (2014), “A comparative usability study of two-factor authentication”, Internet Society, February.

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

- European Commission (2017), “E-commerce sector inquiry”, Final Report, May.

- Ecommerce Europe Association (2016) “Recommendations for improving European online payments regulation”, Report commissioned to and prepared by CleverAdvise (https://www.ecommerce-europe.eu/app/uploads/2016/09/Suggestions-to-improve-European-Online-Payments-Regulation.pdf).

- European Banking Authority (2014), “Final guidelines on the security of internet payments”, 19 December 2014.

- European Banking Authority (2016), “Response to the EBA Discussion Paper on Strong Customer Authentication and Secure Communication”.

- Federal Reserve Board (2015), “Consumer and mobile financial services 2015”, https://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201503.pdf.

- Greene W.H. (2012), “Econometric Analysis”, VII edition, Pearson.

- Hayashi F., Moore T., and Sullivan R. J. (2015), “The Economics of Retail Payments Security”, working paper, Federal Reserve Bank of Kansas City, June/2015.

- Igienico Payment Services (2014) “3-D Secure landscape in Europe”, mimeo.

- Kosse A. (2011). “Do Newspaper Articles of Card Fraud Affect Debit Card Usage?”, ECB Working paper, no. 1389.

- Kosse A. (2013).“The Safety of cash and debit cards: a study on the perception and behaviour of Dutch consumers“, DNB Working paper 245, De Netherlandsche Bank.

- Krol K., Philippou E. , De Cristofaro E. , Sasse M.A. (2015), “They brought in the horrible key ring thing!” Analysing the Usability of Two-Factor Authentication in UK Online Banking University College London.

- Roodman, D. (2005), “xtabond2: Stata module to extend xtabond dynamic panel data estimator”, Centre for Global Development, Washington.

- Roodman, D. (2009), “How to do xtabond2: An introduction to difference and system GMM in Stata”, The Stata Journal n. 1, pp. 86-136..

- Schuh S. and Stavins J. (2015), " How do speed and security influence consumers’ payment behavior?", ECB, Working Paper Series, n. 1871/2015.

- Svilar A. and Zupancic J. (2016), " User experience with security elements in Internet and mobile banking", Bank of Italy, Organizacija, vol. 49/2016.