Latest news of research

February 2016

Penal Issues

CESDIP
Centre de Recherches Sociologiques sur le Droit et les Institutions Pénales
UMR 8183

www.cesdip.fr

Banking Frauds in Metropolitan France: Profiles of Victims and Decisions to Report to the Police

***Bilel Benbouzid**, lecturer at the LISIS (Laboratoire Interdisciplinaire Sciences Innovations Sociétés), University Paris Est, Marne-la-Vallée and **Sophie Peaucellier**, research engineer at the CESDIP, discuss the findings of an analysis of banking frauds, based on data collected by the INSEE in its Living environment and security (Cadre de vie et sécurité) surveys.*

Methodology

A first step in the analysis of these data has been the use of a multivariate statistical method, multiple correspondence analysis (MCA). This is a standard, efficient way to explore survey data, which summarizes the information contained in the numerous variables present. It enables the simultaneous study of several variables, showing resemblances and dissimilarities between individuals, and is also a means of studying the links between variables as well as the ways in which their modalities are associated.

Introduction

The French criminal code defines fraudulent obtaining as the act of misleading a natural or legal person, thus leading such a person, to his prejudice or to the prejudice of a third party, to transfer funds, valuables or any property. In the cases studied here, the fraud takes the form of one or several debits from a bank account without the consent of the owner of the account, and affecting the entire household. Statistical analysis of data from the last three national victimisation surveys shows a definite rise in the number of victims of this type of frauds, for two reasons: 1) for a large part because of the increase in fraudulent transactions via the Internet, which almost doubled between the 2011 and the 2013 survey, and seem to have leveled off since, according to the 2015 report by the Observatory of Payment Card Security of the *Banque de France*[1] ; 2) new techniques for banking card frauds[2], mentioned consistently by the police and gendarmerie in their preventive communication campaigns. Victimisation surveys enable us to take analysis beyond the quantitative estimate of the extent of the phenomenon. They provide crucial understanding of the process by which victims pass from undergoing an offence to filing a complaint. With respect to reporting, banking frauds occupy a specific position on the overall complaint-filing scene. Cardholders have no obligation to file a complaint, and banks are obliged to reimburse victims rapidly. Now, contrary to expectations, the rate of reporting for banking frauds is relatively high. The purpose of this discussion is to look at the determinants of reporting for victims with various profiles, and to attempt to understand the role of banks in this process.

Fraudulent transactions

In France offences involving instruments of payment are a type of illegality that has received little attention by sociologists of crime since Davidovitch's work[3] on frauds and bad checks. In the first national victimisation survey, in 1985, CESDIP researchers included a question on defrauding, but they later decided to withdraw it, since "the definition of a fraud is complex: either we eliminate it or we run the risk that respondents will interpret it as referring to any unscrupulous attitude in business relations."[4] This difficulty in defining the offence may be avoided, however, by concentrating on one type of fraud in particular. This is the option chosen by the administrators of the national victimisation survey when they collected data on banking frauds, defined as *debiting money on your bank account without your consent and through the use of personal information such as an illegally obtained bank card number, or else by theft or counterfeiting of a check. This fraudulent debit may have taken place via the Internet.*

Banking frauds did not await the generalized use of bankcards as instruments of payment, or the development of the Internet. Every form of bank transactions, throughout the history of banking, has stimulated its own astute defrauding techniques. The quantitative history of banking frauds remains to be written, how-

[1] https://observatoire.banque-france.fr/en/home.html
[2] ONDRP, La criminalité en France, Paris, La Documentation française, 2013.
[3] A. Davidovitch, "L'escroquerie et l'émission de chèques sans provision à Paris et dans le département de la Seine. Enquête de sociologie criminelle », L'Année sociologique, 1955-56, pp. 3-130
[4] M.-L. Pottier, Ph. Robert, R. Zauberman, Victimation et insécurité en Ile-de-France. Les résultats de la première enquête (2001). Rapport final, CESDIP, Guyancourt, 2002, p. 8.

Data, indicators and methods

The "fraudulent transaction" section of the CVS survey

The national victimisation surveys conducted by the INSEE annually question a sample population (averaging 16,000) on the offences the participants claim to have suffered over the past two years. Following a timid attempt in 2010, the CVS survey included a new 52-question module in 2011, entirely devoted to banking frauds. Police statistics cannot be used to assess fraudulent transactions (items 89 to 91, "counterfeiting and use of stolen checks and credit cards" and "fraud and breach of trust" cover a much broader range of offences) and the Observatory of payment cards security (OSCP), which collects data on fraudulent transactions annually from a large panel of banks does not provide access to its database. The CVS survey is therefore the only source of information on banking frauds available to researchers for the time being. Aside from the socio-demographic characteristics of victims, 16 variables derived from this survey enable us to qualify banking fraud victimisation. Two broad categories of variables may be identified:

- Characteristics of the fraud (discovery of a fraudulent transaction, use of the Internet, method used to get hold of banking details, method used for the fraud, country involved, serial nature of the fraud, amount involved in the series of fraudulent transactions)
- Reporting (reporting other than to the bank, reason for filing a complaint or recording on the police docket, object of the complaint, reasons for not reporting, reasons for deciding not to report once in the police station, follow-up on the complaint, reimbursement, outcome of the complaint)

This study is based on the pooled data of the three CVS surveys conducted in 2011, 2012 and 2013. The total population questioned thus amounted to 45,145 households. Only bankcard possessors were interviewed in the banking fraud module, representing 99% of households in the sample. In each sweep, only households claiming to have been victims of a banking fraud were selected.

Indicators

The surveys provide information on the proportion of respondents who were victims (**prevalence**) and the number of incidents of the same kind (**multi-victimisation**) over the past two years. Multiplying one by the other yields the **incidence rate** (number per 100 respondents of incidents of the same type suffered over the reference period). When the latter rate is multiplied by the complaint-filing rate we find the **rate of reported incidence**, which is the figure known to the police or gendarmerie through the complaints that victims claim to have filed. **Reporting** corresponds to the victims' propensity to inform some institution (primarily the police or gendarmerie) of the fraud they have suffered. This may or may not be attended by the **filing of a complaint** – the only procedure, in France, which requires the police officer to write a report to be sent to the Public prosecutor – or a recording with no report (**police docket**), which does not involve transmission to the Public prosecutor's office.

ever. It would no doubt relativize the idea that this type of offending has risen spectacularly. The historical perspective afforded by findings from victimisation surveys is not sufficient to indicate long-term, structural trends. There are indications, however, that over the period covered by the last three CVS surveys (from 2009 to 2012), slightly over 3 million households were victims of a fraudulent withdrawal of funds from their bank account – which is to say, on average, a scant 4% of households in metropolitan France. This overall rate is of course very low, but observation of its trend shows it to have risen steadily and significantly (with a 1% margin of error) with each new CVS survey (chart1), from 3% for the 2011 survey to 5% for the 2013 one. Almost two thirds (59% of the aggregate samples) of the victims had suffered a fraud on the Internet (chart2): their banking details had been retrieved on the Internet and/or a fraudulent transaction made by that means. This particular type of victimisation apparently accounts for the upward trend. Observation of the means used to operate the latest fraudulent transaction shows that the Internet is the only one to be increasingly utilized, whereas the others seem to have levelled off, or even to be used less often than before (chart3). Whereas the median annual sum remains stable (300 euros), conversely, the rise in amounts debited, including some very large sums, has led to a dazzling increase in the average sum debited over the last two years (see chart4).

CVS surveys still cover too short a period to uncover trends with respect to banking frauds, so that for the time being their contribution in terms of knowledge pertains primarily to the analysis of reporting. It should be noted, first, that defrauding is one of the types of victimisation for which the reporting rate is highest. Its magnitude is comparable to rates for burglary and car thefts (see chart5). Between the first and the third survey, for all victims taken together, we find an overall decline in reporting (going to a police station or gendarmerie), which affects the number of complaints filed, whereas registration on the police docket tended to rise (between 2009 and 2012). Approximately the same pattern is found for complaints – again, between the first and the last survey – if we concentrate on reporting for defrauding via the Internet, in spite of an upward trend in reporting and police docket rates (chart6).

Why such a high rate of reporting when, as we know, since 2009 victims of banking frauds, and especially those committed on the Internet, no longer need to resort to filing a complaint or obtaining registration on the police docket?[5] Indeed, possessors of credit cards whose numbers have been fraudulently used (counterfeit cards or fraudulent CNP [card-not-present] payments) can object to that payment at their bank without having to previously file a complaint with the police. The same is true for phishing[6] since 2011. The bank is obliged to immediately reimburse the amount of the unauthorized operation in these types of victimisation. How, then, can we account for this unexpected finding?

Exploring reporting using multiple correspondence analysis

Analysis of reporting was performed using MCA (see methodology box) for victimised households only. It shows, concretely, how the various aspects of banking frauds fall into patterns (see chart7).

Patterns of banking fraud victimisation

The multivariate analysis included a number of questions pertaining to the fraud as well as to the socio-demographic characteristics of the household and of its reference person. A first difference within the sample shows a split that is familiar to victimisation scholars, between reporting and non-reporting. On the one hand we find reporting of the fraudulent transaction, usually by filing a complaint, among households which have generally experienced one or several debits of large sums (ranging from 500 to 5,000 euros). On the other hand we see essentially passive households (no complaint filed, no police docket or notification outside of the bank, sometimes even no request for reimbursement by the latter), who suffered fraudulent debits or attempts involving small amounts (0 to 500 euros).

Five variables account for most of a second split: use of the Internet (be it to get hold of banking details or to commit the fraud), the means utilized to operate the fraudulent transaction, the types of methods used to get hold of the banking details, the uncovering of the fraudulent transaction by the victim and its serial nature. On the upper part of the diagram, we find an almost

[5] C. Article L133-19 of the Monetary and Financial Code, paragraph II, in application of the European SEPA directive (Single Euro Payments Area), in force as of November 1, 2009.

[6] Phishing (known as hameçonnage in French) is a technique used by tricksters to obtain personal details. It takes the form of leading the victim to believe he or she is dealing with a reliable third party – a bank, administration, or other – so as to obtain some personal information (password, credit card number, date of birth, etc.). This may be done by electronic mail, phoney websites or other electronic means.

total absence of the Internet as vehicle for the fraud. In most cases the victimised household is informed of it by the police, the gendarmerie, the tax administration, or other. Most involve single transactions, but of large amounts (10,000 euros or more). Not all of these are reported, but when a complaint is filed it generally is successful. On the lower part of the diagram, we find very widespread use of the Internet for the fraudulent transaction. The latter is discovered either by consulting a bank statement or because a purchase via a bankcard is refused. In this case, there are often a series of fraudulent debits of sums ranging from 0 to 5,000 euros. These victimised households are in turn divided between reporting – usually to be reimbursed – and non-reporting. For those who pursue their complaint, the suit generally has a negative outcome in terms of the detection, arrest, and sentencing of the offender.

Three profiles for victims

This initial analysis clearly points to two factors that are key to the study of bank frauds: whether or not the fraud takes place through the Internet and the way victimised households deal with the issue of reporting. These two variables are actually closely tied to all the other variables studied. There is, for example, the fact that serial fraudulent transactions (or the last transaction, when there was not a series) of less than 100 euros are not reported, for the most part (see chart8). This may be because there is a sort of tolerance for debits of small sums, but the most probable hypothesis seems to be that reporting is not required for the problem to be solved. Conversely, for losses of more than 100 euros, reporting prevails significantly, with a peak for debits of 1,000 to 4,999 euros. In other words, beyond a definite monetary threshold, victimised households seem to feel compelled to reporting. But again, for frauds exceeding 5,000 euros, while the majority of cases are reported, the reporting rate declines gradually. This indicates a threshold beyond which we may postulate that victimised households are better informed of their rights, and are well aware that they need not file a complaint to obtain reimbursement.

This is an interesting piece of information, but the financial factors provide only a partial explanation of reporting. To understand the various dimensions of reporting, we use an analysis combining multiple variables and the typological classification of victimised households. This yields a more complex portrayal of reporting. We have retained the breakdown that provides the most refined approach to the different profiles of victims, one which uncovers 4 groups:

1- Reactive households victims of frauds other than on the Internet (22.7% of the sample);
2- Reactive households whose victimisation is linked to the Internet (32.3%);
3- Passive victimised households (44.7%);
4- Uninformed victimised households (0.34%).

The latter group is an artifact of the questionnaire. Since banking frauds are handled as a household victimisation, a single individual (known as the "reference person") answers questions for the household. In some cases, the respondent may have been informed of the victimisation without necessarily having been actively involved with the problem. He or she will therefore respond positively as to the existence of the victimisation but will be unable to provide any details. Inasmuch as this fourth group is not really representative of the consequences of victimisation and the action taken to remedy it, it will not be taken into account for the rest of the analysis.

Furthermore, none of these groups characteristically fall into any socio-economic category, which means that for each of the groups evidenced no category is either over- or under-represented, and all categories are equally affected.

Reactive households whose victimisations are not connected with the Internet

This group is characterised by a very large proportion of households that reported the fraud to the police or gendarmerie or to some institution other than the bank (municipal police, an elected official or directly to the justice department). In every case someone went personally to a police/gendarmerie station to report the offence. Desisting from filing a complaint or from requesting recording on the police docket once the person was on the premises was lowest here (1.5% of households in this group). Access to the victim's bank details was gained, more often than average, during withdrawal of funds at an automated teller, by theft or via a purchase in a traditional shop.

It is no doubt these types of method that explain why this is the only group with an above-average rate of identification of the offender by the police forces (12% vs 3% in the entire sample), and why a larger proportion of these victims chose to file a complaint, with only 11% of households contenting themselves with a mere police docket. Obtaining reimbursement remains the main reason for filing a complaint, but in comparison with the other group of reactive victims, members of this group were slightly less well reimbursed. The majority of households in this group were victims of single fraudulent transaction (79%), amounting to over 500 euros (56% as against 40% on the average). The complaint therefore involved the last fraudulent transaction in most cases, but complaints for all of a series of fraudulent transactions were also over-represented.

Reactive households whose victimisation was connected to the Internet

In this group, all members claimed to have personally gone to the police/gendarmerie station to report the fraud. It should be noted that in 3 out of 4 cases the household discovered the fraudulent transaction on their bank statement. While the rate of reporting to the police or the gendarmerie reaches 95% (as against 56% for the sample as a whole), the move is quite fruitless inasmuch as the person who committed the fraud is even less frequently identified here than in the sample as a whole (1 % vs 3% on the average). Several of these reactive households ultimately desisted from filing a complaint or requesting recording on the police docket once they were on the police premises (5% of households in this group). It is probable that when they were about to inform the police they learned that there was no need to file a complaint. In the vast majority of cases, people who reported the fraud decided to file a complaint, but a few households opted for the police docket (16% of households in this group), on the basis of police advice in slightly over half of cases. It is primarily the desire to be reimbursed that prompts people to file a complaint (in approximately two out of three cases), whereas banks are actually not allowed to condition the reimbursement of fraudulent debits (in most cases via an Internet manipulation) on the filing of a complaint. This situation does not seem to surprise lawyers specialising in banking law, who claim that banks rarely reimburse victims of frauds automatically. Clients are obliged to file legal suits in the hopes of obtaining reimbursement"[7]. This is no doubt a dissuasive measure devised by banks, which generally end up reimbursing these perseverant victims. Banks rarely go as far as the court. They are actually quite frequently to blame, for not having taken the requisite measures to check the conformity of unusual transactions on their clients' accounts. In the long run, their bank in nine cases out of ten reimburses victims in this group.

Passive victimised households

The typology shows this to be a group characterised primarily by extreme passivity in the face of a fraudulent transaction (100%). For the most part, victims in this group suffered one or several fraudulent debit via the Internet (58%). The chartfor

[7] C. Le Parisien, "Alerte à la fraude au crédit mutuel et à la banque postale », May 19, 2014.—http://ww.leparisien.fr/espace-premium/actu/alerte-a-la-fraude-au-credit-mutuel-et-a-la-banque-postale-19-05-2014-3852357.php

those who did not suffer such debits is 28%. The distribution of frauds with or without use of the Internet is therefore the same in this group as in the overall population (see chart9). Study of the above two groups has already shown us that victimised households tend to resort massively to reporting, irrespective of whether the victimisation was connected with the Internet or not. We may therefore assume that victimisation on the Internet does not contribute to passivity, and that the latter is induced by one or several other factors.

Those individuals in the sample who did not go to a police station or a gendarmerie to report the fraud belong almost exclusively to this group. Among the few people who did go to the authorities, none actually filed a complaint or even requested that the incident be recorded on the police docket. This group is therefore entirely composed of non-reporters. While all of the reasons for non-reporting listed on the questionnaire are cited here, the majority of households in this group (37.3%) mention "another reason", other than those suggested on the response list, and 27.5% allege that reporting was "judged useless". Do the variables "other reasons" and "judged useless" mean that these victims are already cognizant of the fact that there is no need to file a complaint in order to obtain reimbursement? The questionnaire is ambiguous on this point: when the respondent answers "judged useless", what does he or she have in mind? There is the possibility that these victims are informed of their rights: they would then be aware that it is *useless* to file a complaint. Their passivity is in fact quite relative, since only 16% of households in the group did not demand reimbursement from their bank. But it is also possible that these households feel that the chances of obtaining reimbursement are slim, and therefore judge reporting (or even merely informing their bank) useless. It is a fact that for this category of victims there is an above-average rate of refusal by the bank of demands for reimbursement. The rest of the group claim lack of reporting because the offence was not judged sufficiently serious (15.9%), because it did not occur to them (12.3%), they did not have the time (3.8%) or for a very small proportion (1.4%), they did not want any dealings with the law or the police. In some cases the victimized households in this group may not have been affected by the fraud, for which there was an above-average absence of demands for reimbursement by the bank. Indeed, we find that the majority (55% of the group) of those who did not ask their bank for reimbursement are those whose financial loss was smallest (under 100 euros). This percentage rises to 90% of the group if all fraudulent transactions under 500 euros are considered. Not only is there little interest in the reimbursement of sums of less than 100 euros, but also a lack of interest in the status of reimbursement of these sums when they did request it – in the group of those who did not know whether or not they had been reimbursed, all claimed a total loss of 0 to 99 euros.

Conclusion

Multivariate analysis and typological analysis provide helpful elements for understanding reporting, inasmuch as they point to three main profiles for victims, depending on their reaction to victimisation and the context surrounding the banking fraud. The profile of reactive households victimised outside the Internet is quite clear-cut, but the situation is more complicated in the case of reactive households victimised via the Internet and passive victimised households: banking card holders are not held responsible if their card was counterfeited or in case of fraudulent payment, in which cases the bank is responsible for the victimisation. In many kinds of bank frauds the victim has no need to file a complaint. The fact that present laws on banking short-circuit the need for reporting to the police forces was not sufficiently incorporated in the survey module on bank frauds, thus leaving many shady areas which were evidenced when interpreting the victimisation typology: why do frauds via the Internet provoke diametrically opposed reactions among victimised households, with some refraining from reporting of any sort, whereas others demand reimbursement? The present study has only partially elucidated this question, and opens paths for further investigation. It shows the need to improve the CVS survey module on banking frauds. To understand the specificity of reporting for this victimisation, surveys would have to introduce new questions collecting information on banks and their interaction with victims. The on-line commercial intermediaries providing transferral of funds from purchasers to banks while offering insurance services for the transactions (Paypal, Amazon, etc.) should also be taken into account. Understanding the propensity to report banking frauds is tantamount to analysing what the interplay between the victim, banks, on-line commercial intermediaries and the criminal justice institutions.

Bilel Benbouzid (*Bilel.Benbouzid@u-pem.fr*)
Sophie Peaucellier (*sophie.peaucellier@cesdip.fr*)

Diffusion : CESDIP
Dépôt légal : 3e trimestre 2016 **ISSN** : 1155-4169

CESDIP - UMR 8183
Immeuble Edison - 43, boulevard Vauban - F-78280 Guyancourt
Tél. : +33 (0)1 34 52 17 00 - Fax : +33 (0)1 34 52 17 17

Directeur de la publication
Christian Mouhanna

Coordination éditoriale
Bettino Dyvrande
(conception et maquette)

Traduction anglaise
Helen Arnold
(révisée par **Renée Zauberman** et **Dinah Gross**)

Chart 1: Banking frauds: prevalence and incidence rates per survey

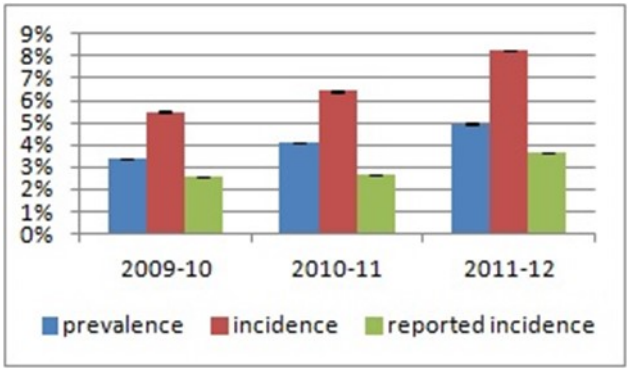


Chart 2: Proportion of banking frauds involving use of the Internet (fraudulently retrieving and using banking details) – cumulated figures over 3 surveys (2009-2012)

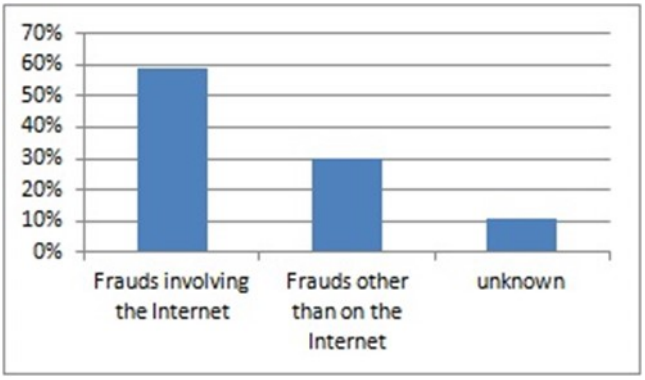


Chart 3: Means used for the last fraudulent transaction, per survey

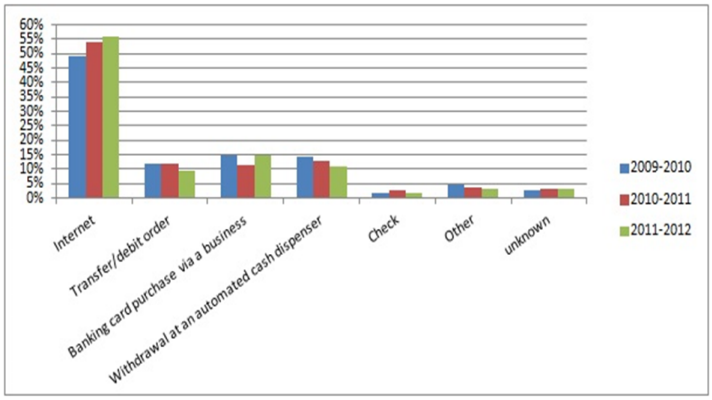


Chart 4: Average and median amounts of serial fraudulent transactions (in euros) per survey

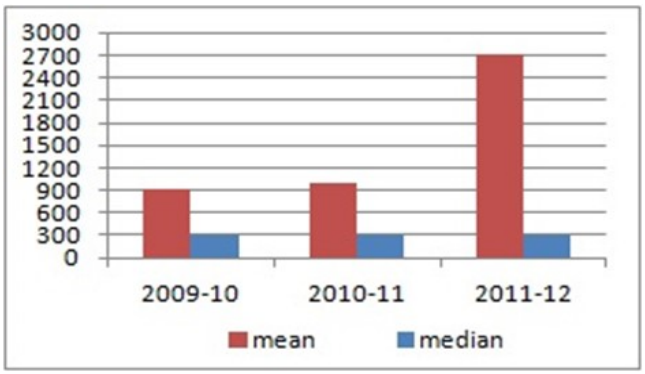


Chart 5: Reporting rate per type of victimisation – cumulated findings over 3 surveys 2009-2012)

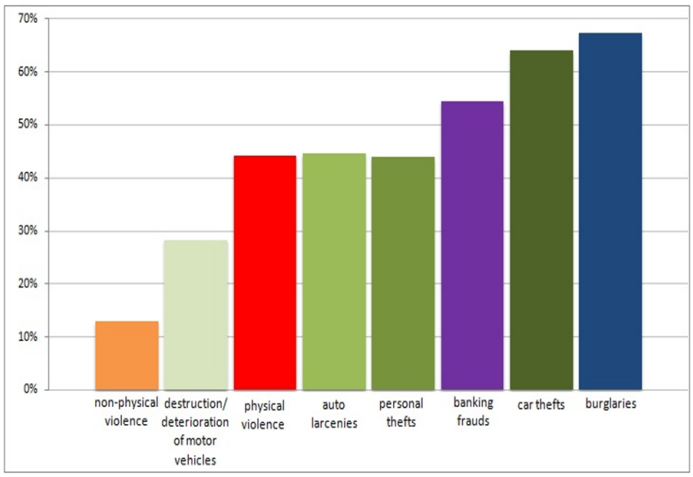


Chart 6: Types of reporting - % per survey

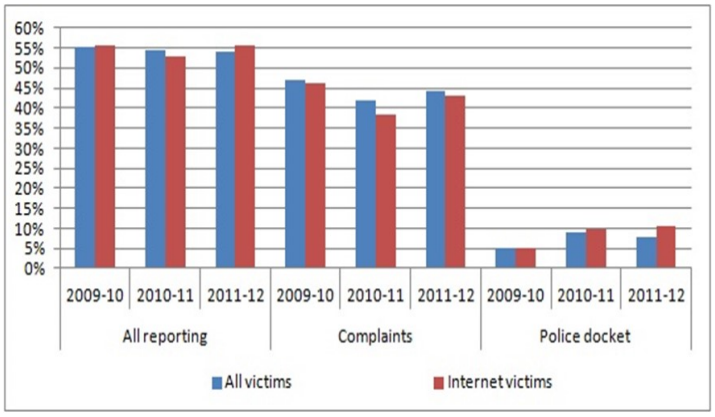


Chart 8 : Reporting according to amount of fraudulent transactions – cumulated findings over 3 surveys (2009-2012)

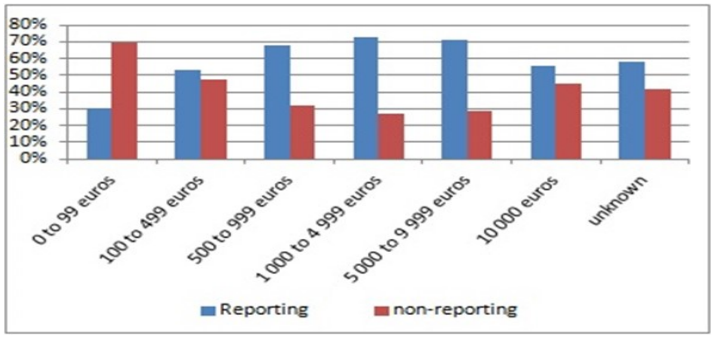


Chart 9: Banking frauds: use of the Internet by passive households – cumulated results over 3 surveys (2009-2012)

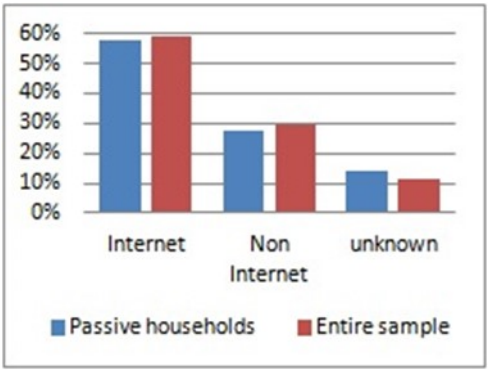
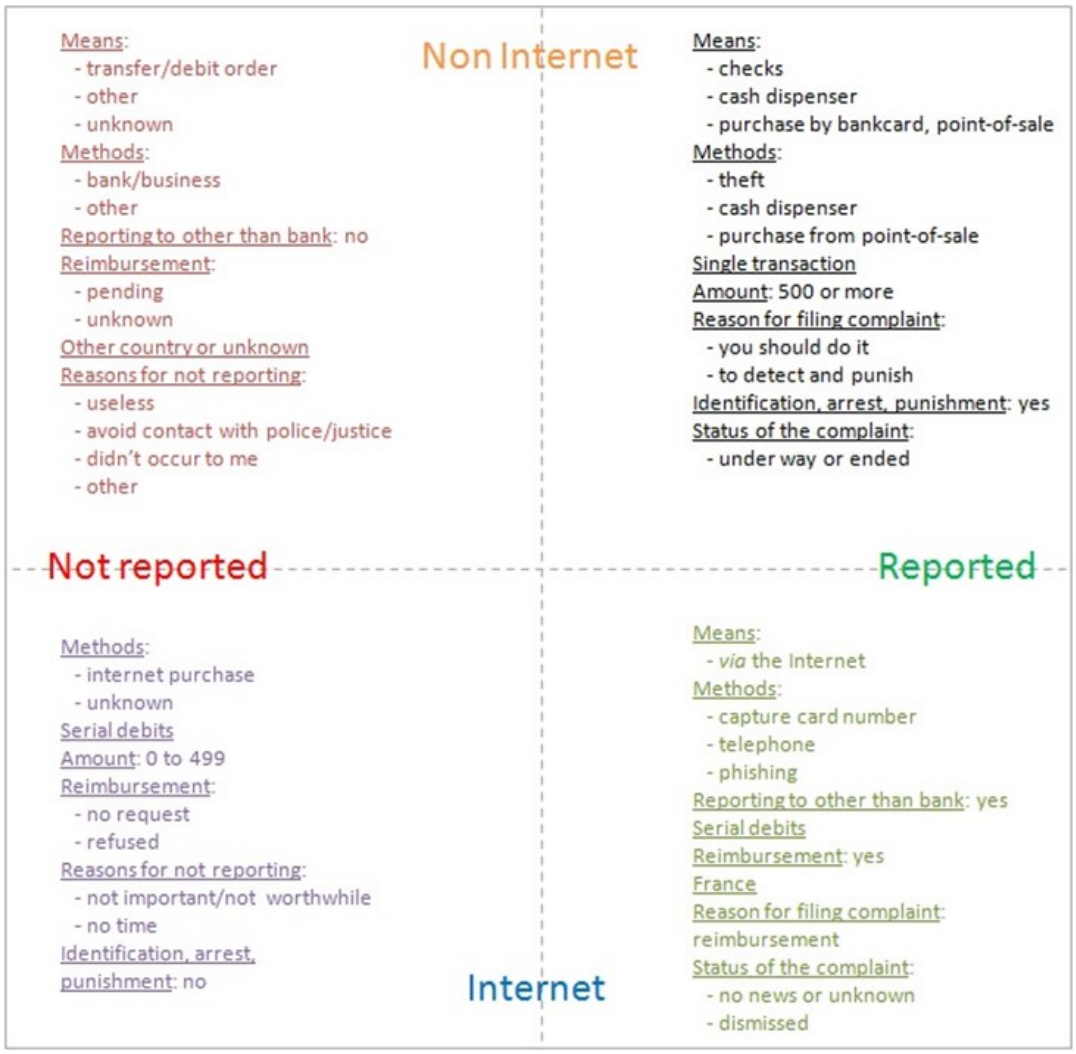


Chart7: Summary distribution of characteristics of banking frauds according to multiple correspondence analysis



All the charts :
Source : INSEE – CVS Field: Metropolitan France

Diffusion : CESDIP
Dépôt légal : 3e trimestre 2016 **ISSN** : 1155-4169

CESDIP - UMR 8183
Immeuble Edison - 43, boulevard Vauban - F-78280 Guyancourt
Tél. : +33 (0)1 34 52 17 00 - Fax : +33 (0)1 34 52 17 17

Directeur de la publication
Christian Mouhanna

Coordination éditoriale
Bettino Dyvrande
(conception et maquette)

Traduction anglaise
Helen Arnold
(révisée par **Renée Zauberman**)