THE IMPACT OF MICROCHIP ON PAYMENT CARD FRAUDS

by Guerino Ardizzi*

Abstract

The issue of payment card frauds has received a great deal of attention from the authorities. A large share of card frauds can be ascribed to the phenomenon of counterfeiting debit cards, a widely used payment instrument in "face-to-face" transactions. With the advent of the Single Euro Payment Area, the European banking community has shared and almost reached the ambitious goal of replacing all payment cards (and accepting terminals) with chip-compatible ones, which are considered harder to clone than those with magnetic stripes. Using a biannual balanced panel data from over one hundred Italian banks, we estimate for the first time the real impact on card frauds caused by the chip card migration. The results confirm the positive effects of the new technology: the ratio between frauds and ATM-POS transactions (card fraud loss rate) decreases significantly if the chip card is used.

JEL Classification: C22, C23, D12, E21

Keywords: fraud, debit card, payment instrument, security, chip, technology, prevention, EMV, SEPA

Contents

---

* Banca d'Italia, Market and Payment System Oversight Department. The views expressed in the article are those of the author and do not involve the responsibility of the Bank. I wish to thank Paolo Angelini, Gerardo Coppola, Claudio Impenna, Giuseppe Orru, Ravenio Parrini, Carmelo Petraglia, Eva St. Onge, Gilberto Turati and the anonymous referee for their helpful comments. The usual disclaimers apply.

1. Introduction

The confidence in the means of payment is a public good of which production requires investments in technology. From this point of view, card frauds represent a serious threat to the functioning of one of the most used payment networks in both domestic and international transactions. According to estimates, the fraudulent transactions carried out in Europe on POS and ATM amount to over one billion euros annually; similar figures are recorded in the United States. Much of this amount is used to finance other illegal activities, including international terrorism (Shen et. al. 2007).

The prevention and reduction of risks in the usage of electronic payment instruments are crucial for the integration and integrity of retail payment systems in Europe. The adoption of common security standards, together with the exchange of information and financial education, represents one of the fundamental pillars for the prevention and the reduction of the social costs due to frauds, and the development of secure electronic payments.

The success in the adoption of new preventive technologies represents a strong incentive for market operators to continue in the path of modernization. The savings from the technological innovation, even when they are not properly perceived by the players of change (typically known as "free riding" problems), are then felt by everyone, banks and consumers alike.

The adoption of the “microchip” in the countries involved in the creation of the Single Euro Payments Area (SEPA) is an example of how the strategy of cooperation under the aegis of the authorities, primarily the central banks, could produce positive results. At the end of 2011, about 90 percent of the cards and the accepting terminals (POS, ATM) in Europe (70 percent in Italy), have migrated to the so-called “EMV” microchip technology, developed by Visa Europay-Mastercard since 1999 and endorsed by the European banking community in SEPA. This technology makes it more expensive for the fraudster to duplicate the card with respect to the old "magnetic stripe", and, above all, to capture sensitive data on the microchip.

Ten years ago, with the advent of the euro, the rates of chip migration in Europe were a tenth of the present ones; in Italy virtually nil. With reference to the physical terminals[1], the fears of fraud have recently been directed to countries outside the EU. Among these, the United States, which still allows a widespread use of the magnetic stripe technology, stands out. This technology is still combined with the microchip of the cards issued in Europe in order to preserve the fundamental principle of full accessibility of the payment instruments.

Recently, the "chip only"-based solutions have been under scrutiny within the Eurosystem, with cards issued without magnetic stripes and with limited possibilities of usage outside of the chip-EMV networks (European Central Bank, 2010). These are more incisive solutions to the problem of illegal card usages because most of which involve counterfeit cards used in face-to-face transactions in areas where the "magnetic stripe" is still prevalent (ECB 2011, VII Sepa Report). The “liability shift rules”, issued by the governance authorities of the card payment schemes, allow transferring the losses from frauds to the unsafe operators, thereby giving a decisive incentive to the European migration. Nevertheless, such rules are not applicable in the other contexts. In the countries outside the EU, the self-regulation bodies – even among the common cards and brands (e.g. Visa and Mastercard) - pursue different strategies to protect the interests of the local bank communities.

The Italian banks have accelerated the replacement of cards and terminals with "chip compliant" devices after the initial uncertainties, especially since 2006, when the rate of card fraud (fraud losses out of total operations) reached the maximum point (Bank of Italy, Report on the 2009).

The debate is still in progress between the opposing positions of the European banking community, which supports the general shift towards the chip, and the United States where only recently has settled some of the resistance after a serious debate on the issue. Given the migration costs, the chip represents an effective solution to the problem of the asymmetries in the security provisions both at national level and at international level. To date, there are

[1] This work does not consider the fraudulent activities carried out using cards in virtual transactions (so-called "card not present" frauds).

no rigorous (redundant) empirical studies that demonstrate the effectiveness or benefits of microchip technology in the reduction of card frauds.

The objective of this study is therefore to verify empirically the impact of the microchip on card frauds, taking into account the Italian case study. In Section 2, the available literature on the subject is reviewed. In Sections 3 and 4, more details of the problem of card frauds and the database used in this work are presented. Section 5 illustrates the model of analysis and the econometric approach, aimed to verify the relationship between microchips and debit card frauds. 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 opportunistic and illegal behaviours in several economic and financial sectors (insurance, accounting, finance, etc.) Nevertheless the analyses of the links between fraudulent utilizations and payment technologies are scarce. The analytical approaches to the issue of frauds in the payment system are essentially twofold. The fraudulent phenomena are evaluated either in terms of their impact on the demand for means of electronic payments, or in terms of their effects on the risk management models.

In the first approach the fraud is an explanatory variable in a micro-founded payment instruments demand equation. The purpose is essentially to evaluate the consumer behaviours in choosing secure payment instruments. Kosse (2010) demonstrates for example that frauds significantly reduce the use of payment cards both in the POS, and in the ATM[2]. These works do not deal, however, with the issue of the determinants of frauds.

In the second approach, the fraud assumes the role of dependent variable. The fraudulent event is the random variable which the analyst has to interpret on the basis of a probabilistic model. The probabilistic fraud function can be estimated through various quantitative methods (logistic or neural models, Bayesian approaches, actuarial models). In

[2] The negative impact of the fraud on the use of payment cards is also confirmed in a recent work that for the first time utilizes macro-territorial data for Italy (see Ardizzi and Iachini, 2012).

this context, the analyst's goal is essentially to calculate the probability of a given tool being used fraudulently (Shen et al., 2007, Pulina and Paba, 2010). At the same time, once identified the probabilistic model of the fraud, the risk manager's goal is to prevent and intercept anomalies, and to reduce the risk of losses for the bank (Caimi et al., 2006).

Among the econometric techniques most often used for the detection of the risk of fraud is the binomial logistic regression (Shen et al., 2007). It is based on high-frequency time series of micro-data, where the dependent variable takes the value 1 when an irregular event occurs (es. theft, loss, cloning) and 0 in all other cases[3]. Among the explanatory variables of the equation, a series of covariates that identify the type of instrument (e.g. debit card), the type of technology (e.g. chip card), the brand (e.g. Visa) and "individual specific" characteristics of the card holder (e.g. expenditure ceilings, age, income, residence, and so on) can therefore be inserted. This type of analysis requires a considerable amount of confidential information, available only in the protected archives of the anti-fraud offices of the companies that either issue or manage payment cards.

However, the regression techniques used by the risk management analysts provide useful insights for applications addressed to the policy maker, taking into consideration bank-level data sets and non-categorical fraud risk indicators.

3. Payment card frauds

The analysts distinguish between "gross fraud" and "net fraud" (Caimi et al., 2006). The "gross fraud" is the total amount of transactions disclaimed by the cardholder (also automatically through card blocking or alert systems) when the card has been compromised. This is thus typically measured from the “issuing” side of the card[4] (so-called "issuing fraud").

[3] The most complex models consider multinomial categorical variables, with reference to specific events: theft, loss, interception of the card, etc.

[4] When the irregular transaction is detected, on the contrary, on the side of the operator who accepts the card, we talk about "acquiring fraud". In this paper we do not consider this possibility, since the information available on the "acquiring side" are difficult to distinguish by type of card (debit, credit or prepaid card) or channel (Internet, physical).

The fraudulent claims of the card can be traced back to several causes: theft, loss, cloning, non-receipt, etc. The gross fraud represents the potential loss for the circuit, and does not take its actual economic impact (loss) on the intermediary and on its capital into account. The "net fraud" is instead the accounting loss recorded on the balance sheet by the acquirer or the issuer due to the occurrence of the gross fraud. The incidence of the gross fraud on the net one depends on the mechanisms of transfer of responsibility (liability shift) between the various parties involved (issuer, acquirer, owner, operator).

In this paper we consider the amount of the gross fraud, divided by the gross amount of the total card transactions (known as “card fraud loss rate”) as a synthetic indicator of the risk of the instrument. Moreover, we consider only the fraudulent uses as a result of card counterfeiting or cloning, namely the interception of sensitive data and the duplication of the physical supports for illicit purposes unknown to the legitimate cardholder. This is the fraud case that has involved the transition to the microchip technology in order to prevent frauds. Compared to the magnetic stripe, the "chip" enables both the direct and the protected on-line dialogues (encryptions) between the card and the acceptance device (ATM or POS) in the preliminary phase of authentication of the cardholder, and the encrypted storage of the sensitive data once the transaction has been completed.

Cloning is still the main cause of payment card frauds. It is perpetrated by means of "skimming" devices which allow fraudsters to decode the data contained in the magnetic stripe card (e.g. holder’s name, card number, etc.) in order to use them in devices duplicated through ATM and POS. Excluding the frauds carried out without the presence of the physical card (the so-called "card not present" fraud, for example via Internet, telephone or mail), cloning represent about 70 percent of all card frauds (Central Office for Means of Payment Fraud-UCAMP Report 2010[5]). The debit cards record lower levels of fraud (about 1/5) than those on average experienced on the credit cards, most of which at the domestic level, as a result of the combination of the PIN code on ATM and POS (Bank of Italy, 2009). However, frauds committed through counterfeit cards used in the systems that do not

[5] The Report contains also an illustration of the different types of fraud and of the underlying mechanisms.

adopt the chip technology have risen during the last few years, also for debit cards[6] (e.g. ATM, Maestro, Visa Electron circuits).

This study focuses therefore on debit cards, which are mainly used in face-to-face transactions. The credit card, besides not requiring the compulsory matching of the PIN code when the operation takes place, is also used in the "distance" transactions, such as the Internet or telephone ones. This instrument presents, therefore, an area of risk that is more extensive in terms of security provisions and is fundamentally different compared to the debit card (Sahin and Duman, 2011). Furthermore, the higher concentration in the credit card market strongly reduces the statistical numerosity of the information available on the debit card, issued by nearly all Italian banks and more popular among clients (Bank of Italy, Survey on Household Income and Wealth, 2010).

Since 2009, after the constitution (Act 166/2005) of the antifraud system at the Ministry of Economy and Finance-Central Office for Means of Payment Fraud (UCAMP), people can rely on the publications of reports on card frauds in Italy to provide a great deal of systemic level information relative to the size and the dynamics of frauds with respect to the different types of instrument or channel (debit card, credit, internet, etc.) and the underlying causes (cloning, theft, loss, etc.) According to the biannual report on 2009-2010 (the latest data available), the credit card fraud losses, divided by the total amount of POS and ATM transactions, have decreased by 11 percent (UCAMP Report 2010) compared to the preceding two years. Those related to cloning have decreased by 27 percent. In the biennium in question, the percentage of microchip cards increases by 10 percent, going from 60 to 70 percent (ECB 2011). Since 2007, in line with an acceleration of the migration to EMV chip required by SEPA, the (credit and debit) card fraud rate indicates a downward trend, decreasing from 0.07 percent (as a share of the level of POS transactions) to 0.05 per cent in 2010 (Bank of Italy, Annual Report 2010).

Similar trends can be inferred even at international level, despite that the data relative to the phenomenon of fraud available are subdued. Combining the information released by the EAST (the European ATM Security Team) on fraud via ATMs and those published by

[6] In the case of the debit cards the proportion of the frauds attributable to the clonings is higher (80%) than that relative to the credit cards (60%).

the ECB on the percentages of the compliant chip cards in Europe, an inverse relationship can be interpreted: as the proportion of microchip cards increases the rate of fraud decreases[7] (Figure 1).

4. Dataset

In this work we use data drawn from the reports of the intermediaries on the payment services collected by the Bank of Italy from each reporting body (bank or financial company) on a cumulative and anonymous basis, available since 2009. The available information allow us to construct a longitudinal database for the years 2009 and 2010, which includes 108 intermediaries representative of over 60 percent of the debit card market. We have excluded the banks that have missing values[8] as well as those that do not report all the relevant data (e.g. frauds, transactions, number of cards issued) in both reference periods, in order to obtain a strictly balanced panel dataset.

The panel data for the two years under consideration show a decreasing trend in the rate of debit card frauds - calculated as the ratio between the amount of gross frauds and the total amount of the transactions processed by the card issuer, consistent with the whole banking system (Table 1) as reported by the Central Office for Means of Payment Fraud-UCAMP[9] (2011).

Figure 2 shows the accumulated banking statistics available at the Bank of Italy (but not for individual banks) on the fraud rates relative to the transactions and the share of the migrations to the chip debit cards occurred in Italy between 2003 and 2010; it also shows a sharp increase in the fraudulent transactions in 2006, caused mainly by the intensification of

[7] On this point see also CapGemini, World Payment 2011.

[8] If we consider also the banks which do not report frauds data (missing), conventionally setting them equal to zero, we run the risk of underestimation of the phenomenon and of selecting intermediaries with a fraud risk equal to zero not in a random way.

[9] In particular, the UCAMP archive collects personal daily data from the single intermediaries (banks, companies issuing credit cards on the basis of information directly coming from the anti-fraud offices of the companies. Information are shared between the reporting institutions for preventive reasons, according to the provisions of the law. The statistics used in the present work, instead, concern semi-annual or annual information, aggregated and signaled by the banks to the Bank of Italy with the aim to provide the information concerning the pattern of the phenomenon.

cloning, followed by a gradual reduction that coincides with an acceleration of the migration to the chip.

5. Model of analysis

In the literature review we have shown that in the approach adopted by the sector analysts in the study of card frauds for forecasting purposes it is related to a set of explanatory variables within regression models for categorical data (e.g. logit, probit models). The relationship is expressed according to a function like this:

$$y_i = f(x_1 .... x_n)$$

Where y is the target variable for the instrument of payment i, generally expressed as a binomial function. The variables that affect the probability of occurrences of fraud (Caimi et al., 2006) and which represent the arguments (regressors) of the function, consider the type of cards used (e.g. credit or debit), the presence of chip on the card, the type of control over shipping and activation processes of the card, the credit limit granted to the customer, the licensing and warning systems (e.g. sms alert), an so on.

On the ground of the available data (accumulated at the bank level), you may consider only some of the variables listed above. In particular, the available variables (counted from the side of the issuing bank) are:

- Total number of cards in circulation issued by the reporting institution

- Number of cards with the chip

- Amount of POS transactions and ATM withdrawals through cards issued by the reporting institution

- Amount of transactions carried out through cards issued by the reporting institution at its own acceptance points (so called “on-us transactions”)

- Amount of disclaimed transactions due to operations with cards issued by the reporting institution (issuing fraud).

The equations of the fraud analysis model are therefore as follows:

$$FRAUD = \alpha_0 + \beta_1 CHIP + \Sigma_j \beta_j Z_j + u_{it} \quad [1]$$

con j=2…n

The dependent variable (FRAUD) is equal to the ratio of operations disclaimed by the holder (gross fraud) to total transactions (POS and ATM), which is also the card fraud loss rate. As the rate of fraud increases, the potential loss and hence the risk borne by the cards issued by the reporting bank increases. This variable does not follow a dichotomous distribution such as in the logistic model, nevertheless it is distributed continuously in the range [0-1] with a concentrated mass of (positive) values close to zero. Figure 3 shows the empirical distribution of the variable FRAUD calculated from data provided by the Italian banks and pooled for the biennium 2009-2010. Figure 4 shows the density function of the same logarithmically transformed data, from which a log-normal empirical distribution can be inferred.

The first variable in the right-hand side of equation [1] is equal to the percentage of microchip cards (CHIP). Its coefficient, expected to be negative, aims to capture the effect of the technology believed to be safer against fraud. This variable is considered exogenous to the model, as the choice to adopt chip cards has been driven by the European Payments Council (EPC, the self-regulatory body of European banks), and the banks are committed to migrate all SEPA cards and terminals to chip EMV standards by the end of 2010[10].

The summation term among the covariates indicates the set of environmental variables (Zj), and that of the relative coefficients, which can influence the indicator of fraud. One of the control variables used in the context of the risk management systems (Caimi et al., 2006) identifies the so-called “on-us” operational component (ONUS), equal to the percentage of transactions that are completed at POS and ATM terminals owned by the same bank that issued the card. Therefore, we consider Z1 = ONUS. Even the expected effect of this variable on the fraud rate is negative: the higher the share of transactions within its own

[10] The EPC's SEPA Cards Framework (SCF) recognises the EMV standard for SEPA-wide acceptance of payments with cards at very high levels of security (European Payments Council, 2009).

network, the lower the information asymmetries, and the higher the ability of the intermediary to prevent the frauds promptly (Giacomelli, 2008).

The data in Figure 5 show a lower incidence of the "on-us" fraud rate compared to the overall fraud rate.

A second control variable (Z2 = QCARTE) takes into account the relative size of the intermediary, expressed as a percentage of the cards issued compared to the overall number of cards in circulation or to the intermediated transactions. The effects on the fraud indicator can be ambiguous: on the one hand the larger diffusion of the instrument may increase the probability for the bank to have counterfeited cards (positive coefficient); on the other hand, the bank can better diversify the risk (negative coefficient) by expanding its market share.

Finally, in the longitudinal models the term u_{it} in the equation [1] can be broken down into an individual specific effect, a temporal effect, and a stochastic disturbance. In particular, the individual specific effect incorporates the unobservable elements[11] of "firm specific" heterogeneity, reducing the omitted variable bias in the estimates. The time specific effect can be captured by providing a year dummy variable.

6. Estimation of the model

The parameters of the equation [1] were estimated using the balanced panel of 108 intermediaries observed in 2009 and 2010. The dependent variable (FRAUD), i.e. the fraud rate is expressed in terms of logarithms (lnFRAUD), in order to reduce the dispersion and the asymmetry. The explanatory variables, instead, are expressed in percentage terms:

a. the percentage of CHIP cards

b. the percentage of on-us transaction (ONUS)

c. the market share (%) of the cards issued (QCARTE)

[11] These elements may for example be linked to the internal control and risk management system, to the type of customer, etc. See Giacomelli, 2008

Table 2 describes both the descriptive statistics and the correlation matrix for the above-mentioned variables, from which collinearities strong enough to reduce the consistency of the estimates do not seem to arise.

First of all, we estimate the "basic" log-linear model[12] that considers only CHIP among the covariates. Then we include the control variables and test the stability of the results with respect to the disturbances affecting the initial model. In all cases a time dummy variable has been included.

We have used a panel model with "random effects". The Hausman test strongly rejects the hypothesis of "fixed effects"[13], while the Breusch-Pagan test refuses that of "poolability" (cross-sectional model instead of panel model).

6.1. Results

The results of the estimates are shown in Table 3. Since the dependent variable is logarithmic, the regression coefficient β must be interpreted as a one unit change in the regressor X (expressed as a percentage), which is associated with a percentage change in Y, which exactly equals β.

As expected, the coefficient of the rate of migration to chip cards (CHIP) is consistently negative. The magnitude of the effect, moreover, is significant: an increase of ten (percentage) points of the number of chip-compliant cards is associated with a reduction in the fraud rate of approximately 6 -7 percent[14].

---

[12] The log-linear models are usually applied in the presence of dichotomous explanatory variables. In this case, the independent variables are all continuous but fall within the range [0-1], being expressed in percentage terms.

[13] The lower accuracy of the "fixed effect" estimator, which considers time-invariant individual characteristics, moreover, is also detected when the "within" (intra-group) variability is dominated by the "between" (inter-group) variability, see Cameron and Trivedi 2005. This is exactly the case under consideration (see Table 2). In addition, we have conducted the J-test for overidentifying restrictions (fixed vs. random effects), which is also robust to heteroskedasticity: also in this case the fixed effect model is rejected.

[14] Based on the estimated coefficient, ceteris paribus, EMV technology would have resulted in fewer debit card fraud losses for about 35 million euro from 2006 (the year of the pick of frauds) to 2010, freeing potential resources to continue to innovate in prevention.

The incidence of the ONUS transactions turns out to be not significant[15]; however, the market share (QCARTE) shows a significant negative impact on the fraud rate. Nevertheless, this variable may also be a proxy of the probability that the intermediary intercepts the cards used at its own points of acceptance and of the ability of the intermediary to diversify the risk and reduce the potential loss. This effect partially offsets the low significance of the estimated coefficient for the variable "ONUS".

This is true even if we replicate the regression exercise within the ambit of homogeneous circuits, which is distinguished between domestic fraud rates (cards issued and used in Italy) and cross-border fraud rates (usage abroad). The results are reported in Table 4[16].

6.2. Robustness checks

We conducted robustness checks of the outcomes discussed in the previous paragraph, using alternative estimation methods that control: 1) heteroskedasticity and autocorrelation of the residual terms; 2) non-normal distribution of the variables; 3) simultaneous causality. Each of the above-named points highlights a violation of the assumptions underlying the regression models and can make the results inconsistent.

The method used to control the first distortion factor (1-PCSE) considers an OLS estimator of the parameters that nevertheless allows us to take into account the possible autocorrelation within the panel and the contemporaneous heteroskedasticity of the residual terms[17].

---

[15] The variables representative of the acceptance infrastructure of the cards (ATM, POS, chip-compliant devices) located in the same seat of the issuing intermediary have not turned out to be significant on the contrary. This is consistent with the approach followed which just carries out a census of the phenomenon from the perspective of the issuer of the card and not from the perspective of the intermediary who manages the POS or the ATM terminal (acquirer). For the sake of brevity we do not present these estimations.

[16] The estimations are in this case carried out on the unbalanced panel, since the breakdown between Italy and foreign countries entails a loss of statistical information and of sample numerosity in the considered period.

[17] Beck and Katz (1995) suggest this approach, of the so-called OLS panel-corrected standard error PCSE model, with OLS estimators, preferring it to the "generalised least square" (GLS) generalized model, which instead requires T> n. On this point see also Hoechle (2007) and Podestà (2002). We apply also a random effects panel model that admits the presence of "clustered standard errors" that is of errors correlated "between" (per unity of the panel) and robust against heteroskedasticity. This method does not control also for, however, the contemporaneous presence of serial and cross sectional correlation. The estimated coefficients

In addition, we also consider a so-called "quantile" regression estimator (2-quantile method) where the relationship between y and x is not expressed by the variation of the conditional mean of y given x (classical linear model), but by the variation of one of its quantiles (e.g. median). This approach is useful in the presence of non-normal distributions of the dependent variable, or that of high statistical dispersion, which may make the mean value less significant. Furthermore, it may be interesting to calculate the impact of the chip on the median fraud rates of the distribution computed at the level of the riskier intermediaries (i.e. 75th percentile). For this method we have also resorted to the non-parametric bootstrap to calculate the standard errors and test the significance of the estimated coefficients without necessarily making assumptions about the probabilistic model and the reference distribution of the sample. The results reported in Table 5 consider the regression on the median value and on the 75th percentile of the dependent variable[18].

The third factor of distortion (simultaneous causality) is the possibility that the relationship between the rates of fraud and chip cards being bi-directional. For example, the trend of the fraud rate in the period can also expedite the decision of the bank to migrate to the chip card. Hence, also an OLS regression (3-OLSlag method) of the fraud rate (always expressed in logarithmic form) on the one year lagged values of the CHIP variable has been taken into account. Such solution should reduce this problem[19]: the fraud rate reported in the year t can be influenced by the migration rate in the period t-1, whereas the opposite is not logically true.

---

for the variable CHIP are however always significant and comparable in intensity with each other; also the results of these estimations are available in Appendix (Tables 5 and 6).

[18] The estimation for quantiles is conducted on the "pooled" panel, in order to gain degrees of freedom. The quantile regression applied to panel models in fact requires a high sample size to unbundle the unobservable individual specific effects and produce consistent estimates (see Koenker, 2004).

[19] The general approach to follow for dealing with the problem of the simultaneous causality or endogeneity of the regressors is the one of the regression with instrumental variables. However, in this case there are no instrumental variables that simultaneously satisfy the requirements of relevance and of exogeneity available (see Cameron and Trivedi, 2005)

Table 5 shows a comparison between the different estimators, applied to the basic model[20], which includes the impact of the chip and the time dummy among the explanatory variables:

$$lnFRAUD = \alpha_0 + \beta_1 CHIP + \beta_2\, d\_anno \qquad [2]$$

The basic model has proved to be sufficiently robust to perturbations of the same (see par. 6.1), and has the advantage of parsimony in the parameters to be estimated.

The robustness checks seem to be more than satisfactory. In all the methods adopted, the significance and the intensity of the CHIP effect on the fraud rate (lnFRAUD) are confirmed. The magnitude of such effect is higher in the regression estimated with the 75th percentile method, compared to that estimated on the 50th (median), suggesting that the benefits derived from the microchip are most evident in the presence of high fraud rates[21].

7. Conclusion

The payment card fraud issue is the focus of growing attention, especially after the initiation of the SEPA. The phenomena of cloning and counterfeiting significantly affect the segment of the debit cards (e.g. ATM), where some asymmetries in the field of the security systems, both between banks and between domestic and international systems, are exploited. Among these asymmetries, the non-uniform migration of the card schemes to the microchip technology, especially in countries outside the Eurosystem, stands out. In this work an empirical exercise aimed at assessing the benefits arising from the microchip cards in terms of reduction of fraud rates in Italy has been carried out for the first time. The results confirm the positive effects of the new prevention technology: faced with an increase of 10

[20] The results relative to the whole model obtained through the different estimation methods are reported in Table 6.

[21] Final tests concerns the robustness of the results obtained even apart from the log normal model, considering the absolute values of the rate of fraud as the dependent variable (FRAUD). We use a Tobit regression model: unlike the standard panel regression with individual random effects, this model can accommodate the particular distribution of the dependent variable, which is censored (non negative) and has a concentrated mass of positive values very close to zero. The results confirm the significance of the coefficient (negative) the degree of migration to the chip on the rate of fraud. Moreover, all results are robust aggregating the 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, available on request from the author.

percentage points (in absolute terms) in the cards migrated to the chip, the ratio of frauds to transactions is reduced by 6 - 7 percent on average. That would imply that in Italy since 2006, the year in which the frauds reached their maximum peak, the chip technology has resulted in a reduction in the losses arising from frauds of several tens of millions of euros on payment card transactions through ATM and POS, freeing potential resources that can be devoted to prevention innovations.

However, we must also admit that the migration to chip is an expensive process; this is one of the factors that led to the strong resistance by the banking community, especially in the United States.

Indeed, the major step in making the switch to the EMV has been the installation of new hardware for all cards and accepting devices (automated teller machines and points of sales). Nevertheless, it is quite impossible to conduct a systematic and robust cost-benefit analysis to evaluate if there are net revenues of the single banks net of the start-up infrastructural expenses (costs) due to the expected decrease in the fraud losses (benefits). Specific business data are required and they are not available. We can just formulate some general considerations. The cost-benefit analysis relies on the timing of the switches, on the processing time and on other ICT cost trends (e.g. the cost of each new chip card was lower than $1 per card in 2007, but it was about $8 ten years before), and on the kind of the operator. Moreover, the cost of the chip migration is affected by the individual choice of the type of authentication protocol[22] (e.g. static data authentication or dynamic data authentication). Another important element to be taken into account in the decision-making is the type of the incentive rules defined by the regulation/self-regulation authority in the field of the transfer of responsibilities so as to support the more reliable operators (liability shift rules).

[22] In particular, the standard EMV chip, in its original version proposed by the debit card companies (1998), included two typologies of authentication protocol of the rightful possessor of the card: the “static method” (so called "static data authentication") and the dynamic one (so called "dynamic data authentication"). The latter, compared to the first one, allows to regenerate some control codes for each new operation, thus making in fact the eventual chip card cloning useless, as well as costly for the fraudster. As part of the migration process in Europe, most operators have chosen the "static" method of the standard chip, which is obviously less expensive but does not reduce to zero (minimize) the risk of cloning.

From just an issuing perspective, in Italy between 2006 and 2010 about 24 million debit cards have been moved to EMV technology. As someone estimates that the additional cost of each new chip card is equal to about 1 $ (First Data 2011), we can compute that the total migration costs to the chip debit cards have been equal to about 18 million euros in the same period for the Italian banks. The cumulative reduction of losses arising from the frauds in the issuance of the cards in the same period has been equal to over 46 million euros in the case of the debit cards, giving rise to a net benefit on the issuing bank side equal to about 22 million euros in 5 years. On the acquiring side the cost-benefits calculation is much more complicated and strongly depends on the migration strategy and on the market share on the issuing and acquiring sides, but we think that net benefits are possible, especially considering that the reduction of the fraud losses due to the chip transactions is permanent over the years while the start up costs are one-off. Moreover, if the "liability shift" rule applies, the EMV compliant bank can avoid high fraud losses on the acquiring side.

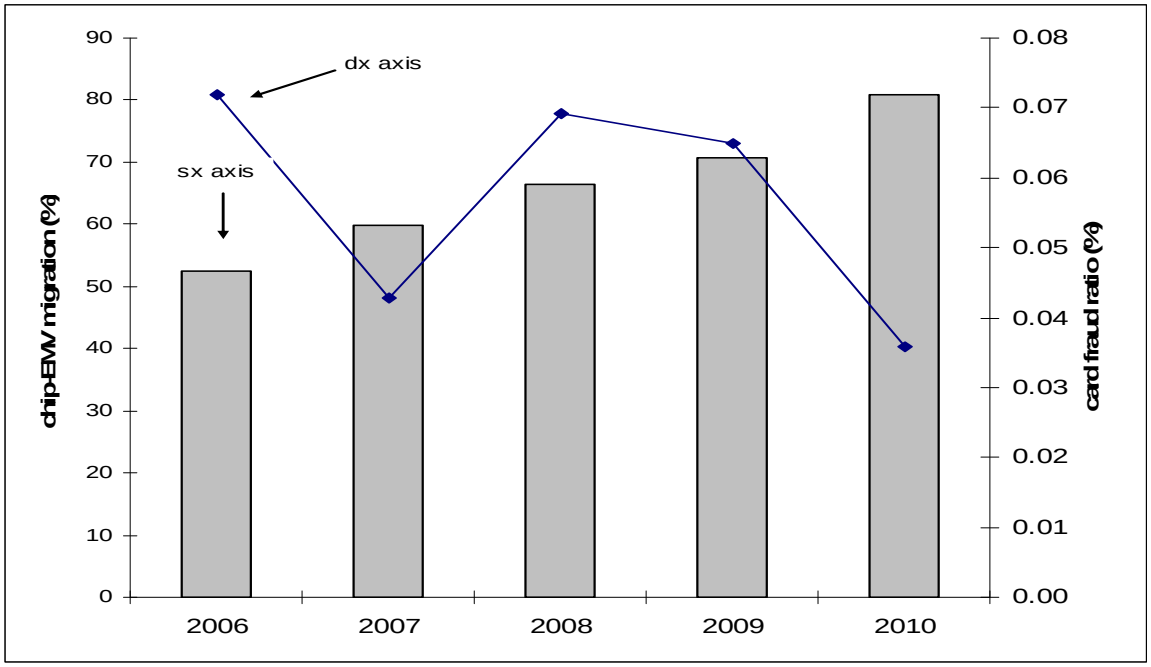
Finally, we should not forget that the enhanced safety in the payment network, following a global reduction of frauds, is an important benefit (public good) from a social planner's perspective, also if it is underestimated by a private short-term profit function. Indeed, in the medium term the benefit will overcome the cost for all the operators, considering that major safety enhancement can increase card usage and the additional revenues for the banks.

It is therefore necessary to strengthen the international commitments aimed at promoting the widest possible adherence to the new technology standards, planning also the so-called "chip only" option, favourably accompanied by incentive-compatible rules on the transfer of responsibility so as to support the more reliable operators[23] (so called "liability shift rules").

[23] See the considerations of the Eurosystem in the seventh Report (2010) on the state of the art of the Single Euro Payment Area (SEPA), p. 7.

Tables and Figures

Figure 1: Pattern of the fraud rate (issuing side) and % of EMV cards in Europe (issuing side) and % of EMV cards in Europe



Source: EAST, ECB

Table 1: Card fraud (clonation):

Description	Panel	Total Italy (1)
Fraud rate (clonation): year 2010	0.016%	0.015%
% change 2009-2010	-22.79%	-17.14%

(1) – Source: Ministery of Treasure, Antifraud Office

Table 2: Panel dataset - descriptive statistics

Variable		Mean	Std. Dev.	Min	Max	Observations	
lnFRAUD	overall	-8.956	1.405	-16.367	-5.492	N =	216
	between		1.192	-13.357	-6.227	n =	108
	within		0.748	-11.966	-5.946	T =	2
CHIP	overall	0.684	0.320	0.000	1.000	N =	216
	between		0.284	0.000	1.000	n =	108
	within		0.150	0.184	1.184	T =	2
ONUS	overall	0.113	0.138	0.000	0.943	N =	216
	between		0.120	0.001	0.836	n =	108
	within		0.068	-0.163	0.389	T =	2
QCARTE	overall	0.005	0.022	0.000	0.175	N =	216
	between		0.021	0.000	0.174	n =	108
	within		0.003	-0.026	0.035	T =	2
FRAUD	overall	0.000	0.000	0.000	0.004	N =	216
	between		0.000	0.000	0.003	n =	108
	within		0.000	-0.001	0.002	T =	2

Correlation matrix

Variable	CHIP	ONUS	QCARTE
CHIP	1		
ONUS	-0.103	1	
QCARTE	0.066	0.150	1

Dependent variable: lnFRAUD

Source: Bank of Italy, banking statistics

Figure 2: Rate of fraud and chip-EMV indicator in Italy

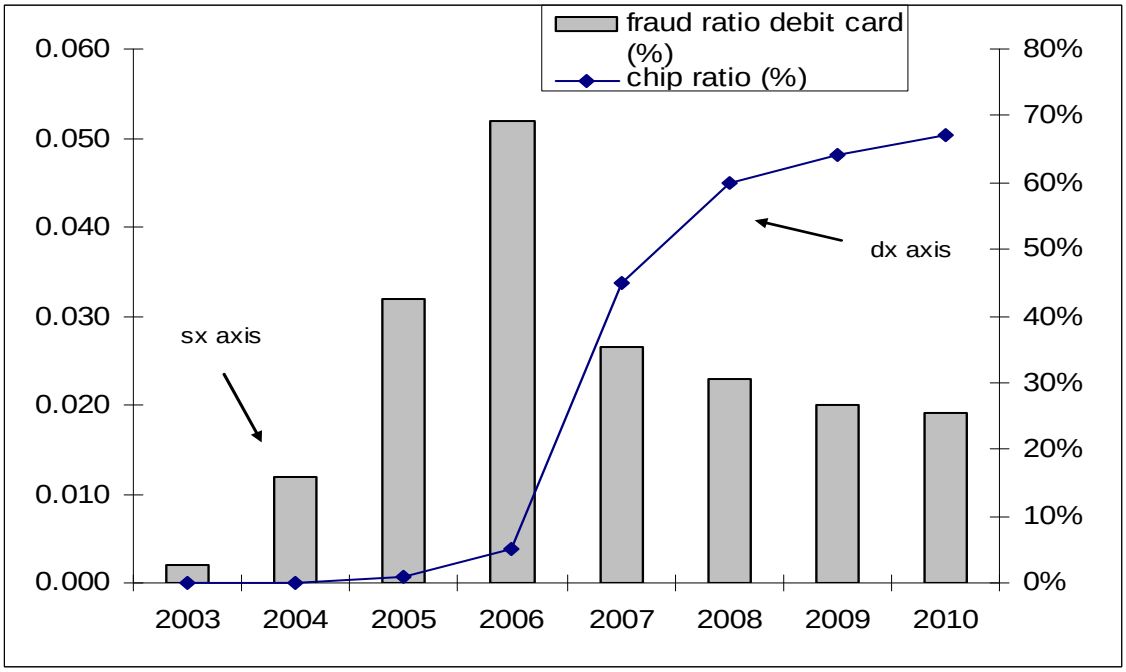


Figure 3: Empirical distribution (number of banks) rate of fraud on debit cards

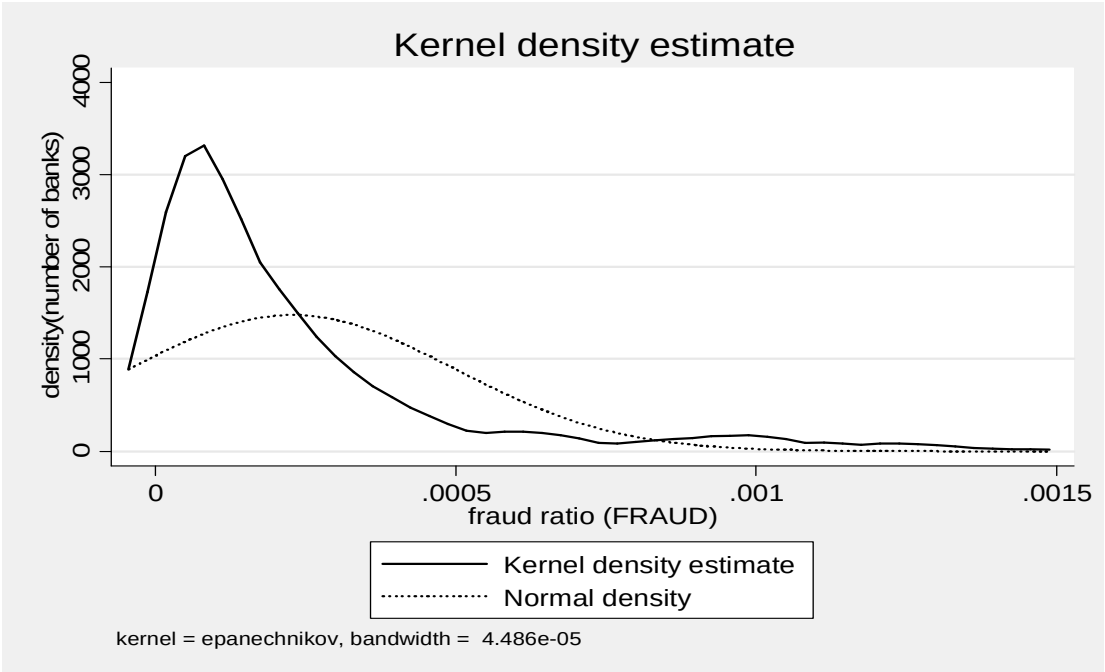


Figure 4: Empirical distribution (number of banks) of the log - fraud rate

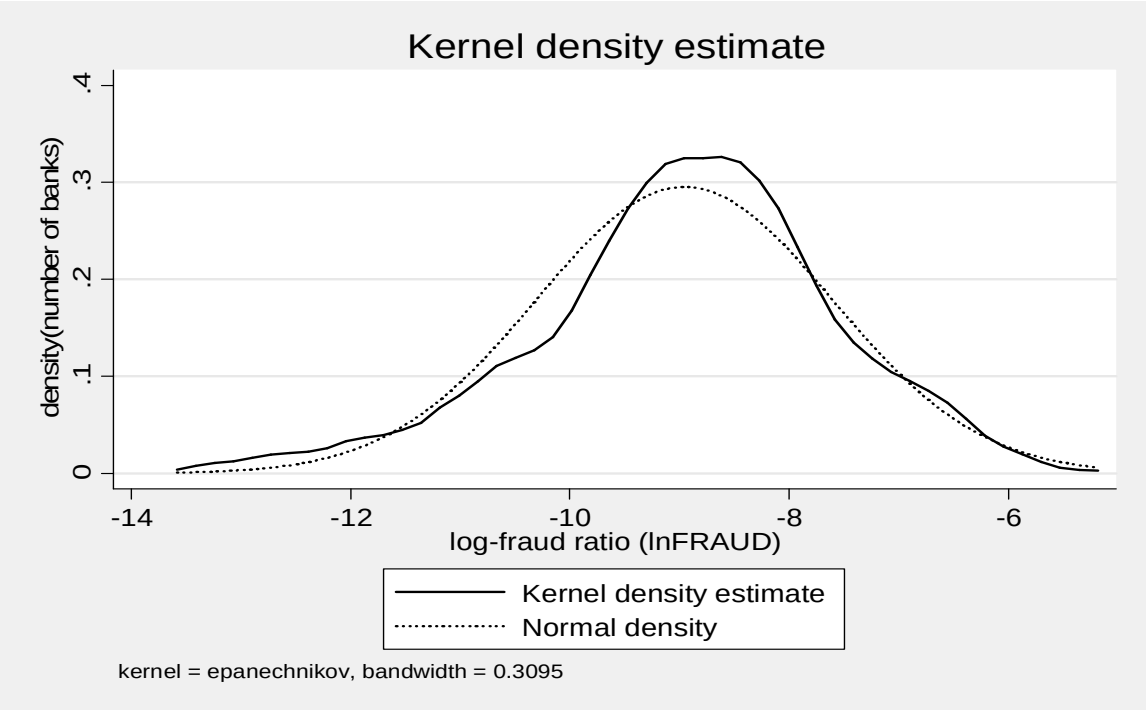


Figure 5: “Onus” card fraud rate vs total card fraud rate

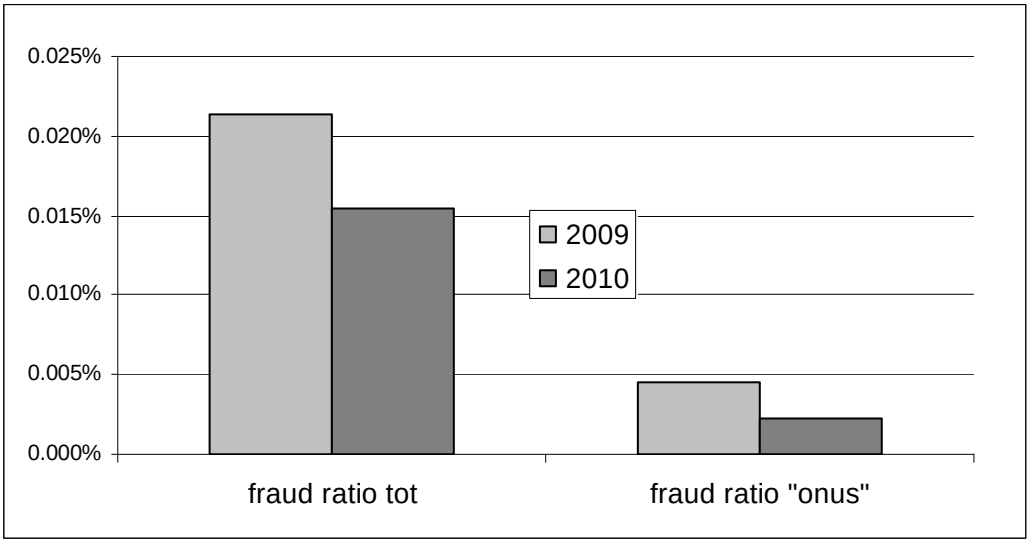


Table 3: Estimation of the log-linear equation model 1 and 2; panel random effect (balanced panel)

Regressor	Random Effect Base	Random Effect Full
CHIP	-0.665***	-0.641***
	(-0.265)	(-0.266)
d_anno	0.292**	0.309*
	(0.149)	(0.157)
ONUS		0.271
		(0.780)
QCARTE		-15.319*
		(8.281)
Constant	-594.93***	-629.8
	(300.53)	(317.22)
Observations	216	216
Groups	108	108

Table 4: Estimation of the log-linear equation model with cross-border or domestic frauds as dependent variable (unbalanced panel)

Regressor	Cross-border fraud rate (log)	Domestic fraud rate (log)
CHIP	-0.692*	-0.702***
	(0.412)	(0.2514)
d_anno	-0.018	0.151
	(0.208)	(0.120)
ONUS	1.042	0.130
	(0.670)	(-0.565)
QCARTE	-13.573*	-10.828
	(7.204)	(9.218)
Constant	26.540	-310
	(419.581)	(-241.421)
Observations	201	336
Groups	108	108

Table 5: Robustness checks against violations of the linear regression assumptions (base model)

Regressori	1-PCSE	2-QUANTILE		3-OLS_lag
		50° percentile	75° percentile	
CHIP	-0.622***	-0.418**	-0.831*	
	(-0.078)	(-0.211)	(-0.487)	
CHIPt-1				-0.920**
				(0.418)
d_anno	0.296***	-0.233	0.292	
	(0.067)	(0.206)	(0.051)	
Constant	-604.0***	-476.19	-254.78	-8.512**
	(133.85)	(369.10)	(327.61)	(0.266)
Observations	216	364	364	165
Groups	108	108	108	.

Table 6: Robustness checks against violations of the linear regression assumptions (all variables)

Regressore	PCSE	re cluster	q50	q90	OLS_lag
CHIP	-0.647***	-0.641**	-0.433*	-0.726**	
	((0.197)	(0.268)	(0.2271)	(0.3037)	
chip t-1					-0.885**
					(-0.4113)
anno	0.303***	0.309*			
	(0.038)	(0.163)			
QCARTE	-14.75**	-15.32*	-15.47*	-0.121	-5.683
	(3.917)	(8.197)	(8.275)	(9.979)	(5.806)
ONUS	0.125	0.271	0.0610	-0.0391	-1.138*
	(0.299)	(0.848)	(0.8405)	(0.6391)	(0.6174)
costante	-616.6	-629.8***	-8.540***	-6.822***	-8.385***
	(75.928)	(326.831)	(0.175)	(0.218)	(0.278)
Observations	206	216	331	331	165
Groups	108	108	.	.	.

Standard errors in parentheses: p<0.10, ** p<0.05, *** p<0.01

Legend: PCSE= panel corrected standard errors regression (balanced data); re cluster = random effect panel with robust cluster standard errors (balanced data); q50 e q90=quantile (pooled) regression (50° e 90° percentile); OLS_lag=ordinary least square regression with lagged control variable (chip t-1).

References

Ardizzi G. e E. Iachini (2012). “Why are Payment Habits so Heterogeneous Across and Within Countries? Evidence From Europe and Italy, Unpublished, Banca d’Italia.

Banca Centrale Europea (2010). “Seventh single euro payments area (SEPA) progress report”, October.

Banca d’Italia (2012), “Survey on Households Income and Wealth”, January.

Banca d’Italia (2010), “Annual Report 2009”, May.

Banca d’Italia (2011), “Annual Report 2010”, May.

Beck, N. e J. Katz (1995), “What to do (and not to do) with time-series cross-section data”, American Political Science Review 89: 634–647.

Cameron C. e K. P. Trivedi, (2005), “Microeconometrics: Methods and Applications”, Cambridge University Press, New York.

Caimi C., Ghisellini R. e A. Giacomelli (2006). “Forecasting model of fraud”, unpublished Si Holding.

Capgemini (2011). “World Payment, Report 2011”.

Central Office for Means of Payment Fraud, (2010). “Rapporto statistico sulle frodi con carte di pagamento”, 1/2011, Ministery of Treasury. http://www.dt.tesoro.it/it/antifrode_mezzi_pagamento/rapporti_statistici/carte_pagamento.html

European ATM Security Team-EAST (2011). “ATM Fraud Analysis Report”, version 18/7/11.http://www.european-atm-security.eu

European Payments Council (2009), “SEPA Cards Framework, version 2.1”, Brussels. http://www.europeanpaymentscouncil.eu/knowledge_bank_detail.cfm?documents_id=330.

First Data (2011), “EMV in the U.S: Putting into Perspective for Merchants and Financial Institutions”, First data corporation.

Giacomelli A. (2008), “Non si gioca con le carte”, in Internal Audit, May-August.

Hoechle D. (2007) “Robust Standard Errors for Panel Regressions with Cross-Sectional Dependence”, The Stata Journal.

Kosse A. (2010).“The Safety of cash and debit cards: a study on the perception and behaviour of Dutch consumers“, DNB Working paper 245, De Netherlandsche Bank.

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

Podestà F., (2002). “Recent Developments in Quantitative Comparative Methodology: the Case of Pooled Time Series Cross-Section Analysis”, DSS Papers Soc 3-2002.

Pulina M., e A. Paba (2010), “A discret choice approach to model credit card fraud”, MPRA Paper No. 20019.

Koenker R., (2004). “Quantile Regression for Longitudinal Data”, Journal of Multivariate Analysis, vol 91, Issue 1, October, 74-79.

Sahin Y. e E. Duman (2011).“Detecting Credit Card Fraud by Decision Trees and Support Vector Machines“, IMECS, March 16-18.

Shen A., Tong R. e Y. Deng (2007).“Application of Classification Models on Credit Card Fraud Detection, IEEE.