eurofinas

SPECIALISED CONSUMER CREDIT PROVIDERS IN EUROPE

IVZW ACCIS

FRAUD PREVENTION AND DATA PROTECTION

A Eurofinas - ACCIS Report on Fighting Fraud in Consumer Lending

CONTENTS

ABOUT THE AUTHORS

Eurofinas

Eurofinas, the European Federation of Finance House Associations, is the voice of consumer credit providers in the EU. As a Federation, Eurofinas brings together associations throughout Europe that represent finance houses, specialised banks, universal banks and captive finance companies of car, equipment, etc. manufacturers. The scope of products covered by Eurofinas members includes all forms of consumer credit products such as personal loans, linked credit, credit cards and store cards. Consumer credit facilitates access to assets and services as diverse as cars, furniture, electronic appliances, education, etc. It is estimated that together Eurofinas members financed over 324 billion Euros worth of new loans during 2010 with outstandings reaching 824 billion Euros at the end of the year.

Visit www.eurofinas.org

ACCIS

Established in Dublin in 1990, the Association of Consumer Credit Information Suppliers (ACCIS) is an international non-profit association under Belgian law bringing together 37 consumer credit reference agencies in 27 European countries and 3 associate members from other continents. ACCIS' main role consists in representing, promoting, protecting and preserving the common interests of its members. This includes in particular the representation and advocacy of members' interests' vis-à-vis government agencies, the public and all other third parties and to inform its members about matters of concern to them, including information about practices of other members. It also coordinates their mutual interests and to represent them in the global community. ACCIS aims to create a legal climate in which its members can continue to offer and further develop their services both at home and in Europe.

Visit www.accis.eu

FOREWORD

The fight against fraud is of crucial importance to consumer credit providers. Not only does it affect their business, but it also has a significant impact on consumers.

This explains lenders' commitment to help prevent, detect and fight fraud.

The review of the Data Protection Directive presents an opportunity to address and resolve a number of obstacles that arise in this context.

In this report, concrete recommendations are made to policy makers as to how to overcome some of these obstacles.

Eurofinas and ACCIS, co-authors of this report, remain at policy makers' disposal to actively participate and contribute to future work on these important issues.

PEDRO GUIJARRO | Eurofinas Chairman

ACCIS very much welcomes the opportunity to be able to work with Eurofinas on this very important Task Force looking at fraud in consumer credit in the European marketplace. Our members play a very active role in many Member States working with lending institutions to ensure that the growing threat of fraud is prevented.

One of the key tools that enable organisations to help prevent fraud is the availability of timely, accurate and relevant information. So as the European Commission undertakes its review of the Data Protection Directive (95/46/EC), it is timely that this report highlights areas where it is important for access to information to be not only maintained but also improved if fraud prevention is to be effective.

I would like to take this opportunity to thank those of our members who have provided input to the work of the Task Force.

NEIL MUNROE | ACCIS President

THE CONTRIBUTORS

LUCA ARTIZZU
Chief Operations Officer
CTC
l.artizzu@ctconline.it

ANYA FOULDS
Deputy Money Laundering Reporting Officer
Swift Group
anya.foulds@swift.co.uk

LUISA MONTI
Operations Manager
Credit Bureau Services
CRIF
l.monti@crif.com

STEPHAN R. PETERS
Head of Business Area Development
SCHUFA Holding AG/ General Manager
Fraud Prevention Network GmbH
stephan.peters@schufa.de

FABIO TORTORA
Chief Executive
Ournext
fabio.tortora@ournext.eu

JAMES BAIRD
Partner
Gateley LLP
jbaird@gateleyuk.com

MARK GLEESON
Legal Director
Addleshaw Goddard LLP
mark.gleeson@addleshawgoddard.com

NICK MOTHERSHAW
Director of Fraud & Identity Solutions
Experian
nick.mothershaw@uk.experian.com

MIKOLAJ RUTKOWSKI
Manager
Fraud Investigation & Dispute Services
Ernst & Young
mikolaj.rutkowski@pl.ey.com

MONIKA WOLSKA-HERTMAN
Director
Compliance Department
Santander Consumer Bank
monika.wolska-hertman@santanderconsumer.pl

MONIKA CWIERTNIA
Deputy Secretary General
Société Générale Consumer Finance
monika.cwiertnia@socgen.com

PETER HOFMAN
Manager operations
BKR
p.hofman@bkr.nl

CORDULA NOCKE
Head of Legal
Bankenfachverband
cordula.nocke@bfach.de

LAURENCE TASTETS
Secretary General
Société Générale Consumer Finance
laurence.tastets@socgen.com

Eurofinas and ACCIS

ANKE DELAVA
Legal adviser
Eurofinas
a.delava@eurofinas.org

PIERO CRIVELLARO
Public Affairs Manager
ACCIS
pam@accis.eu

LAURA REGINATO
Public Affairs
ACCIS
lreginato@czfpbrussels.com

EXECUTIVE SUMMARY

The results of fraud are often seen as only affecting the credit provider in question. However, in practice this is not the case. Fraud in consumer lending can have a significant impact on consumers. Consumers who have fallen victim to fraud, such as identity fraud, may see their credit history deteriorate when fraudsters take out a loan in the victim's name and subsequently default on payments. These consumers will have to spend a considerable amount of time correcting their record and may face difficulties obtaining a loan in the future, as a result of these fraudulent activities. The impact on their emotional well-being and sense of security should also not be underestimated.

Fraud is a cause of great concern for credit providers. Fraud, in its various forms, results in financial losses for the lending institutions, which therefore have to dedicate expensive resources to identifying and preventing fraudulent acts. This inevitably causes the average cost of credit to increase, thereby affecting all retail borrowers. It is therefore in the interest of all parties to prevent and fight fraud as effectively as possible.

To fight fraud effectively in consumer lending involves the access to, and exchange of, fraud data amongst institutions, private concerns and public databases. This is not always simple due to the lack of harmonisation in data protection rules and/or the stringent nature of these rules.

This report, produced jointly by the European Federation of Finance House Associations (Eurofinas) and the Association of Consumer Credit Information Suppliers (ACCIS), considers the impact of existing data protection rules on the (ability to) fight fraud in the area of consumer lending. It draws on the experience and expertise of the members of a Joint Eurofinas/ACCIS Task Force created to consider this subject.

The report considers the different types of fraud that can occur in relation to consumer lending, discrepancies between national regulations, how lending institutions detect and fight fraud, the role of databases in this process, the size and extent of the fraud problem and the data protection obstacles faced.

Finally, concrete recommendations are made towards ensuring that the future EU legislative framework in the area of data protection is appropriate and workable in practice to fight fraud. In particular, Eurofinas and ACCIS call on policy makers to:

1. Recognise fraud prevention and detection as a legitimate purpose for data processing

2. Adopt a targeted full harmonisation approach in the future EU framework on data protection

3. Encourage public-private data sharing further.

If these recommendations were to be adopted by policy makers, it is Eurofinas and ACCIS' strong belief that consumer credit providers would be in a position to tackle fraud much more effectively. This would ultimately increase the protection of consumers against fraud across Europe.

1.
WHAT IS FRAUD ?

1.1 Types of fraud in consumer lending

In 2007, Eurofinas organised, with the support of ACCIS, an event on fraud during which the participating experts highlighted the wide range of internal and external activities that can constitute fraud in consumer lending.

Subsequently a Joint Task Force on Fraud Data, composed of experts representing both consumer credit providers and credit bureaus across Europe was set up in 2011. Experts were tasked with examining fraud in consumer lending and drafting this report. They also highlighted the wide range of activities that can constitute fraud in consumer lending.

Eurofinas/ACCIS Joint Task Force on Fraud Data meeting, 10 May 2011

TYPES OF FRAUD IN CONSUMER LENDING INCLUDE THE FOLLOWING:

FRAUD IN CONSUMER LENDING

IDENTITY THEFT AND FRAUD
The identity of another person is misappropriated without his/her knowledge or consent, and then used to obtain goods and services in that person's name

CREATION OF SHELL COMPANIES
Which are subsequently used as vehicles to commit fraud

FRAUD LINKED TO THE DISTRIBUTION CHANNEL
For example fraudulent dealers or phone or internet credit fraud

FACILITY TAKEOVER
Where a person unlawfully obtains access to the details of an existing facility and fraudulently operates the facility for his/her benefit

THE UNLAWFUL USE AND DISPOSAL OF FINANCED ASSETS
Also known as 'conversion', where an asset still on finance is sold (often related to financed vehicles)

CREDIT SCORE FRAUD
The provision of false information in order to influence a score

INTERNAL FRAUD
i.e. committed by the finance company's employees

CREDIT DATA/APPLICATION FRAUD
This can include the falsification of documents, such as forged statements of income or bank statements

PHISHING AND PHARMING
Typically involves impersonating a financial institution and using emails to steal personal identity data and account details

CREDIT CARD FRAUD
Fraud committed using a credit card, including operations executed with cards obtained on the basis of a false credit

MISUSE OF FACILITIES
i.e. using a loan for another purpose than that which was agreed

Many of these categories of fraud refer to examples of successful or unsuccessful attempts to deceive a consumer credit provider about facts which influence the creditworthiness assessment of the applicant borrower.

When deciding whether to grant a loan or credit facility to a consumer, a finance company has to assess the creditworthiness of the applicant borrower, i.e. it must examine the individual's ability to meet his/her financial commitments to repay the loan. Assessing the creditworthiness of applicant borrowers is a legal obligation. Before the conclusion of the credit agreement, the creditor has to assess the consumer's creditworthiness on the basis of sufficient information obtained not only from the consumer but also where necessary after consultation of the relevant database(s), in line with Article 8 of the Consumer Credit Directive.[1] Access to, and exchange of, credit data is an essential tool which helps ensure continued sound lending practices by credit providers.[2]

In practice, lending institutions use a computer aided system which carefully and precisely gathers and uses customer information obtained from a variety of sources. The verification of the customer's creditworthiness is done by the lender and it is often in this phase that fraud occurs, such as through the falsification of documents. These cases of fraud and the way lending institutions deal with them should be distinguished from the official prosecution carried out by the national enforcement authorities.

In order for consumer credit providers to establish whether an (attempted) fraud, in whichever form, has taken place, access to and exchange of data is needed beyond the data required to verify creditworthiness. Consumer credit providers need to be able to verify the information and documents supplied to them by applicant borrowers as well as detect possible inconsistencies. Unfortunately, as will be made clear in the following sections, there is no consistent approach across Europe. Whilst in some countries public authorities provide the facility to check the validity of identity documents (e.g. in the Netherlands), in others this is not possible.

Examples of fraud suffered by a lending institution

In 2009, Ournext, an Italian operational risk management consultancy, conducted an analysis on 35 cases of fraud (29 perpetrated and 6 attempted) suffered by a motor finance company in Italy.

The analysis showed that:

- in 4 cases documents containing chief executive officers' (CEO's) personal data - except ID documents - were fake;
- in 4 cases, data related to the company (addresses, VAT numbers, activity data) were false, while in 7 cases they were altered;
- in 6 cases (excluding attempted cases of fraud) ID documents were fake, while in 3 cases one or more of the data was found to be altered;
- in 6 cases (excluding attempted cases of fraud) it was found that income documents were false, while in 4 cases they were altered.

How identity theft can affect a consumer

CRIF, an Italian credit bureau, came across the case of Paola (fictional name). The problems of Paola, a 43 year-old housewife who fell victim to identity theft, started in 2007 when an unknown fraudster obtained a loan to be paid in 36 instalments with her as co-borrower. Having obtained the loan, the fraudster took out two further loans as well as two credit cards in Paola's name. Paola did not have any knowledge of what was happening until 2009 when she applied for a loan with her husband. The finance company rejected the couple's application because she already held other loans and credit cards with various companies.

To make things worse, Paola was cited in a road traffic accident involving people unknown to her, and a motorcycle for which she denies ownership, in 2010.

Worth noting is that Paola had never lost her identity documents, but had given copies to several recruitment agencies when she was looking for work. [3]

1. *Article 8, Directive 2008/48/EC of the European Parliament and of the Council of 23 April 2008 on credit agreements for consumers and repealing Council Directive 87/102/EEC, OJ 22.5.2008, L133/66.*
2. *This is also in line with the requirements of the Capital Requirements Directive: Directive 2006/48/EC of the European Parliament and of the Council of 14 June 2006 relating to the taking up and pursuit of the business of credit institutions (recast), OJ 30.6.2006, L 177/1 and Directive 2006/49/EC of the European Parliament and of the Council of 14 June 2006 on the capital adequacy of investment firms and credit institutions (recast), OJ 30.6.2006, L 177/201.*
3. *Source: CRIF.*

1.2 The legal definition of fraud

Discussions amongst the members of the Eurofinas/ACCIS Joint Task Force on Fraud Data revealed significant differences in the legal definitions of fraud in different EU Member States. Certain Member States have legal provisions in place, specifically in the context of consumer lending or for various types of fraud, whilst other countries do not have any.

A BRIEF OVERVIEW OF THE SITUATION IN FIVE MEMBER STATES:

The Netherlands

In the Netherlands fraud has no legal definition *per se*. Instead, within Dutch private law the term "swindle" is used. In the area of financial services, fraud usually occurs as a property crime that leads to illegal advantages for those committing the crime.

Typically, every fraud exhibits the following characteristics:

- A wilful act;
- A misleading representation of facts;
- The intention of achieving an economic advantage;
- There is a victim; and
- There is an unlawful act.

The term "fraud" is used in several articles of the Dutch Penal Code. The Dutch Act to prevent Money Laundering and the Financing of Terrorism also deals with fraud.

Poland

There is no specific definition of fraud in Polish law. However a definition of a deception in the context of a loan/credit can be found in Article 297 of the Polish Criminal Code which refers to any type of loan/credit. It reads as follows:

"Whoever, in order to obtain a loan, bank loan, loan guarantee, grant, subsidy or public procurement order for himself or for another person, submits false documents or documents attesting untruth, or dishonest statements regarding their circumstances that are of significance for the obtaining of such a loan, bank loan, loan guarantee, grant, subsidy or a public procurement order shall be subject to the penalty of deprivation of liberty for a term of between 3 months and 5 years."

Italy

In Italy fraud is broadly defined as a crime committed in order to make an unlawful gain by using deceptions and tricks[4].

The Italian law transposing the Consumer Credit Directive[5] includes a definition for identity theft, which is the misappropriation of the identity of another person without his knowledge or consent. Identity theft can be total, if it is committed by using only another person's identity, or partial, which means that the fraudster uses both his data and another person's data.

Germany

The German definition of fraud can be found in the German Criminal Code[6]:

"Whosoever, with the intent of obtaining for himself or a third person an unlawful material benefit, damages the property of another by causing or maintaining an error by [presenting] false facts or by distorting or suppressing true facts shall be liable to imprisonment of not more than five years or a fine."

The German Criminal Code further provides definitions of especially serious cases of fraud. For instance:

"An especially serious case typically occurs if the offender

1. acts on a commercial basis or as a member of a gang whose purpose is the continued commission of forgery or fraud;
2. causes a major financial loss or acts with the intent of placing a large number of persons in danger of financial loss by the continued commission of offences of fraud [...]"

4. Article 640, Italian Penal Code.
5. Article 30-bis, Legislative Decree n. 141/2010 of 13 August 2010.
6. Section 263, German Criminal Code, available at: http://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#StGBengl_000P263

The United Kingdom

Fraudulent activity has become a focal point for the UK government over the last 5 years. To reflect the increasing awareness of the problem, new legislation has been passed and new monitoring bodies have been formed to try to counteract the increasing number of cases of fraud.

There is no single definition of fraud in the UK, but rather categories or types of fraud whose definitions can be extended to cover a variety of scenarios. Civil and criminal fraud in the UK consists of an act of deception, intended either for personal financial or proprietary gain or to cause financial or proprietary loss to another.

The Fraud Act 2006, which is the starting point for the definition of fraud in the UK, brought in a new definition of fraud under three "umbrella" categories (which may be committed by individuals or companies): dishonest deception by knowingly making a false representation, dishonest failure to disclose information and dishonest abuse of a position of responsibility.

Most types of fraud in the UK will fall under one of these headings. The Fraud Act also establishes certain specific types of fraud which may not fit easily into the above categories. These include: possession of articles (including electronic data and programs) for fraudulent use, manufacturing of such articles, obtaining services dishonestly. Other types of fraud are identified in other legislation and case law.

It is not difficult to show that the actual transactions or acts involved in fraud have actually occurred (for example, that money has changed hands or a document has been tampered with). The difficulty in UK law arises in that fraud must involve both dishonesty and intent to either make a gain or cause a loss (which must be a gain or loss in terms of money or other property). These are essentially subjective classifications and are therefore difficult to justify objectively. When this is combined with the high burden of proof required for criminal fraud (the intent must be established beyond all reasonable doubt), then fraud can become difficult and expensive to establish.

1.3 Diversity of definitions

The above examples illustrate the wide range of types of fraud that can be perpetrated in the area of consumer lending, as well as the differences that exist across the Member States with regard to legal definitions.

Whilst there is no single definition of fraud in the EU, the following elements seem to be necessary: need for a victim, a wilful act, misleading representation of facts (dishonesty), intention to achieve an economic advantage or to cause economic loss to a third party, and an unlawful act.

As fraud results in a breach of confidence and harms consumers and lending institutions alike, it is of great importance that the necessary information is available and accessible in order to prevent and fight fraud.

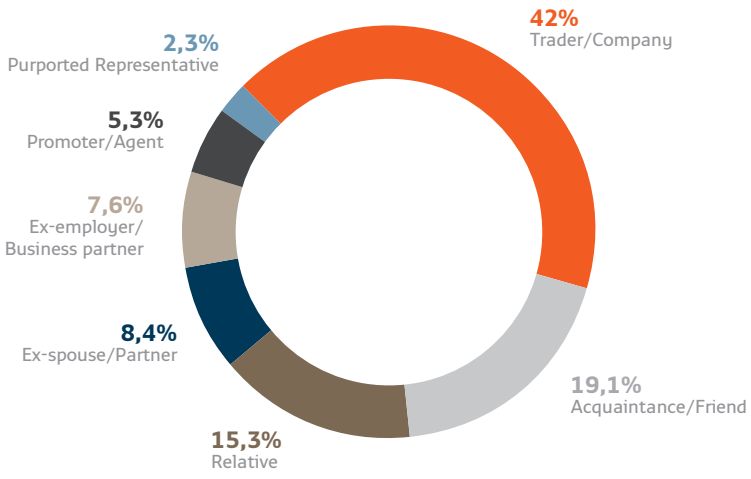
2.
THE IMPACT OF FRAUD

Fraud, be it first-party fraud where an individual misrepresents personal circumstances to secure credit or other financial services, or the more serious threat of fraudsters masquerading as someone else, continues to be a major cause for concern amongst the credit and wider financial services community. The rate of fraud continues to increase and the ways in which it is perpetrated are becoming ever more ingenious and elaborate. This increase is also driven by economic pressures, such as: pay freezes, unemployment and business closures.

2.1 Fraud perpetration and the impact on consumers

Studies by CRIF in Italy, in 2010, found that in only 19% of cases of identity and credit fraud, the alleged fraudster was reported to the police. When the presumed perpetrators of the fraud are identified, in 42% of cases they are traders/shop-keepers, whereas 23.7% of cases involve a relative of the victim. Compared to previous years, a fall in fraud was recorded for fraud carried out by friends or acquaintances, although these still represented 19.1% of the total. It is worth noting the growth in alleged fraudsters in the former employer or business partner category (7.6% of cases).

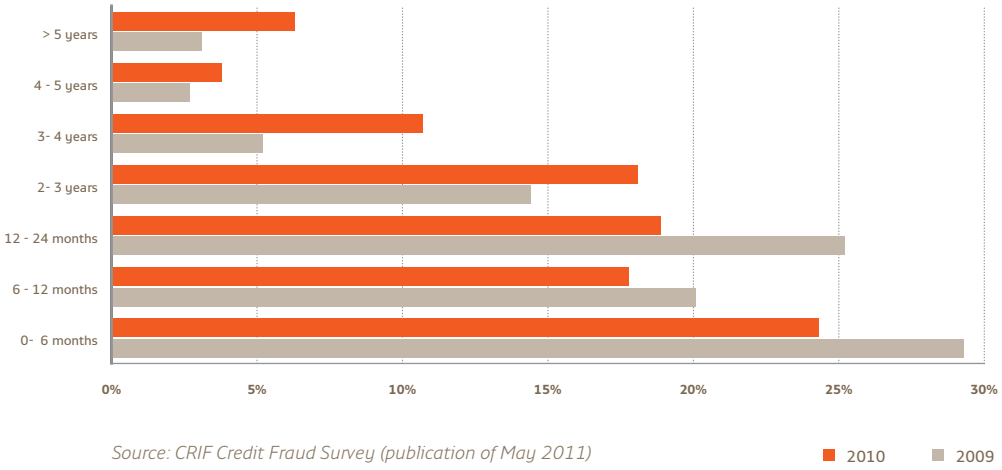
ALLEGED PERPETRATOR OF FRAUD



Source: CRIF Credit Fraud Survey (publication of May 2011)

The time that elapses before a fraud is detected has increased further compared to the previous year. In 40% of cases, fraud victims realised they had suffered fraud 2 years after the credit had been taken out, whereas in 2009 this happened in a little more than 25% of cases. On the other hand, fraud detected within 6 months of the credit being granted fell, with 24% of the total, remaining the most frequent amongst fraud cases.

DETECTION TIME



Source: CRIF Credit Fraud Survey (publication of May 2011)

More specifically, in most cases individuals became aware that they have been the victim of a fraud only after being contacted by the credit institution that granted the credit (around 40% of cases), or when they applied for credit themselves (11%). 11.5% discovered fraud after checking their bank statement.

Fraud negatively impacts consumers, because it may:

- lead to increased costs for all consumers;
- result in the access to certain services becoming more burdensome due to increased security measures (e.g. more extensive ID verification);
- create an aversion towards certain products, services, providers or applied information technology solutions;
- reduce the level of trust that consumers have in a product or service; and
- result in reputational damage for the credit provider.

On a more personal level for individual consumers, it is worth noting that in 2010 the United Kingdom's National Fraud Authority estimated that in very serious cases, it can take consumers up to 200 hours to repair the damage done to their identity. In working hours, this is equivalent to a year's annual leave.[7] Additionally, the impact on the emotional well-being and sense of security of the victims should not be underestimated.[8]

The above highlights the importance for lending institutions to focus on preventing fraud.

7. National Fraud Authority, "Identity fraud costs UK £2.7billion every year", 18 October 2010; available at http://collections.europarchive.org/tna/20110203091302/http://www.attorneygeneral.gov.uk/nfa/WhatAreWeSaying/NewsRelease/Pages/identity-fraud-costs-27billion.aspx

8. CIFAS, "2010 Fraud Trends – CIFAS warns against greeting reduction in fraud too enthusiastically", 20 January 2011, available at: http://www.cifas.org.uk/press_release_twentyeleven_a

2.2 Size of the fraud problem in consumer lending across the European Union

The United Kingdom

In January 2011, the National Fraud Authority reported that fraud costs the UK economy £38 billion a year.[9] Fraud in the public sector amounts to £21 billion, whilst fraud in the private sector amounts to £12 billion. The financial services sector saw the highest losses of the private sector, estimated at £3.6 billion.[10]

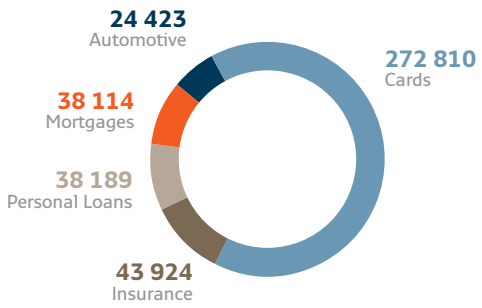
Credit card fraud in the UK in 2010 totalled £365 million according to the UK Payments Administration.[11] 26% of Britons have suffered credit card fraud, and 40% have been subject to a fraudulent takeover of their account.

The Finance and Leasing Association (FLA) reported that in the first three months of 2011 motor finance fraud cost £3.8 million, an increase of 13.8% on 2010.[12] The value of motor finance fraud cases overall in 2010 was £14.6 million,[13] which represents 832 individual cases of motor fraud. According to the FLA, the reduction reflects the commitment of lenders to tackle financial crime and keep credit affordable. Whilst 832 cases of fraud were caught by the checks made by lending institutions, FLA member finance companies prevented over 9 000 cases of suspected or attempted fraud in 2010 and therefore avoided at least £116 million of losses.[14]

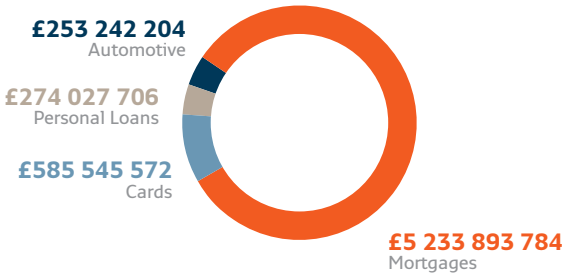
Motor finance companies recovered 40% of all cars acquired through fraud thanks to their own investigations and to partnerships with police forces, including the industry-funded AVCIS Vehicle Fraud Unit.[15] Now in its fourth year, the Vehicle Fraud Unit has recovered over 900 vehicles worth £15.5 million. While government funding for the AVCIS has been cut, the Vehicle Fraud Unit itself is funded by FLA members and can therefore continue to operate.

However, in terms of numbers of instances, as opposed to value, identity fraud remains the UK's most commonly occurring fraud, with over 102 500 cases reported in 2010.[16] The tables below show figures on confirmed cases of fraud and associated savings as reported by the National Hunter[17] membership between 2005 & 2010 (inclusive):

CASES OF FRAUD IDENTIFIED BY SECTOR



FRAUD PREVENTED BY SECTOR (£)



9. At 30 November 2011, the exchange rate stood at € 1.1685 for £ 1.
10. National Fraud Authority, "Annual Fraud Indicator", 27 January 2011, more information available at: http://www.homeoffice.gov.uk/publications/agencies-public-bodies/nfa/fraud-focus-newsletter/fraud-focus-feb11?view=Binary and http://www.homeoffice.gov.uk/agencies-public-bodies/nfa/news/press-releases/fraud-costs-over-38-billion/
11. Financial Fraud Action UK, "Fraud the facts 2011 – The definitive overview of payment industry fraud and measures to prevent it", available at: http://www.financialfraudaction.org.uk/Publications/#/1/zoomed
12. Finance and Leasing Association, "News – Illegal hiring contributes to rise in car fraud", 13 June 2011, available at: http://www.fla.org.uk/media/130611_q1_fraud
13. Finance and Leasing Association, "News – Police car crime partnership keeps down motor finance fraud in 2010", 10 March 2011, available at: http://www.fla.org.uk/media/100311_q4_motor_fraud
14. Finance and Leasing Association, "News – Police car crime partnership keeps down motor finance fraud in 2010", 10 March 2011, available at: http://www.fla.org.uk/media/100311_q4_motor_fraud
15. AVCIS Vehicle Crime Intelligence Service, more information at: http://avcis.police.uk/
16. CIFAS, "2010 Fraud Trends – CIFAS warns against greeting reduction in fraud too enthusiastically", 20 January 2011, available at: http://www.cifas.org.uk/press_release_twentyeleven_a
17. National Hunter is an anti-fraud data sharing system for use by members of the Financial Services Industry.

Germany

A 2006 PricewaterhouseCoopers (PwC) survey of banks and insurance undertakings' experience with economic crime revealed that:[18]

- 63% of German financial institutions experienced 11 cases on average over a two year period;
- Mature financial markets (e.g. Germany and North America) are exposed to higher risks;
- Risks are still underestimated. Only one in five companies was found to assess risk in a realistic manner;
- Embezzlement and fraud cost an average of €2 million per company with a maximum damage per case of €1 million;
- The aggregate of all losses reported over a 4-year period amounted to €255 million;
- More than a quarter of German financial institutions suffered from serious non-material loss (e.g. tarnished reputation, interference of business relations, reduction in staff motivation, etc.).

Two additional PwC surveys dating 2009 and 2011[19] as well as the yearly statistics of the German Federal Criminal Police Office (*Bundeskriminalamt*, BKA)[20] provide further data on the subject. Although a decrease in the number of cases for damages for economic crime have been reported in 2011, compared to 2009, nearly every second polled company (52%) had experienced at least one case. The BKA, on the other hand, published an overall increase in severe economic crimes of 1,5% in 2010 compared to 2009 whereas fraud rose by 5%.

Furthermore, all three publications reported a significant increase in financial damages; for example the average loss per company was €5,57 million in 2009, whereas in 2010 this rose to €8,39 million – a 58% increase.[21] Of all the damages reported to the BKA concerning economic crime, fraud in the asset and finance area made up more than 55% in 2011, a 5% increase.

Finally, from the publications referred to above, it appears that the estimated number of unreported cases is high. The BKA states that its data cannot be interpreted as representing the true extent of business crime. On the one hand economic crimes are often dealt with internally - without the involvement of the police – or by public prosecutors or tax authorities which do not contribute to police statistics. On the other hand, the victims' interests (e.g. the fear of the loss of reputation) appears to lead to only a small number of complaints being reported, due to which a high number of unreported cases may exist.[22]

18. *PricewaterhouseCoopers and Martin-Luther-University, "Wirtschaftskriminalität bei Banken und Versicherungen - Tatort Deutschland 2006", 2006, available at: http://www.business-keeper.com/Docs/Attachements/474b7ac9-60de-4b58-a484-6a6fc449f0bb/Wikri_Banken_Versicherungen-06.pdf*
19. *PricewaterhouseCoopers and Martin-Luther-University, "Wirtschaftskriminalität 2009 – Sicherheitslage in deutschen Großunternehmen", 2009, available at: http://www.pwc.de/de/risiko-management/assets/Studie-Wirtschaftskriminal-09.pdf and PricewaterhouseCoopers and Martin-Luther-University, "Wirtschaftskriminalität 2011 – Compliance im Aufwind", 2011, available at: http://www.pwc.de/de/risiko-management/studie-zur-wirtschaftskriminalitaet-2011-kommissar-zufall-deckt-am-meisten-auf.jhtml*
20. *Bundeskriminalamt, "Bundeslagebild Wirtschaftskriminalität 2010, 2011", page 6, available at: http://www.bka.de/nn_193376/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Wirtschaftskriminalitaet/wirtschaftskriminalitaetBundeslagebild2010,templateId=raw,property=publicationFile.pdf/wirtschaftskriminalitaetBundeslagebild2010.pdf*
21. *PricewaterhouseCoopers and Martin-Luther-University, "Wirtschaftskriminalität 2011 – Compliance im Aufwind", 2011, available at: http://www.pwc.de/de/risiko-management/studie-zur-wirtschaftskriminalitaet-2011-kommissar-zufall-deckt-am-meisten-auf.jhtml*
22. *Bundeskriminalamt (BKA), "Bundeslagebild Wirtschaftskriminalität 2010, 2011, page 6, available at: http://www.bka.de/nn_193376/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Wirtschaftskriminalitaet/wirtschaftskriminalitaetBundeslagebild2010,templateId=raw,property=publicationFile.pdf/wirtschaftskriminalitaetBundeslagebild2010.pdf*

Italy

Quantifying the size of the problem is problematic given that financial and non-financial institutions are reluctant to share data on fraud. Also, fraud can prove difficult to detect in more complex cases such as internal fraud, shell companies or certain distribution channels.

According to a survey carried out by *Il Sole 24 Ore*, identity fraud is on the increase, with almost 25 000 cases of fraud in 2010 and losses in the credit sector amounting to €1.6 - €2 billion in 2009.[23]

Research carried out within the ALIAS project[24] concerning the prevalence of certain types of fraud showed that the level of victimisation of Italian citizens is 2.1% for credit card fraud and 0.56% for identity fraud.

The Netherlands

In the Netherlands, although there is no precise data on the overall size of the fraud problem, the following estimates and figures have been published:

Type of fraud	Size (in €)	Year
Financial Economic Criminality[25]	Between 14 and 17 billion	2009
Skimming fraud[26]	36 million	2009
Skimming fraud[27]	19.7 million	2010
Losses suffered by banks due to internet banking fraud[28]	1.9 million	2009
Losses suffered by banks due to internet banking fraud[29]	9.8 million	2010
Total losses suffered by banks due to fraud in payment transactions[30]	57 million	2010

2.3 Fraud has a significant impact

The above data from various EU Member States provides an indication of the scale of the fraud problem. These figures show that fraud has a significant impact on consumers, lending institutions and the economy at large. It is therefore crucial that all necessary steps be taken to allow the detection, prevention and fight against fraud to be conducted in an effective manner. Effective fraud prevention would result in lower victimisation rates as well as lower cost of credit.

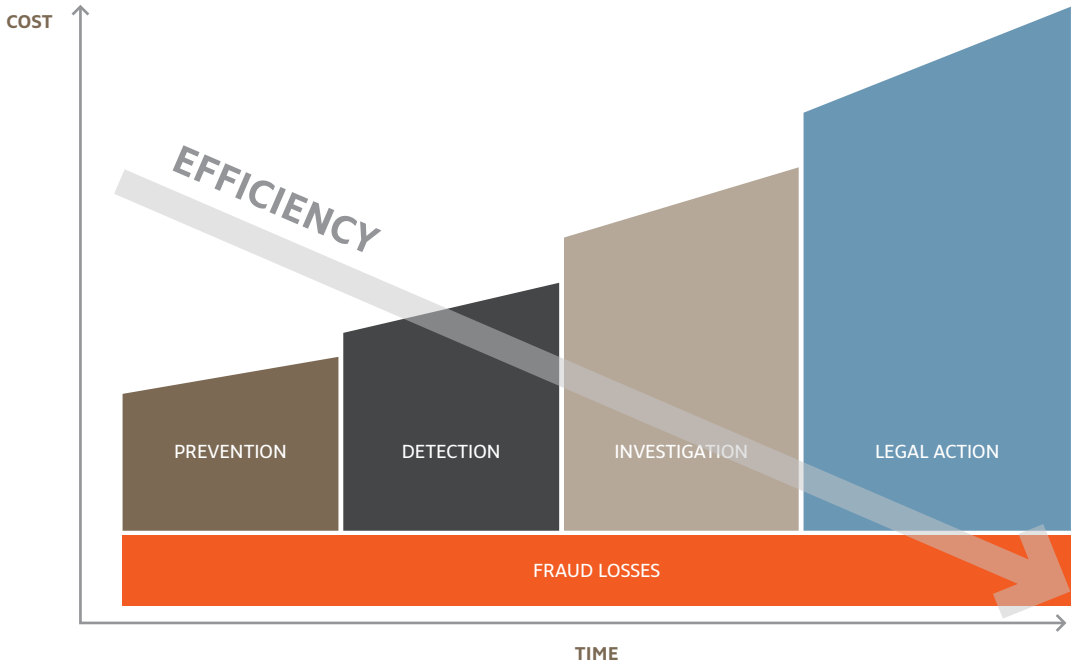
23. Il Sole 24 Ore, "Acquisti e prestiti con falsa identità", 18 August 2011, 29.
24. ALIAS, more information available at: http://www.rissc.it/alias/
25. Grinsven, van. Jürgen H. M., De Groot, Arthur., "Financieel Economische Criminaliteit", in Finance & Control, Kluwer, February 2010, available at: http://www.vangrinsvenconsulting.com/downloads/FEC.pdf
26. Nederlandse Vereniging van Banken, "Jaarverslag 2010", pg 19-20, available at: http://www.nvb.nl/scrivo/asset.php?id=915656
27. Nederlandse Vereniging van Banken, "Jaarverslag 2010", pg 19-20, available at: http://www.nvb.nl/scrivo/asset.php?id=915656
28. Nederlandse Vereniging van Banken, "Jaarverslag 2010", pg 19-20, available at: http://www.nvb.nl/scrivo/asset.php?id=915656
29. Nederlandse Vereniging van Banken, "Jaarverslag 2010", pg 19-20, available at: http://www.nvb.nl/scrivo/asset.php?id=915656
30. Nederlandse Vereniging van Banken, "Jaarverslag 2010", pg 19-20, available at: http://www.nvb.nl/scrivo/asset.php?id=915656

3.
PREVENTING AND FIGHTING FRAUD IN CONSUMER LENDING

Fighting fraud involves multiple steps, from prevention to detection, investigation and in some circumstances legal action. The sooner (attempted) fraud can be detected, the better.

Access to data is required for consumer credit providers to establish whether (attempted) fraud, in any of its forms, has taken/is taking place. Lenders need to be able to verify, for instance, whether documents provided at the application stage are genuine, whether the applicant borrower is employed at the time of application or whether the applicant's purported business is still running. Lenders also need to be able to check whether the submitted documents contain correct information (level of remuneration disclosed, alleged working period, etc.).

Lending institutions have processes in place in order to detect (attempted) fraud. They rely on internal databases (to the extent permitted by law) as well as on existing external databases and public information.



The costs and efficiency of the fighting fraud process over time. Source: Ournext.

3.1 Lending institutions

Lenders have put in place robust internal procedures to fight fraud, such as dedicated training programmes for staff members, rigorous reviews of credit approval processes and continuous internal checks.

Case study: Santander Consumer Bank S.A. (Poland)

One of the measures that Santander Consumer Bank uses to prevent credit fraud is the internal prevention system 'tMAK'. This internal system produces daily alert reports on suspicious credit authorisations as well as weekly alert reports which also contain trends of transactions. The reports are analysed by the Lending Processes Monitoring Team and any non-typical characteristics of the purported fraudulent transaction is then carefully analysed by cross-checking data with other banking systems, such as the complaints' management system.

To prevent fraud, the bank also consults its database of internal restrictions which contains information about persons who committed/attempted to commit fraud and the companies that were used as a tool to commit fraud. The database is used in the credit approval process: any new application found to be linked with information contained in the database is automatically sent for manual verification and decision.

The bank further monitors credit card transactions in order to detect and prevent any credit card related fraud. A system delivered by an external company to operate the credit cards issued by Santander Consumer Bank Poland is used for that purpose. The system enables the generation of daily reports based on pre-defined requirements. As with the tMAK system, these reports show non-typical activities that may give rise to the suspicion of fraud. Reports are analysed by the Lending Processes Monitoring Team on a daily basis. Any suspicious transaction is carefully analysed. If fraud is detected, the credit card is cancelled.

Case study: Société Générale Consumer Finance (France)

In its consumer finance activity, the Société Générale entities are notably concerned by fraud connected with stolen ID and income falsification. In these contexts, one of the key factors of success in fighting fraud is the access to information on identified fraudsters, stolen documents and fraudsters' common practices. Most of the Société Générale Consumer Finance (SGCF) entities build internal databases when possible. They also use existing external databases and lists containing data on known cases of fraud. However, local legislation can sometimes hinder the ability to fight fraud efficiently and quickly.

In addition, SGCF constantly works with its entities in order to define, share and implement best practices in terms of training, procedures, key risk indicators, and last but not least, in terms of fraud detection tools and analysis of cases of fraud. Best practices are centralised and, when relevant, disseminated into local markets.

Main actions implemented at SGCF:

In terms of governance and organisation:

- Centralisation of fraud management in each entity within a specialised department (risk department, debt collection, operational risks for instance);
- Co-ordination with permanent supervision (developing checks to ensure that the alert systems are efficient).

In terms of prevention:

- Prevention/pre-approval checks (including checks between the information provided by the client and the supporting/external documents);
- Comprehensive identification, such as, checking whether the client has been listed as a fraudulent client (internal or external database);
- Analysis of fraud cases (including quantitative and qualitative analysis of actual fraud per month by region, branch, employee, etc.) in order to create conditions for risk mapping;
- Provisioning (e.g. split of fraud provisioning from the credit risk provisioning policy in order to facilitate fraud risk management).

In terms of communication and training:

- Comprehensive communication about fraud to all employees and management in order to develop a culture of awareness and understanding of this risk at operational level;
- Specific development and updating of operational training courses for sales staff;
- Communication with partners on this issue.

The wide variety of retailers and motor dealers involved in the distribution of consumer credit at the point of sale as well as the major differences in their working environments and business models, require lending institutions to deliver retailers and motor dealers highly customised training programs.[31] Lenders themselves are often best placed to provide these. This training is vital in order to adapt to the various fraudulent techniques used at point of sale, which are constantly evolving.

A lender's senior manager is usually responsible for the successful implementation of those training programs. These may comprise of a combination of on-site and online training which includes a focus on how products work and their key features and pre-contractual information (including the Annual Percentage Rate of Charge). In addition, the lender will teach retailers and motor dealers how to spot fraudulent identity or income documents. The lender ensures that the necessary training is always available.

National trade associations and other bodies have also taken initiatives to help fight fraud in consumer credit transactions. These include organised exchanges of information on best practices in fraud prevention within the sector.

Rules and industry guidelines in the United Kingdom

The UK Government takes a prescriptive approach to fraud. A wealth of legislation, guidelines and monitoring bodies has been introduced in order to prevent fraud. Combined, these give financial institutions and consumer lending companies various ways of preventing, identifying and tackling the various types of fraud.

On the one hand, the Financial Services Authority (FSA) Principles are binding on firms. They require firms to conduct their business with integrity and with due skill, care and diligence as well as to take reasonable care to organise and control their affairs responsibly and effectively with adequate risk management. Severe penalties can be imposed on firms where losses have occurred due to inadequate internal rules and risk controls. Furthermore the FSA is currently consulting on the possible introduction of a guide for companies on financial crime, to complement the existing rules.[32]

On the other hand, other official bodies such as the Office of Fair Trading (OFT), the Serious Fraud Office, the UK Payments Administration and the National Fraud Authority, as well as being responsible for investigating and enforcing fraud legislation, also publish guidelines which lenders are encouraged to follow when undertaking consumer (and other) lending and financial dealings. Specific to the asset, consumer and motor finance sector in the UK is the Finance & Leasing Association (FLA) which was formed in 1992 and is the industry representative for Finance Houses in the consumer lending market.

Guidelines set by these bodies include the OFT's "Irresponsible Lending Guidelines" and the FLA's "Lending Code" and "Business Finance Code". These guidelines are complimented by legislation such as the "Money Laundering Regulations 2007", which also aims to prevent identity fraud by ensuring that finance companies thoroughly investigate the identities of new and existing customers on an ongoing basis. Therefore, companies involved in consumer lending have a wide range of guidelines to incorporate into their internal procedures which, if followed, will aid in the limitation or prevention of fraud.

31. For further information on this important topic, please see: Eurofinas response to the European Commission's consultation on responsible lending and borrowing in the EU, August 2009, available at: http://www.eurofinas.org/uploads/documents/positions/Eurofinas%20response%20to%20consultation%20on%20responsible%20lending.pdf

32. Financial Services Authority, "Financial Crime: A guide for firms", June 2011, available at: http://www.fsa.gov.uk/pubs/cp/cp11_12.pdf

3.2 Databases

Fraud in the financial sector is a growing business for fraudsters using increasingly innovative and creative ways of targeting any perceived weaknesses in the credit granting system. Fraudsters have become ever more sophisticated, which means that fraud prevention measures need to constantly evolve to ensure they are capable of handling the threat.

The financial services industry is committed to sharing intelligence as it strives to counter increasing levels of fraudulent applications in all sectors.

Lending institutions have to be able to check the validity of documents, verify the information supplied to them by applicant borrowers and detect inconsistencies. To do this they require access to databases, both public and private (internal and external) initiatives.

It is important to note that consumers themselves can also benefit and utilise this. For example, consumers can request regular copies of their credit file from Credit Reference Agencies, allowing them to verify whether their identity has been fraudulently used to obtain credit.

There are two main types of anti-fraud databases which are used when processing consumer lending applications:

- **Negative data only:** contains known fraud records.
- **Negative and positive data:** contains known fraud records and other data such as previous applications for credit which were not identified as fraudulent at the point of application. These previous applications are used to find anomalies in data between applications which could indicate attempted fraud.

Shared database systems can help companies detect fraud by sharing data on a nationwide basis. However, databases can differ from country to country. Some examples of databases are provided below.

Case study: Combating fraud and criminality in the Netherlands

Since 1990 an antifraud system, currently known as the Information system of the Financial Institutions (IFI), has been in use by banks in the Netherlands. In 2002, as a consequence of the implementation of the Data Protection Directive,[33] the system was broadened through co-operation with insurance companies. This move was duly approved by the supervisory Data Protection Authority (DPA), acting on the basis of Article 20 of the Directive on prior checking. Such prior approval was necessary given that the processing of this kind of data is seen as presenting specific risks for the rights and freedoms of data subjects. The approval was renewed on May 18, 2011.

IFI is based on the registration of incidents which occur within a company or group. An incident is defined as every event that might influence the integrity and security of a financial institution, such as, falsification of invoices, identity theft, skimming, misappropriation of funds, phishing and credit card fraud. Non-insurance financial institutions wishing to participate in this system must be a member of either the Dutch Banking Association (NVB) or the Vereniging van financieringsondernemingen in Nederland (VFN). Almost all banks and finance houses participate in the system. Participants are obliged to assign responsibility to a special security department for the processing of the data. The registration is not restricted to proven incidents as severe suspicions of criminal behaviour are processed as well. This processing must be notified to the DPA.

Continued on next page >

33. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 23.11.95, L 281/31, hereafter: "Data Protection Directive".

> Continued (Combating fraud and criminality in the Netherlands)

Under described conditions, the data necessary to identify a data subject is stored in a database, which is accessible to all financial institutions participating in the system. The conditions are:

- it must be sufficiently clear that the incident has taken place;
- the incident must in principle be reported to the police or the justice department; and
- a proportionality check is to be made in order to ensure that privacy is not breached in a disproportionate manner.

This system can be checked by the departments of the participating financial institutions that are responsible for accepting (new) clients and staff. The result of a check is either a 'hit' or a 'no-hit' depending on whether it matches the data of an incident contained in the system. The financial institutions do not see the data itself. In the event of a hit the security department of the primary source must be contacted in order to verify that it is the same person and that all the conditions are met.

IFI can be considered as a reliable common system to combat fraud and criminality. Having obtained the prior approval of the DPA, it is recognised that there are no legal obstacles to the exchange of personal data between the participants. However, some problems remain on an operational level as not all institutions use the system when checking data. Also, the exchange of data between banks and insurance undertakings is not optimal due to a lack of compatibility of the systems of the two sectors.

Italy

While a variety of sources are available in the Italian market for verifying and certifying identity, lenders are nevertheless required to invest heavily in IT and information sharing.

In Italy there are three different credit registers. Two are positive and negative (CRIF and Experian) and one is negative only (CTC).

With regard to public sources of data a number of specific tools to prevent fraud in consumer lending exist. These are:

- A free online tool made available by the Italian Revenue Agency[34] which allows institutions to verify whether a fiscal identification code (series of letters and numbers which unequivocally identify an individual) and a person's identity correspond.[35] An enhanced version will soon be made available to banks;
- The 'Antifraud Central Office on Payment Methods'[36] which has a strategic role in fraud prevention as it allows the sharing of information on possible or ascertained cases of payment fraud;[37]
- A database concerning lost and stolen identities, managed by the Ministry of Internal Affairs; and
- A credit card fraud database, managed by the Ministry of Economy and Finance.

On an administrative level, a legislative decree was recently approved by the Ministry of Economy and Finance[38] which will establish a system that can be used by financial institutions and telecommunication companies. It will be based on the following:

- Interconnection of public administration databases (Ministry of Internal Affairs, Revenue Agency, Social Security Agency, Government Printing Office and Mint) allowing for identity certification;
- A centralised information form, containing anonymised data, established to monitor fraud under specifically defined guidelines; and
- Alerts of suspected or confirmed cases of fraud.

This system is expected to be operational in 2013 at the earliest. While it could prove particularly helpful in verifying customer identity, it will have some limitations:

- The system will not be accessible to all those with an interest in preventing identity fraud (e.g. the entities fighting against organised crime);
- The system will not aim at preventing money laundering and it can therefore not be used for financial transactions that do not involve the granting of credit (such as credit transfers, checks, opening of current accounts); and
- The system will not allow for the interconnection with credit registers.

34. Agenzia delle Entrate.
35. Decree-law n. 78/2010.
36. Centrale antifrode dei mezzi di pagamento.
37. Law n. 166/2005.
38. Legislative decree n. 64, 11 April 2011.

The United Kingdom

Finance companies contribute to various national databases which can be publicly accessed to verify transactions. Examples include: the HPI Register (non-statutory) which is a searchable record of all vehicles subject to registered finance agreements which is designed to prevent vehicle fraud, the Motor Insurance Database to help prevent insurance fraud and the availability of Consumer Credit Reports to establish customer identity and creditworthiness. Information sharing and suspicion reporting to authorities as well as implementing internal procedures remain the two main methods of preventing fraud in the UK consumer lending market.

Two of the main anti-fraud databases are as follows:

- *CIFAS* is a negative only database, and contains records of fraud identified by the members. CIFAS information is distributed to lending institutions through the three UK credit bureaus and other anti-fraud solution suppliers. A flag to indicate a match to a CIFAS fraud record is returned when an application for credit is made to alert the lender to fraud risk. This must then be reviewed to ascertain whether it is valid or not. CIFAS is a not-for-profit organisation funded by its members.
- *Hunter* is hosted by Experian and is split into 3 different sectors, National Hunter (Financial Services), Telco Hunter and Insurance Hunter. Hunter is a negative and positive database: it contains known cases of fraud and previous applications for credit which were not identified as fraudulent. Hunter works by matching new applications for credit against both non-fraud previous application records and known fraud records using a sophisticated set of matching and anomaly detection rules. Rules triggered are returned for investigators to view and investigate. Identified cases of fraud are shared by simply flagging that the application record contains fraud, ensuring a quick protection against fraud for the membership.

Both of these databases are closed user groups which operate on a reciprocal basis. Both systems are audited on an annual basis to ensure compliance with the rules and obligations of membership.

Germany

A variety of tools exist in Germany, including:

- The Hinweis Informationssystem (HIS) of the German insurance industry (which has existed in different forms since 1993) in which insurance undertakings exchange information about persons and assets (mostly cars) which have been identified in fraudulent or suspicious cases throughout the course of investigations of claims.[39]
- The Fraud Prevention Pool of the telecommunications companies in Germany, which is a database containing information on customers' payment behaviour and use of telecommunications facilities.
- The Fraud Prevention Network (FPN), a joint initiative of the German credit industry and credit bureau SCHUFA. The FPN is a centralised database organised by an independent intermediary acting as an enquiry agency. It will contain information on fraud and suspected fraud in the field of identity theft, creditworthiness fraud (forged statements of income, forged bank statements, etc.), fraudulent payment transactions and embezzlement. The FPN is not yet operational as the relation between the provisions of the data protection legislation and specific regulations applicable to banks must first be clarified.

39. More information available at (both in German):
http://www.informa-irfp.de/de/index.html and
http://www.informa-irfp.de/de/onlineservice/hufigefragen/index.html

4.
DATA PROTECTION OBSTACLES FACED WHEN FIGHTING FRAUD

4.1 The EU legislative framework on data protection

As explained in the previous sections, the access to, as well as the storage, exchange and retention of personal data are essential for the detection and prevention of fraud.

Within the EU the processing of personal data is covered by Directive 95/46/EC on data protection (the "Directive).[40]

The Directive aims at guaranteeing the free flow of data within the EU and sets out a number of criteria for making data processing legitimate. Member States may, in certain circumstances, further determine the necessary conditions for data processing.[41]

Member States had to transpose the Directive into their national laws by 24 October 1998. The Directive is currently being reviewed by the European Commission.[42]

Key concepts of the Directive

Personal data is defined in the Directive as any information relating to an identified or identifiable natural person, whereby an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Data processing encompasses the collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, etc. of personal data.[43]

With regard to consumer lending this means that all information provided by an (applicant) borrower can only be processed in accordance with the rules laid down in the Directive.

40. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 23.11.1995, L 281/31.
41. Article 5, Data Protection Directive.
42. Communication from the Commission to the European Parliament, The Council, the Economic and Social Committee and the Committee of the Regions: A comprehensive approach on personal data protection in the European Union, COM(2010)609, available at: http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf
43. Article 2(b), Data Protection Directive.

General rules on the lawfulness of the processing of data

The Directive requires Member States to provide in their national laws that personal data must be:

- processed fairly and lawfully;
- collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;
- adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which is inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, is erased or rectified; and
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data was collected or for which it was further processed.

It should be noted that in the United Kingdom, the Court of Appeal of England and Wales has taken the view that "fairness" of data processing requires consideration of the interests of not only data subjects, but also of data controllers.[44]

Criteria for making data processing legitimate

Under the Directive, personal data may be processed only if:

- the data subject has unambiguously given his consent; or
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
- processing is necessary for compliance with a legal obligation to which the controller is subject; or
- processing is necessary in order to protect the vital interests of the data subject; or
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data is disclosed; or
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data is disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection.

Certain personal data, such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or concerning health or sex life, may not be processed unless certain additional, strictly defined conditions are met.[45]

Exemptions and restrictions: data relating to offences, criminal conviction or security measures

Member States may adopt[46] legislative measures to make data processing more flexible by restricting the scope of some of the principles laid down in the Directive when this is a measure necessary for, for example, the prevention, investigation, detection and prosecution of criminal offences.[47]

As data protection is enshrined as a fundamental right in the EU, any derogation of this right must be subject to a strict interpretation and requires that there is a pressing social need involved and that the measures employed are necessary and proportionate to the legitimate aim pursued.[48]

44. Johnson v Medical Defence Union [2007] EWCA Civ 262 at paragraph 62, available at: http://www.bailii.org/ew/cases/EWCA/Civ/2007/262.html
45. Article 8, Data Protection Directive.
46. Some Member States have adopted specific legislation in this respect.
47. Article 13(1), Data Protection Directive.
48. EU Fraud Prevention Expert Group Subgroup on Data Management, Report from the Secretariat, 8 December 2006, 3, available at: http://ec.europa.eu/internal_market/fpeg/docs/fpeg_data%20management_reportsecretariat_final.pdf and Joined Cases C-465/00 Rechnungshof v. Österreichischer Rundfunk and o., C-138/01 Christa Neukomm and C-139/01 Joseph Lauermann v. Österreichischer Rundfunk of 20 May 2003.

Notifications and prior checking

In principle, lending institutions or any other organisation or body (the data controller) shall notify their Data Protection Authority before carrying out any wholly or partly automatic processing operation.[49]

This notification shall include, at least, the identity of the data controller, the purpose of the processing, a description of the personal data that will be processed, recipients to whom the data may be disclosed, any proposed transfers of data to countries located outside the European Union and a description of the measures taken to ensure that the security of the processing can be ensured.[50]

Upon receipt of the notification, the DPA must determine whether the processing operations to be carried out are likely to present specific risks to the rights and freedoms of data subjects. They must also ensure that the contemplated operations are checked prior to the start of the sought after processing.[51]

Safeguards for individuals

On top of the above-described *ex ante* controls, individuals are entitled to receive from data processors a certain amount of information, especially regarding their right to access the data and to object to the processing thereof. This ensures a high level of protection for individuals and their personal data, whilst allowing effective data processing for legitimate purposes.

4.2 Data protection obstacles

Despite the European framework on data protection having the dual objectives of ensuring the protection of individual's personal data and guaranteeing the free movement of such data, many obstacles exist and remain which restrict lending institutions' ability to effectively fight fraud.

One of the main obstacles to setting up anti-fraud databases are the strict conditions for personal data processing imposed at national level and the very divergent ways Member States have interpreted and transposed the Directive.

Access to data

While, as explained above, lenders may have access to a variety of data, this differs significantly from country to country. Access to different types of data would help lenders significantly in their fight against fraud. Yet national data protection legislation does not always allow this.

Access to public sector data such as address details, income, employment, document identifier numbers and social security numbers would allow lenders to verify the information provided by the applicant borrowers and help prevent identity theft. The sharing of data for fraud prevention purposes between public sector organisations as well as between the public sector and the private sector has proved a real challenge (if not impossible) in a number of Member States.

In the United Kingdom, to try and overcome this, the Government has created the concept of Specified Anti-Fraud Organisations (SAFO). These are government accredited organisations which can share data between public and private sectors for fraud prevention purposes. The accreditation criteria relate to security and controls for data sharing. This accreditation and the management of standards regarding SAFOs is fairly loose, and could be more tightly administered to create formal "Anti-Fraud Agencies".

49. Article 18, Data Protection Directive.
50. Article 19, Data Protection Directive.
51. Article 20, Data Protection Directive.

Data sharing

The cases of fraud discussed above, and the way they are dealt with by lending institutions, should be distinguished from the official prosecution by the national enforcement authorities. Lenders rarely have a prior conviction on the ground of which the sharing of fraud data could be justified.

In the UK, data sharing of detected cases of fraud that have not been convicted is however allowed, as long as the contributor of the fraud data to the sharing pool can satisfy a "burden of proof". This essentially means that they would be confident of a conviction if they were to prosecute.

To support this, fraud data sharing systems generally record a reason for filing the data, which allow the organisation submitting the record to record why the person/record is fraudulent. These reasons for filing are generally directly related to the three categories contained in the UK Fraud Act.

Obtaining authorisation from Data Protection Authorities

In some countries, such as the Netherlands (see p.20-21) and the United Kingdom, permission has been obtained from the DPA to operate anti-fraud databases. This approval by the DPA is a *sine qua non* for setting up and running such databases.

United Kingdom

The Data Protection Act in the UK has a number of sections which allow exemptions for certain reasons such as the prevention and detection of crime and for matters of national security which allows agencies to access personal data upon the provision of the correct documentation. This, and the information commissioner's endorsement on types of data sharing to combat fraud, means protocols for storage and exchange of data are agreed.

For private sector credit applications, application forms (verbal or written) contain a clause which relate to the processing of the data and the fact that it may be shared with fraud prevention agencies, which the customer has to agree to before the application can actually be processed. This is known as a Fair Processing Notice or FPN. Experian and the National Hunter data sharing system store the data securely in designated data sets. Information is matched and then shared only where specific rules are triggered. There are two arrangements available for controlling how and when data is shared:

Reciprocal sharing – When a rule is triggered affecting data across more than one lender, each lender is informed that the rule has triggered. So, if a rule involved an anomaly between a new application for lender A, and previous applications for lending institutions B and C, each of A, B and C will be aware that the rule has triggered. National Hunter (financial services) and Insurance Hunter operate in this way.

Non-reciprocal sharing – When a rule is triggered affecting data across more than one lender, only the lender who has received the new application is aware of the rule triggering. Other lenders whose previous application records may have been involved in causing the rule to trigger are not made aware that the rule has triggered. Experian's Detect fraud system is an example of this type of reciprocity.

In other countries, such as Ireland, obtaining the approval of the Data Protection Authority has proved impossible so far.

Ireland

In Ireland it has proved impossible to create a fraud prevention data sharing schemes equivalent to the existing UK scheme, due to the way the Directive has been interpreted and transposed into Irish law.

Section 8(b) of the Irish Data Protection Acts permits the disclosure of personal data for the purposes of "preventing, detecting or investigating offences, apprehending or prosecuting offenders". However, the Office of the Data Protection Commissioner has expressly stated, following an investigation of the use of data sharing in the context of insurance fraud, that section 8(b) can only be relied upon by a law enforcement authority.[52] The Irish Acts would need to be amended by ministerial extension to permit data sharing between data controllers in relation to the commission of an offence or alleged commission of an offence. This has not been achieved thus far. In these circumstances, the Irish Data Protection Commissioner has advised that information about insurance claims can only be shared if the individual has explicitly consented or following the receipt of a court order.

Consent

The Data Protection Directive lists a number of conditions that have to be fulfilled in order to make the processing of data legitimate,[53] one of which being that the data subject needs to have unambiguously given his consent for his data to be processed. This can lead to a, somewhat absurd, situation where a fraudster's consent is required in order to process his data to prevent further fraud.

Data retention

Data retention periods can vary between organisations and systems. It needs to be possible to store data for a long enough period of time, so that this data can be cross-referenced with new credit applications. It should also be noted that in addition, data needs to be recent enough (e.g. < 12 months) to provide a benefit when identifying fraudulent applications.

52. Irish Data Protection Commission, Twenty-Second Annual Report of the Data Protection Commissioner 2010, available at: http://www.dataprotection.ie/documents/annualreports/2010AR.pdf
53. Article 7, Data Protection Directive.

Interaction of data protection legislation with other legislation

In some Member States where rules are in place to allow data sharing to prevent fraud, these conflict with other legislation, thereby rendering the practical implementation of fraud databases impossible.

Germany

The German Banking Act (KWG) requires credit institutions to operate and update appropriate IT systems to allow them to identify business relationships and individual transactions in payment operations that appear dubious or unusual in the light of knowledge available publicly or within the credit institution on money laundering methods, terrorist financing and fraudulent acts. Where such circumstances are identified, they must be investigated in the context of the current business relationship and individual transactions in order to be able to monitor and assess the risk involved in the relevant business relationships and transactions and, if necessary, examine whether there are grounds for suspicion.

The credit institutions may collect, process, use and share with other credit institutions personal data insofar as this is necessary to fulfil this duty. The recipient may use the information solely for the purpose of preventing money laundering, terrorism financing or other criminal acts and subject to conditions to be laid down by the German Federal Financial Supervisory Authority (BaFin).

In practice, however, credit institutions cannot share this data until it is clarified that the Banking Act overrules the Data Protection law and that it is in the general interest to avoid harm to the financial institutions and their customers.

Furthermore, it is not clear what kind or which parts of the data protection law have to be followed even in a clear case of fraudulent activity (e.g. notification of the person concerned in case of sharing data or reporting to a fraud prevention data base).

It is therefore important in that context that the relationship between the regulatory requirements of special laws such as the KWG and data protection legislation be clarified.

Cross-border implications

The problems and consequences of the various interpretations and transpositions of the Data Protection Directive into the national laws of the Member States are magnified when it comes to cross-border fraud prevention.

While it is difficult to access data that could help detect and prevent fraud from occurring in consumer lending at national level, it can be impossible to achieve it in a cross-border context.

Often consumer credit providers do not have access to foreign databases for the purpose of fighting fraud; and when they do, the concurrent application of more than one national law[54] makes it difficult, if not impossible, for them to proceed and prevent fraud without fear of being in violation of existing data protection laws.

54. EU Fraud Prevention Expert Group Subgroup on Data Management, Report from the Secretariat, 8 December 2006, pg 3, available at: http://ec.europa.eu/internal_market/fpeg/docs/fpeg_data%20management_reportsecretariat_final.pdf

5. RECOMMENDATIONS

The data presented in this report has shown that the size of the fraud problem is significant and that fraud can have a detrimental impact on society. To address this, efficient and effective solutions need to be put in place to prevent and detect fraud. Eurofinas and ACCIS feel that fraud prevention and detection should be high up on the agenda at both European and national level.

As within the consumer lending industry, detecting and preventing fraud requires access, sharing and storage of personal data in order to detect potential cases of fraud, we consider that this issue can be addressed by the European institutions in the framework of the ongoing review of the Data Protection Directive.

The current Directive, as implemented into the national laws of the Member States and interpreted by data protection authorities, does not always allow the processing of personal data for the purpose of fraud prevention and detection. As the protection of personal data is a fundamental right, any processing of data can only take place under strict legal conditions. Procedural safeguards are in place to protect consumers from the unlawful processing of their personal data.

Given the impact fraud can have on the individuals affected by fraud, on the lending institutions as well as on the economy and society at large, data processing - such as data access, sharing and storage - for the purpose of fraud prevention and detection should be considered a legitimate purpose within the framework of data protection legislation. The future EU framework for data protection should include a specific reference to fraud prevention and detection, **explicitly recognising processing of data for that purpose as legitimate.**

Ensuring a high level of data protection within the EU will be a key objective in the future framework. The explicit inclusion of fraud prevention and detection as a legitimate purpose will not detract from this. Any processing for this purpose will still have to fulfil the other legal requirements contained in the data protection framework. Any processing, even for the legitimate purpose of fraud prevention and detection, should always be for a specified and explicit purpose, the processing should be adequate, relevant and not excessive and the data processed should be accurate and up-to-date. This goes hand in hand with the provision for consumers to have inaccurate or incomplete data rectified or erased as appropriate.

The formal inclusion of fraud prevention and detection as a legitimate purpose would, in our view, greatly contribute to resolving national divergences that have been observed following the implementation of the 1995 Data Protection Directive. In this context, we also consider that the future framework should focus on targeted high level principles. A targeted full harmonisation approach will take into account the diversity of national specificities across various EU Member States, whilst still creating a level-playing field. If a targeted full harmonisation approach is not adopted, this will inevitably lead to further regulatory inconsistencies across the national markets and an incoherent data protection framework for both consumers and businesses.

Furthermore, the sharing of information between the public and private sector is of crucial importance for the effective prevention and detection of fraud. As shown in this publication, various levels of co-operation exist across Member States. Plenty of opportunities remain for initiatives and co-operation to be established between public and private bodies. Whilst we consider that this can hardly be addressed within the European data protection framework, we would nevertheless like to highlight the importance of such co-operation. The commitment of public authorities to help the fight against fraud and their willingness to provide lending institutions and credit bureaus with the necessary, appropriate tools to achieve our common goals in this field, are essential.

Eurofinas and ACCIS call on policy makers to:

1. Recognise fraud prevention and detection as a legitimate purpose for data processing

2. Adopt a targeted full harmonisation approach in the future EU framework on data protection

3. Encourage public-private data sharing further.

Eurofinas and ACCIS remain at policy makers' disposal to actively participate in, and contribute to, future work on these issues.

Responsible Editor:
Anne Valette, Head of Communications, Eurofinas

Editors:
Anke Delava, Legal Adviser, Eurofinas
Piero Crivellaro, Public Affairs Manager and
Laura Reginato, Public Affairs, ACCIS

Contact:

Eurofinas AISBL
Boulevard Louis Schmidt, 87 | B-1040 Brussels
www.eurofinas.org

ACCIS
Rue Defacqz 52 | B-1050 Brussels
www.accis.eu

Published by Eurofinas and ACCIS - December 2011

eurofinas

SPECIALISED CONSUMER CREDIT PROVIDERS IN EUROPE

EUROFINAS
Boulevard Louis Schmidt 87
1040 Brussels – Belgium
T +32 2 778 05 60
www.eurofinas.org

ACCIS
Rue Defacqz 52
1050 Brussels – Belgium
T +32 2 536 86 76
www.accis.eu

Publication date: December 2011