Eurofinas Conference on Fighting Fraud in the Consumer Credit Industry

Summary notes

eurofinas

4 NOVEMBER 2016

Radisson Blu Royal Hotel
Brussels, Belgium

www.eurofinas.org

ABOUT EUROFINAS

Representation at EU level

Eurofinas, the European Federation of Finance House Associations, is the voice of consumer credit providers in Europe. As a Federation, Eurofinas brings together associations throughout Europe that represent consumer credit providers. 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 more than 423.1 billion Euros worth of new loans during 2015 with outstandings reaching 981 billion euros at the end of the year.

What is consumer credit?

Consumer credit enables people to purchase goods or services for personal or household purposes. It is a vital tool to finance individuals or households' needs and projects. Vehicles, higher education, home repairs are examples of assets and services financed by consumer credit.

More information at www.eurofinas.org

CONTENTS

eurofinas

SPECIALISED CONSUMER CREDIT PROVIDERS IN EUROPE


Luxem
bourg


finas

FOREWORD

Valentino Ghelli
Eurofinas Chairman

As is clear from the recent research Eurofinas jointly produced with Roland Berger, our economy is increasingly digital. The digitalisation of consumer credit means that the nature and aspects of fraud that our industry face up to are changing.

Risk awareness and early prevention undoubtedly prove to be a significant challenge for our industry. This is why Eurofinas decided to organise a dedicated event to better understand the dynamics of fraud in our markets through real case studies.

The seminar helped participants to identify opportunities and brainstorm on tomorrow's challenges. It was also an occasion to better understand the future of the European data protection regulatory framework and its impatc on the fight against fraud.

I am very grateful to Experian and Xperta who sponsored this event. They are a strong and committed group of people serving the industry and their support was vital to the success of the seminar.

Eurofinas is strongly committed to support the industry in its work on fraud detection and prevention.

SESSION 1
INTRODUCTION
SETTING THE SCENE

Digitalisation is creating massive business opportunities for growth. By 2020, it is estimated that there will be 33 billion active devices worldwide, i.e. four for every person.

Customers are also changing. Tomorrow's core customers, so-called „millenials", are digital natives and widely prefer digital transcations through mobile devices. This brings new challenges to retain and attract customers.

The estimated total annual fraud loss in the United Kingdom is of 282 billion dollars.

ANNUAL FRAUD LOSS IN THE UK 282 BILLION DOLLARS =

20% CLEAN WATER FOR THE ENTIRE PLANET

40% END WORLD HUNGER ACCORDING TO UN

60% BUY TWO THIRDS OF FACEBOOK

> "Since 2000, three-quarters of retail sales growth has occurred through online channels"
>
> PWC JULY 2015

Our industries strongly rely on customers to secure their various online activities (Facebook, PayPal, Uber, etc.). It is estimated that an individual holds 26 online accounts of various sorts but only five different passwords. It is therefore easy to obtain valid data and fraudsters now value data customer accounts more than credit cards.

What is the impact of data breaches? Experian projections based on historical breached data studies from Rand Corporation, Javelin and in-house data, shows that 1 in 12 existing accounts is at risk of attack and 1 in 10 new applications may be an imposter using breached data.

> "Mobile is already the largest banking channel by volume of transactions for majority of banks"
>
> KPMG GLOBAL RESEARCH JULY 2015

It is vital to understand the total cost of fraud in terms of direct losses but also in terms of management costs, lost revenue and lifetime customer value.

THE WAY TO WIN THE WAR

KNOWN CUSTOMER DATA ↓ | TRANSACTION & CONTEXT ↓ | DIGITAL BEHAVIOURS ↓

ADVANCED ANALYTICS ↓

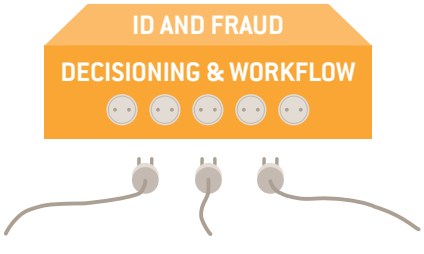
ADVANCED TECHNOLOGY ↓

INCREASED CUSTOMER TRUST | INCREASED REVENUES | REDUCED FRAUD LOSSES | REDUCED TOTAL COST OF FRAUD

A cross core solution needs to be deleveloped to manage strategy at the pace of fraudsters.

CROSS CORE:
MANAGE STRATEGY AT THE PACE OF FRAUDSTERS

> Integrated "plus and play" platform
> Define the level of confidence required at a transaction level
> Optimise decisions across services



EXPERIAN ID & FRAUD SOLUTIONS | THIRD PARTY SOLUTIONS | CLIENT'S OWN SOLUTIONS

CRÉDIT AGRICOLE CONSUMER FINANCE

CRÉDIT AGRICOLE CONSUMER FINANCE (CACF)

THE ROLE OF BIG DATA IN THE FIGHT AGAINST FRAUD

* 71.2 billion EUR outstandings
* 9800 employees, of which 3400 in France
* Serving more than 10 million customers in 21 countries

THE NETHERLANDS	FRANCE	GERMANY	PORTUGAL	ITALY	MAROCCO
CACF NETHERLANDS	CACF FRANCE	CREDIT PLUS BANK	CREDIBOM	AGOS	WAFASALAF
2.7 BN €	25.8 BN €	2.6 BN €	1.1 BN €	15.2 BN €	2.5 BN €

Fraud covers a wide range of behaviours and malpractices ranging from false statement to the use of forged documents and identity theft. Implications for lending institutions are important in terms of financial loss and customer protection. The fight against fraud is also a key aspect of the sector's social responsibility.

KEY FIGURES

90% OF FRAUD ATTEMPTS ARE
DETECTED BEFORE FINANCING

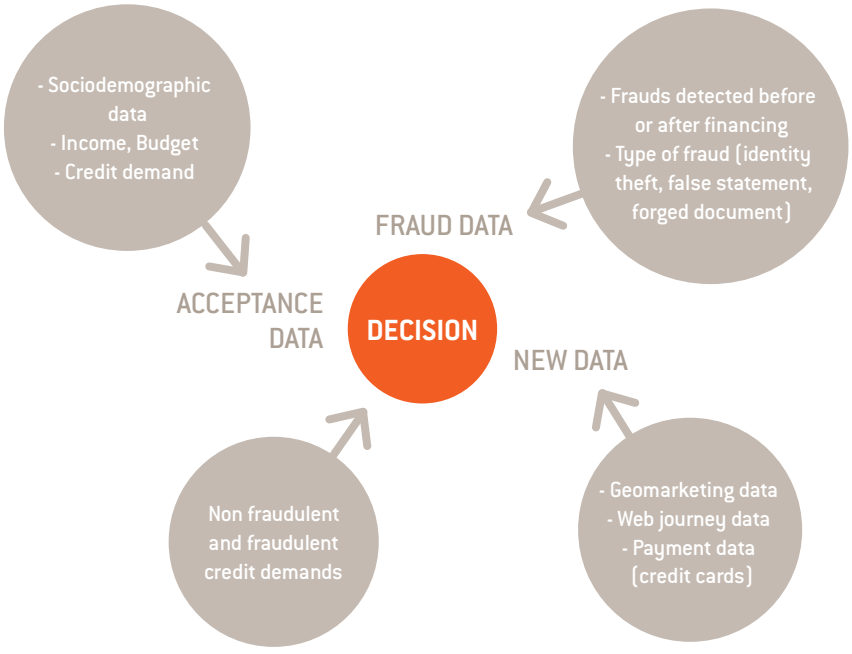
2/3rd OF FRAUD ATTEMPTS ARE
DETECTED THANKS TO HUMAN EXPERTISE

ID THEFT IS A GROWING CONCERN
AND NOW REPRESENTS
2/3rd OF FRAUD ATTEMPTS

THE CACF PROJECT

BIG DATA OPTIMISATION

CACF developed a fraud detection model using machine learning techniques and new predictive data. CACF worked together with a start-up specialised in data analytics. A key priority was to put in place a system which could be easily implemented and industrialised at an acceptable cost.



KEY FINDINGS AND TAKEAWAYS

THE **25%** RISKIEST CREDIT REQUESTS → ACCOUNT FOR **74%** OF THE FRAUD

Some of the variables identified include:

> SOCIAL-PROFESSIONAL GROUP

> EMAIL PROVIDER

> ZIP CODE

The group managed to implement a successful first model under a short period of two months and at a limited cost. The model shows good performance and stability. Next steps include further implementing the model, identifying new predictive data that are currently not as well as adapting the IT and internal governance.

BASISBANK

ID FRAUD IN A DIGITALISED ENVIRONMENT

* 230 million EUR outstandings
* 70 employees serves 75.000 customers
* Basisbank was established in 2000 as an internet bank with no up-front branches

In Denmark, fraud has considerably evolved. Digitalisation stopped the most common and small-scaled types of fraud such as the falsification of pay slips or ID theft.

This is because digital ID as well as the digitisation of official documents make it very difficult to take someone else's place – at least it would require substantially more resources and technology. ID theft is now almost a result of negligence for example by storing together a username and password or sharing personal data with an ill-intentioned partner or child/grandchild.

Fraud schemes nevertheless became larger in scale, more brutal and increasingly related to organised crime.

EXAMPLES OF REPORTED CASES INCLUDED

1. LURED INDIVIDUALS TO DENMARK WITH PROMISES OF JOB

> Forced them to handover Digital ID
> Committed almost every single fraud they can benefit from
> Sent them back home or to work without paying tax

2. AN ERROR IN THE POPULATION REGISTER SYSTEM LED TO THE DELETION OF ALL INFORMATION RELATED TO AN INDIVIDUAL'S ADDRESS WHEN HE/SHE WAS MOVING BACK TO HIS/HER COUNTRY OF ORIGIN

> Foreign residents "moved" their address to vacant flats in Copenhagen
> Took out loans
> Population register canceled their relocation

SOLUTIONS/RED FLAGS

01 Real-time application stability alert
02 Geo location warning (for example where geo location does not correspond to work or home address)
03 IP address used on multiple applications
04 IP address flagged as dubious
> Has open WiFi
> Dubious ports open
> ISP uses routers that are compromised

GOING FORWARD

> Digitalisation prevents most common fraudulent behaviours
> New fraud patterns are without borders and vicious
> As many fraudulent applications have similar characteristics, they are now processed manually
> An identity theft register is required to fight against phishing / large scale identity theft

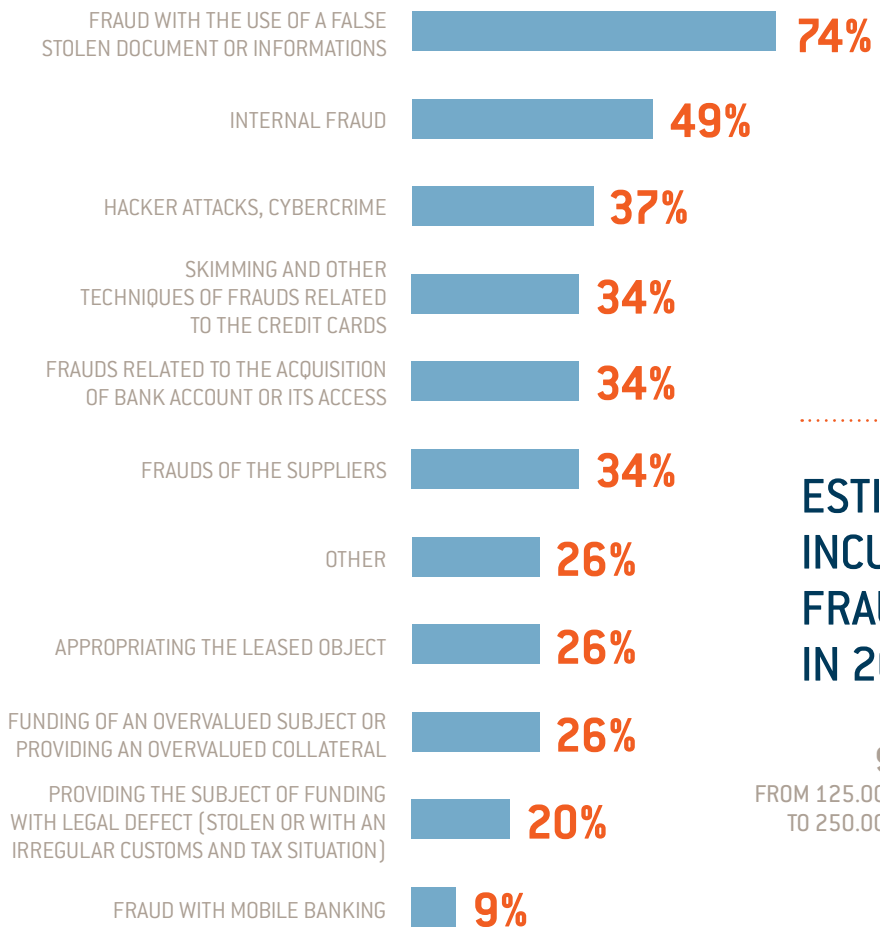
SESSION 2

KPF

FRAUD TRENDS

* Established in 1999, KPF brings together more than eighty financial institutions from the Polish financial sector including banks, advisors, financial intermediaries, loan institutions, repositories of economic and credit information, reverse mortgage and insurance providers.

MOST COMMON TYPE OF FRAUD EXPERIENCED

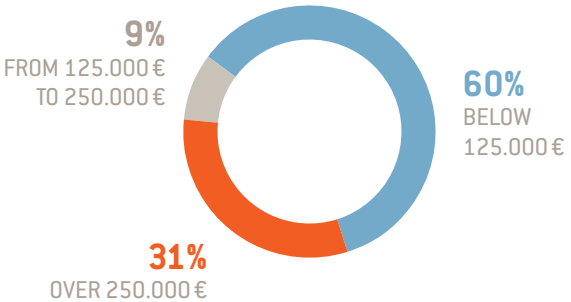


KPF, with the assistance of Ernst and Young (E&Y), has been conducting a survey on fraud in the financial services sector in Poland for six consecutive years.

The latest results of the joint research suggest that the sector is experiencing an increase in fraudulent activities[1]. Financial losses due to fraudulent activities however vary. Exact losses are likely under-estimated as they do not consider indirect implications such as reputational damage.

In Poland, the most commonly encountered type of fraud also relates to the use of falsified and/or stolen documents.

ESTIMATED TOTAL LOSS INCURRED AS A RESULT OF FRAUDULENT ACTIVITIES IN 2015



1. *"Investigating Fraud in the Financial Service Sector 2016"*

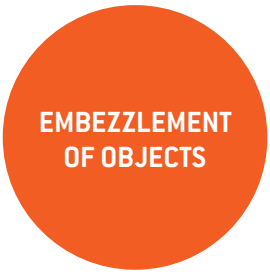
SOCIETE GENERALE IBFS

GLOBAL FRAUD PREVENTION

* 71 billion EUR outstandings
* 148,000 employees
* 32 million customers

International Retail Banking and Financial Services (IBFS) combines the services of the international banking networks and consumer finance activities of the group. The consumer finance activities are centralised around eight countries for nine entities and offer classical consumer credit, revolving cards, motor and boat finance, stock financing / floor plan, leasing and mortgage loans.

The two most common forms of fraud encountered within consumer loan entities relate to identity theft and embezzlement of objects.



The consumer credit activity of the group includes different entities active in various countries, such as CGI in France, FidItalia in Italy, Rusfinance in Russia and Eurobank in Poland. A striking feature of the IBFS' fraud prevention strategy is to support dedicated fraud prevention teams within each local consumer credit entity.

To capture local specificities and fraudulent patterns, each entity develops a dedicated strategy to detect and prevent fraud.

ORGANISATION

REGULAR MEETINGS BETWEEN FRONT OFFICE AND BACK OFFICE

SINGLE GROUP FRAUD COORDINATOR

SYSTEMATIC REPORT TO THE POLICE

DETECTION

CHECK-LISTS WHEN GRANTING CREDIT

SEGREGATION OF DUTIES & 4 EYES-PRINCIPLES

MANAGERIAL SUPERVISION OF CONTROLS

DEDICATED SCORING TOOL

PREVENTION

INTERNAL MEMOS

MYSTERY SHOPPING

CREATION OF INTERNAL DATABASES

SPECIFIC CHECKS ON CREDIT PORTFOLIOS

KEY SUCCESS/ TAKEAWAYS

> Implementation of a dedicated reporting system from 1st Euro granted, by typology including concrete fraud indicators

> Implementation of fraud indicators / scenarios

> Organisation of several workshops to share best practices with the various entities on different types of fraud

TEAMBANK

RISK MANAGEMENT IN E-COMMERCE CREDIT

* TeamBank is a member of DZ Bank Group, one of the largest banking groups in Germany. DZ Bank serves as a central bank for more than 1000 cooperative banks (Volksbanken Raiffeisenbanken) in Germany.

TeamBank is the group's specialised consumer finance entity. TeamBank offers its customers the products "easyCredit" and "Ratenkauf", which are distributed by more than 82% of all cooperative banks.

STRATEGY

TeamBank relies on a sophisticated multi-layer mechanism to minimise credit and fraud risks in relation to its two main products "easyCredit" and "Ratenkauf".

Credit applications are cross-checked in real-time by accessing various databases including internal credit history, external bank fraud pools and online network analysis, allowing the institution to cross-reference and discover relationships between suspicious applicants in different databases.

TEAMBANK USES A TWO-TIERED FRAUD PREVENTION STRATEGY

AUTOMATION + HUMAN EXPERTISE

Automated fraud system is assisted by a virtual database. This database is fed by customer data, application data, inventory data and fraud indicators, such as external fraud pools.

In case deficiencies are noticed, the application will be subject to an additional assessment by **TeamBank's fraud experts**.

CHALLENGES/ TAKEAWAYS

Effective fraud prevention requires layered structures, using different controls at different stages in the application process so that a weakness in one of the stages is compensated for by the strength of a different control.

In an increasingly interconnected business environment, it is vital to ensure that automated processes for fraud detection were improved to eventually reduce the use of manual overrides from human intervention.

20 employees develop and control the credit decision and processes

6 of these employees are part of the fraud management team

10 fraud attempts per month on average

5 cases of fraud per month on average

70 credit enquiries are passed on to the fraud management team on a daily basis

1 MLO fully automated credit enquiries yearly

70% positive decisions in the partner bank business

1700 credit enquiries per day in disbursement

HOGAN LOVELLS

FRAUD PREVENTION AND THE NEW DATA PROTECTION REGULATION

* Hogan Lovells is a global law firm with more than 40 offices in the United States, Europe, Latin America, Asia, Africa, and the Middle East. The firm boasts more than 2,600 lawyers. Hogan-Lovells' focuses on a variety of practices, including litigation, corporate, finance, IP and regulatory work, with prowess in banking, insurance, arbitration, products liability, white-collar, appellate, antitrust, securities, corporate governance and transactions, health care, medical devices, privacy and media matters.

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. With the adoption of the General Data Protection Regulation (GDPR) with application starting as of 25 May 2018, consumer credit providers need to be cautious about their rights and obligations under the legislation, when it comes to data exchange, storage or processing.

THE NEW REGULATION FOCUSES ON THREE KEY LEGAL ISSUES

COLLECTING AND USING

PROFILING AND SHARING

ENHANCED RIGHTS

DATA COLLECTION

When it comes to data collection, the new EU law covers all personal data of EU residents, irrespective of the location of the data processor. Personal data can be collected where the individual concerned has explicitly consented, where it is necessary for the performance of a contract or if it is needed for a legitimate interest. Furthermore, the purpose of the data collection needs to be specified, explicit and serve a legitimate purpose.

"FREELY GIVEN, SPECIFIC AND INFORMED INDICATION OF HIS WISHES BY THE INDIVIDUAL, EITHER BY A STATEMENT OF BY A CLEAR AFFIRMATIVE ACTION."

CONSENT

One of the much-debated issues concerning the new GDPR has been the concept of "consent". The definition of consent has been changed several times during the negotiation of the text and is now much more affirmative.

"MUST HAVE A FREE CHOICE TO ACCEPT (OR NOT ACCEPT) THE PROPOSED USES OF PERSONAL DATA."

"MUST BE PRESENTED IN A FORM THAT IS DISTINGUISHABLE FROM OTHER TERMS."

"CAN BE WITHDRAWN AT ANY TIME."

COLLECTION NOTICES

Individuals must also be informed about the collection of their data by so called "collection notices". Not only does the notice needs to be in clear and plain language, but the information provided must be specifically adapted to the individual concerned and the context of the data collection. Additionally, the channels used to inform customers need to be considered. The collection notices provided to individuals must furthermore include some key information:

ANY RECIPIENTS, OR CATEGORIES OF RECIPIENTS OF THE PERSONAL DATA

THE PERIOD FOR WHICH THE PERSONAL DATA WILL BE STORED

THE NATURE OF RIGHTS AVAILABLE UNDER THE LAW

THE EXISTENCE OF AUTOMATED DECISION MAKING - meaningful information about the logic involved, as well as the significance and the envisaged consequences

LEGITIMATE INTEREST

The concept of *legitimate interest* is an objective, strictly necessary for the collection, retention, or processing of personal data of individuals.

FRAUD PREVENTION AS LEGITIMATE INTEREST

The law stipulates that fraud prevention constitutes a legitimate interest for the purpose of collecting personal data of EU citizens. Under the new rules, proving that a legitimate interest exists for any form of collection of personal data, will require a balancing test against the fundamental right of the individual concerned.

PROFILING AND FRAUD PREVENTION

Individuals have an explicit right not to be subject to a decision solely based on automated processing and which produces a legal effect or a similarly significant effect on the individual concerned.

UNLESS

> it is necessary for entering into, or performance of, a contract

> it is authorised by Union or Member State law

> it is based on the data subject's explicit consent

MUST AT LEAST ENSURE THAT INDIVIDUALS ARE ABLE TO

> obtain human intervention

> express their point of view

> contest the decision

Should the profiling take place in the context of a fraud prevention process, the undertaking concerned must ensure that five legal requirements are met:

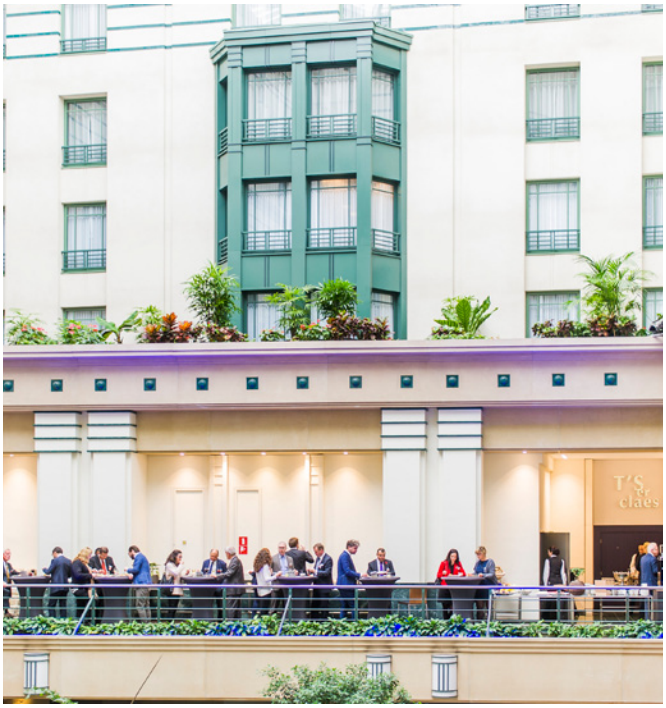
DATA SHARING AND FRAUD PREVENTION

An important question concerns the extent to which undertakings have a right to share and exchange data on individuals. To this end, the law requires that the legitimate interest justifies the sharing of data with others. It also requires undertakings to clearly state in the collection notice, what data is collected and shared with third parties in addition to passing the balancing test between the fundamental rights of an individual and the legitimate interest for the sharing of data.

THE RIGHT TO ERASURE

The new regulation places firm focus on the right to erasure of individuals and stipulates when personal data of individuals must be erased:


eurofinas



SESSION 3

ITALIAN MINISTRY OF ECONOMY AND FINANCE

A FRAUD PREVENTION GATEWAY

* Executive body responsible for economic, financial and budget policy in Italy. Ministry performs a supervisory role of financial services entities and activities. The Ministry of Economy and Finance is divided into eight different Directorates General, the Directorate General in charge of the Prevention of Use of the Financial System for Illegal Purposes is responsible for the analysis of the vulnerabilities of the financial system, with respect to money laundering, usury and the financing of terrorism.

The detection of identity theft has proven to be much of a challenge for public authorities in recent years. SCIPAFI, a computerised central archive developed and operated by the Italian Ministry of Economy and Finance, is intended to make the detection of identity fraud easier and more efficient.

The central archive operates as a gateway, which allows communication between public databases, once it is accessed. It is used for identity verification of potential customers, relating to identity cards, tax codes, health cards, driving license, residence permit and income related documents as available in different public databases.

Operational since early 2015, the gateway makes use of a tiered access for users.

The gateway is accessible by direct users, such as telecommunication operators, banks, and financial intermediaries. Indirect users, such as other credit intermediaries have a limited access. The gateway operates on a fee based system, where a one-time entry fee is charged in addition to a small fee for every check made. Most of the queries (in the first half of 2016) were directed to the database of the income revenue authority.

To date, 1007 banks and financial intermediaries, 4 credit intermediaries and almost 90 insurance companies have subscribed to the gateway.

TOTAL NUMBER OF CHECK QUERIES FROM JANUARY 2015 TO JUNE 2016

EUROPOL

CEO FRAUD IN THE WORLD OF CREDIT PROVIDERS?

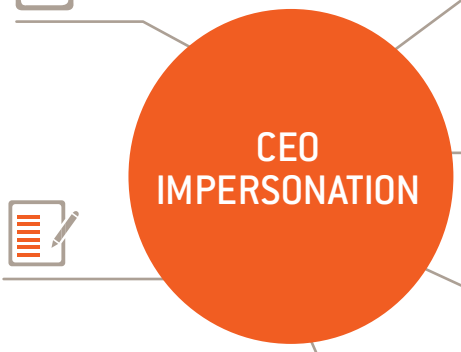
* Law enforcement agency of the European Union headquartered in The Hague
* 940 employees
* Handles criminal intelligence
* Combating serious international organised crime
* Cooperation between relevant authorities of Member States

Businesses are increasingly becoming targets of so-called "CEO fraud" that may end up costing them millions of Euros. A recent case of a major pan European bank being victim of CEO fraud sparked the law enforcement agency EUROPOL, to make the fight against this type of fraud a priority.

CEO fraud involves organised fraud, which purpose is to fraudulently impersonate executives of undertakings in order to gain illegitimate profits.

CEO fraud typically occurs via e-mail or telephone. The victim, normally a high-level member of the finance department, receives a spoofed message from a fraudster, who impersonates the CEO of the company or a partner company, requesting a money transfer. E-mails are often followed-up by telephone calls from a person who sounds trustworthy and who asks the employee to accelerate the payment. In more sophisticated cases, the e-mail account of the executive is hacked by means of malware. This result in fraudsters being extremely convincing regarding both language and content.

KNOW THE SCAMS



STEP 1
A fraudster calls posing as a high ranking figure of the company (e.g. CEO or CFO)

STEP 2
Requires an urgent transfer of funds and absolute confidentiality

STEP 3
Invokes a sensitive situation (e.g. tax control; merger; acquisition)

STEP 4
Pressures the employee not to follow the regular authorisation procedures

STEP 5
Instructions on how to proceed are given later by a third-person or via e-mail

STEP 6
The employee transfers funds to an account controlled by the fraudster. The money is re-transferred to accounts in multiple jurisdictions

ALTERNATIVE

>Requests to receive information on clients (e.g. all unsettled invoices)

>Uses the information obtained to defraud clients

KNOW HOW TO REACT

- Be AWARE of the risks and spread the information within your company.
- Be careful when using social media: by sharing information on your workplace and responsibilities you increase the risks of becoming a target.
- Avoid sharing sensitive information on the company's hierarchy, security or procedures.
- Strictly apply the security procedures in place for payments and procurement. Do not skip any steps and do not give in to pressure.
- Always carefully check e-mail addresses when dealing with sensitive information/money transfers. Fraudsters often use copycat e-mails where only one character differs from the original.
- If you receive a suspicious e-mail or call, always inform your IT department; they are the ones in charge of such issues. They can check the content of suspicious mail and block the sender if necessary.
- In case of doubt on a transfer order, always consult a colleague even if you were asked to use discretion.
- Consider assigning responsibility to an employee whom others can consult in case of doubt.
- If you receive a call/email alerting you of a security breach, do not provide information right away or proceed with a transfer. Always start by calling the person back using a phone number found in your own records or on the official website of the company; do not use the number provided to you in the mail or by the caller. If you were contacted by phone, call back using another phone (fraudsters use technology to remain online after you hang up).
- If a supplier informs you of a change in payment details, always contact him to confirm the new information. Keep in mind that the e-mail/phone number provided on the invoice might have been modified.
- Always contact the police in case of fraud attempts, even if you did not fall victim to the scam.

UK FINANCE AND LEASING ASSOCIATION (FLA)

COLLABORATION WITH PUBLIC AUTHORITIES

* Leading UK trade association for the asset, consumer and motor finance sectors
* Members provided £110bn of new finance in 2015 to consumers and businesses
* New business: £81bn Consumer Finance, £37bn Motor Finance

The FLA is collaborating with the **National Vehicle Crime Intelligence Service (NaVCIS)**, a police unit dedicated to the prevention and the detection of vehicle crime. NaVCIS is operating as a police and private sector partnership and is funded over 80% by the FLA's motor and asset finance members.

It was set up in 2005 following a £19m loss by the industry. The partnership became operative in 2007 and allows the police to track down stolen vehicles.

HOW DOES IT WORK IN PRACTICE?

1. FLA member submits referral pack regarding case of fraud or theft
2. Evidence assessed to ensure a crime has been committed
3. Referral enriched with additional police intelligence
4. Details added to Police National Computer
5. Sent out to relevant police force in England and Wales
6. ANPR cameras or police activity identify stolen / fraudulently obtained vehicles
7. Police recover vehicle and hand back to lender

Interestingly, NAVCIS also helps to recover vehicles that have been transported overseas. Under the Schengen intelligence system, NaVCIS receive alerts and contact from police officers from throughout Europe indicating UK vehicles are in their territories. This information is passed on to lenders who then deploy their recovery agents to pick up the vehicle overseas.

RESULTS TO DATE

> 542 recovered vehicles worth £7.4m in 2015/16 growing from £3.6m in 2007

> Over 2 500 recovered vehicles worth over £40m since 2007

> On average over 50 stolen cars referred to NAVCIS each month and growing to 100 in July and August 2016

CONCLUSION

BY EUROFINAS

Leon Dhaene
Director General

Fraud is a major issue for the consumer finance industry. Fraud threatens consumer trust and ultimately decreases customer loyalty. Fraud has the largest negative impact on a firm's profitability. Current digitalisation of business processes also has a major impact on fraudulent practices.

Fraud management should be a joint industry concern not an issue of business competition. It is also an international matter and we need European-wide solutions to tackle it.

A financial organisation on its own lacks resources to identify all new fraud trends and does not necessarily have access to all available information/data required to prevent fraudulent behaviours at an early stage.

I think that there is a great role for Eurofinas to play in this field and work together with law enforcement agencies and supervisors to assess how best we can exchange information and ensure that sufficient data can be used in the fight against fraud.

We should also look at other industries such as telecommunication companies and retail payment operators to benchmark tools and practices.

Perhaps a friendly warning, more data is not always the right solution. Human expertise remains vital and the training of our staff, a core pillar in the fight against fraud.

I look forward to working on this crucial topic for the industry together with Eurofinas members.

Leon Dhaene
Director General

LEADERS ACROSS EUROPE NOW RATE FRAUD AS A KEY THREAT TO BUSINESS GROWTH FOR THE FIRST TIME EVER

Business see rising levels of risks and costs because they are failing to find the right balance between effective fraud prevention and a smooth customer experience – both of which now have a direct impact on growth.

New research from Experian shows that almost half of CEOs (42%) in large enterprise businesses, now see fraud as the number one inhibitor to business growth, after competitor activity.

The results follow a recent commissioned study conducted by Forrester Consulting, on behalf of Experian. It gauged opinion among nearly 400 CEOs and senior business leaders working across Europe, the Middle East, and Africa.

It also revealed that many boardrooms don't understand the critical balance intrusive fraud prevention and friction have on smooth customer experience and a seamless sales process. It's clear many organisations face critical strategic gaps in analytics, data and fraud technology.

The research showed that more than three out of four (77%) CEOs admit their current fraud prevention strategies were ineffective. In fact, only around one in four (28%) said their business had a balanced approach to complex fraud that does not directly impact customers' online journeys.

Elsewhere, less than one in three (31%) businesses continually monitors fraud attempts, tracks real-time customer transactions, or has access to accurate data sources. As a result, nearly half (45%) of all senior business leaders say they now plan to improve fraud analytics capabilities within the next 12 months, by investing in new technologies, including device recognition software.

But at the same time, many CEOs are aware of the pressing need to act fast amid fears traditional business models could be obsolete within the next five years as they fail to consistently meet customer expectations, or lose ground to smaller, agile, digital-savvy competitors. Many of which are not weighed down by legacy systems or more traditional routes to market. It is a point that is not being lost on boardrooms, with budgets set to be increased to help ensure they continue to meet expectations.

Fraud represents a massive challenge for us all given its increasing complexity, brutally highlighted by current estimates predicting global losses are likely to top US$2 trillion by 2020. Experian has been investing for a number of years to grow its strengths in fraud detection in anticipation that it would become one of the biggest challenges facing its customers across the globe. As a result, it is now at the forefront of the market as industry experts in fraud, data, analytics and online customer experience.

Many business leaders recognise that there is a critical balance that needs to be struck between fraud prevention, online friction and customer experience, reflecting Experian's investment in mobile and device recognition technology. At the same time, the company continues to work closely with thousands of businesses right across the globe to ensure they have balanced fraud strategies in place to meet the expectations of our modern-day online consumers.

This is simply a snapshot of the research. The findings are now published in full in new Experian report Winning In The Customer Era.

ABOUT EXPERIAN

Experian is the world's leading global information services company. At life's big moments – from buying a home or car, to sending a child to college, to growing a business by connecting it with new customers – we empower consumers and our clients to manage their data with confidence. We help individuals take financial control and access financial services, businesses make smarter decisions and thrive, lenders to lend more responsibly, and organizations to prevent identity fraud and crime.

We have 17,000 people operating across 37 countries and every day we're investing in new technologies, talented people and innovation to help all of our customers maximize every opportunity. Experian plc is listed on the London Stock Exchange (EXPN) and is a constituent of the FTSE 100 index. Learn more at www.experianplc.com or visit our global content hub at our global news hub for the latest news and insights from the company.

XPERTA S.R.L. GROUP OF COMPANIES DEALS WITH THE FIGHT OF ID-RELATED FRAUD AND THE FIGHT AGAINST ILLICIT INTERNATIONAL VEHICLE TRAFFICKING, ACTIVELY CO-OPERATING WITH BOTH NATIONAL AS WELL AS INTERNATIONAL POLICE FORCES.

Our Customers range from Telcos to Insurance Companies, from Consumer Credit Entities to Car Rental Companies alike.

We offer a wide range of highly effective tools and innovative services in order to prevent fraud perpetrated with the use of counterfeit documents. We also offer stolen vehicles' localisation, de-seizing and repatriation services both in Europe as well as in Africa with constant trips on-site to manage the direct contacts with local authorities.

We know that each Customer is unique. Therefore our aim is, in fact, to provide our Clients with strongly customised tools and services to be smoothly implemented in their internal procedures. These services can be operated internally or handed out to teams of police-trained experts, ensuring the highest level of performance required by all of our Customers.

CASE STUDIES

ID-SPECIALIST

Our top of the range anti-fraud suite comprises both proprietary software as well as proprietary hardware to offer the highest level of security as far as ID-related fraud is concerned. ID-Specialist is a modular and flexible solution and can be easily and effortlessly implemented by adopting state-of-the-art acquisition devices to suit the need of your work-flow.

ID-SPECIALIST COMPRISES THE FOLLOWING MODULES:

Document acquisition devices:

- ***S.P.I.D.scan***, top of the range multi-spectral A4 flatbed scanner with multiple documents reading at one time
- ***eDocubox***, ICAO Doc 9303 compliant, multi-spectral ID3 acquisition device with RIFD reading capabilities

Automated document analysis:

- ***R.D.C. (Remote Document Check)***, advanced verification service used to verify single or bulk images, sent both via web and via a direct Ethernet request from the S.P.I.D.scan

Positive fraud cases database:

- ***Alert***, existing db with thousands of certified fraudsters' data and actual photos used in conjunction with R.D.C.

Genuine documents' database:

- ***IDIS Pro,*** vast database of genuine HD documents' images and their security features

With the above integrated solution* Italy's biggest Telco since 2014 saved Millions of Euros every year in avoided frauds.

* some of the above mentioned tools are currently at their final stage of development and are undergoing a thorough final testing prior to their release.

NO EX-PORT

A simple yet effective as well as innovative solution developed in-house with the use of hardware, specific protocols developed with the help of Police Forces' Specialists and proprietary software has already been put to work in Spain with the co-operation of the Guardia Civil to prevent vehicles from leaving the European Continent when not allowed. In the first few months of operation, hundreds of thousands of Euros worth of vehicles have been stopped before their illicit departure for Africa.

The plan is to push or the same protocols throughout Europe and its Schengen borders to prevent the illicit vehicles' trafficking for Clients such as Rental Companies, Leasing Companies as well as the Private sector.

.....

DO NOT HESITATE TO CONTACT US TO REQUEST A FRAUD-RELATED CONSULTATION AND SEE HOW XPERTA CAN HELP YOUR BUSINESS.

Xperta: your one-stop supplier of highly efficient anti-fraud services and tools with proven track records for the fight to ID-related frauds and illicit vehicle trafficking.

.....

Responsible editors: Alexandre Giraud, Senior Legal Adviser & Anjena Narang, Legal Adviser - Published by Eurofinas - March 2017

eurofinas

SPECIALISED CONSUMER CREDIT PROVIDERS IN EUROPE

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

Publication date: March 2017