EMEA FRAUD Report 2019

Study conducted by Forrester Consulting on behalf of Experian

Contents

Introduction

Fraudsters are fast, unrelenting, indiscriminate, inventive and opportunistic. It's also clear they will happily switch from sector-to-sector and from one channel to another to get access to funds. Information relating to emerging vulnerabilities will be quick to be traded and shared.

Business recognises the growing risk fraud presents and its direct impact. In an effort to tackle the rising challenges it poses and minimise the impact, firms are investing more time and resources into fraud management.

But is it enough? It's clear many are hampered by the complexity and diverse mix of channels, products, methods of payment, geographies and regulations that now need constant policing. They're also managing budgetary constraints, recruitment, talent retention and related manpower challenges.

At the same time, boardroom demands, differing sector-specific risk appetites, friction versus retention and the impact of emerging regulation all play a part. We look at the key drivers, emerging trends, pain points and favoured areas of investment being made in fraud prevention, across the region.

About the author

Frédéric Dubout
Senior Consultant in Fraud and Identity, at Experian

Frédéric has nearly 20 years' sector-specific expertise working for multi-national telecommunications, banking, automotive and financial services companies, across Europe, Africa and the Middle East. Frédéric has worked across the full spectrum of fraud prevention - from the application of emerging technologies and biometrics, to transactional and payments fraud, to application fraud, online, mobile and card-not-present fraud. Collections, data quality, data management and project management, also fall under his areas of expertise.

Executive summary

- Business, industry and commerce are all locked in a digital arms-race with the fraudsters.
- As a result, AI, automation and machine learning will be the key areas of investment between now and 2022.
- The vast majority of firms (85%) admit they must improve their cyber-security but a significant number are hamstrung by budgetary constraints, recruitment and manpower challenges.
- As a result, less than one in five business (14%) believe their fraud and online security operations are sufficiently well-optimised.
- The arrival of PSD2 and Open Banking is also now driving the pace of innovation across Europe. While most decision-makers are aware of the critical priority compliance poses, many continue to invest effort into ensuring they consistently retain a top-quality customer experience.
- Data theft – malware, hacking and social engineering – impacts around 60% of businesses, while polled respondents' opinions suggest ID theft affects less than half of European firms (47%) – but is it a sign of overconfidence?
- It also emerged Denmark, France, Turkey and Poland are more likely to face ID theft than other European countries – according to more than half (+53%) of respondents.
- Overall across EMEA one in three (34%) decision-makers admit their digital channels are vulnerable, although in France and Turkey, it's around half of all businesses.

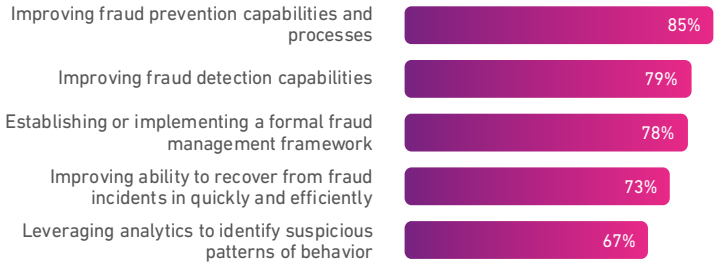
Research methodology and framework

The study was conducted by Forrester Consulting on behalf of Experian. It drew responses from more than 900 cross-industry companies from Europe, Middle East, and Africa. Analysis covered organisations employing more than 50 employees in sectors as diverse as fintech, ecommerce, hospitality, ticketing, banking, retail and telcos. Respondents were managers and senior decision-makers overseeing or influencing fraud and risk strategy. For a full summary, please refer to the Appendix section at the back of the report.

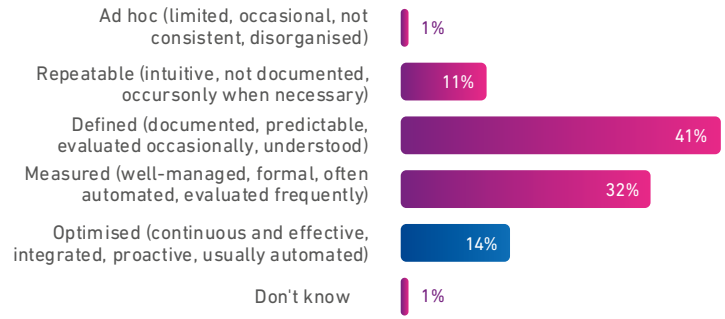
Over-confidence in fraud prevention? The perception versus the reality

Findings clearly show improving fraud prevention and detection is a top priority for the vast majority of firms (85%). Around two in five (40%) firms say fraud is evaluated and understood within their business, but only one in three (32%) say it's clearly defined, measured, or underpinned by automation. In fact, only around one in seven (14%) of firms believe their ability to prevent fraud is genuinely well-optimised. It's also worth noting the relative self-confidence of firms in the UK, Italy, Poland, and Austria/Germany, which are more likely to regard their fraud prevention performance as 'optimised' when compared to their European neighbours.

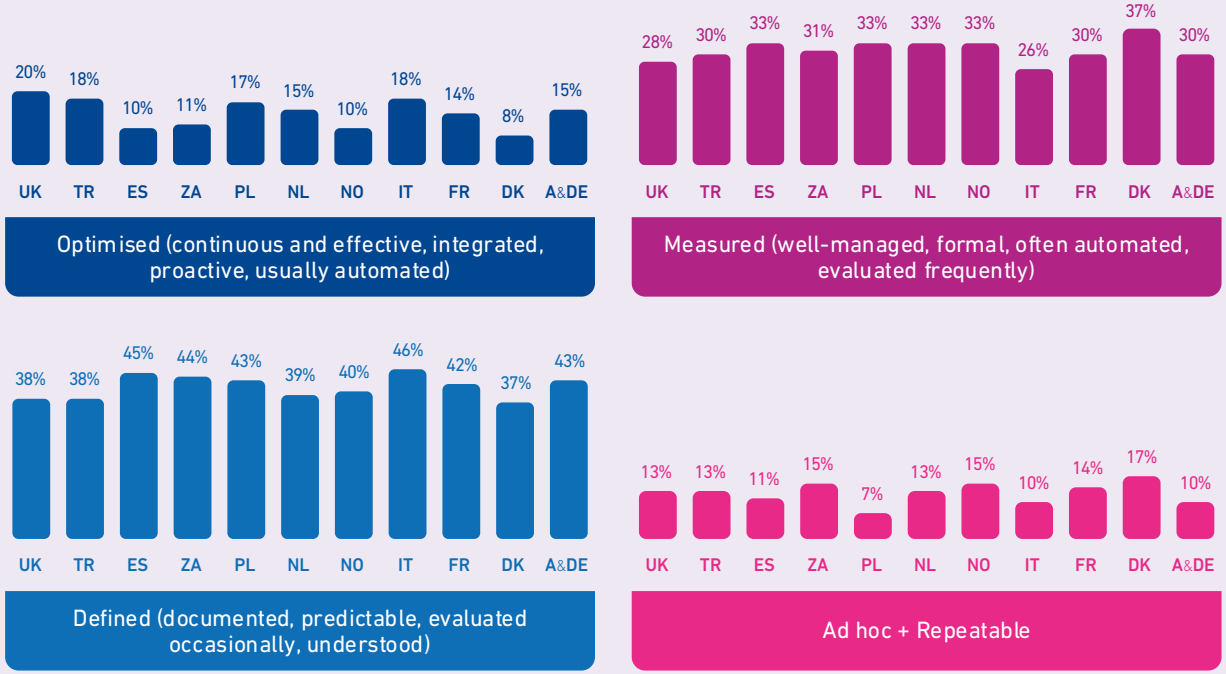
Top-priorities for fraud and risk managers across the region for the next 12 months.



Firms' ability to prevent fraud



Firms' ability to prevent fraud – country variances



Base: 913 decision makers with responsibility or influence over fraud and risk strategy at businesses in EMEA

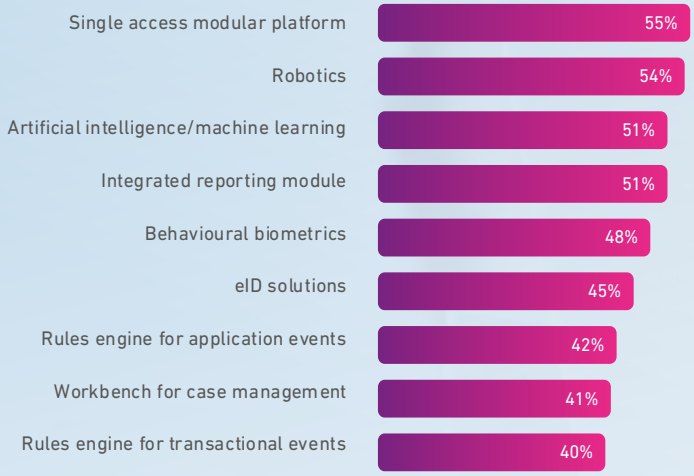
Source: A commissioned study conducted by Forrester Consulting on behalf of Experian, June 2019

Firms in the UK, Italy, Poland, and Austria /Germany are more likely to rate their fraud prevention ability as 'Optimised', compared to other EU countries

What's restricting the adoption of advanced fraud prevention techniques?

Is it financial and budgetary restrictions, cultural, technological, or simply the complexity of fraud today? It's clear that fraud's complexity, rapid change and the emerging challenges continue to pose headaches for many companies. Given fraud's global scale and reach, many firms know they simply cannot completely manage risk internally. It's also clear significant investment will be made by many firms into automation, machine learning and predictive analytics within the next three years.

Firms' planned fraud investments within the next three years



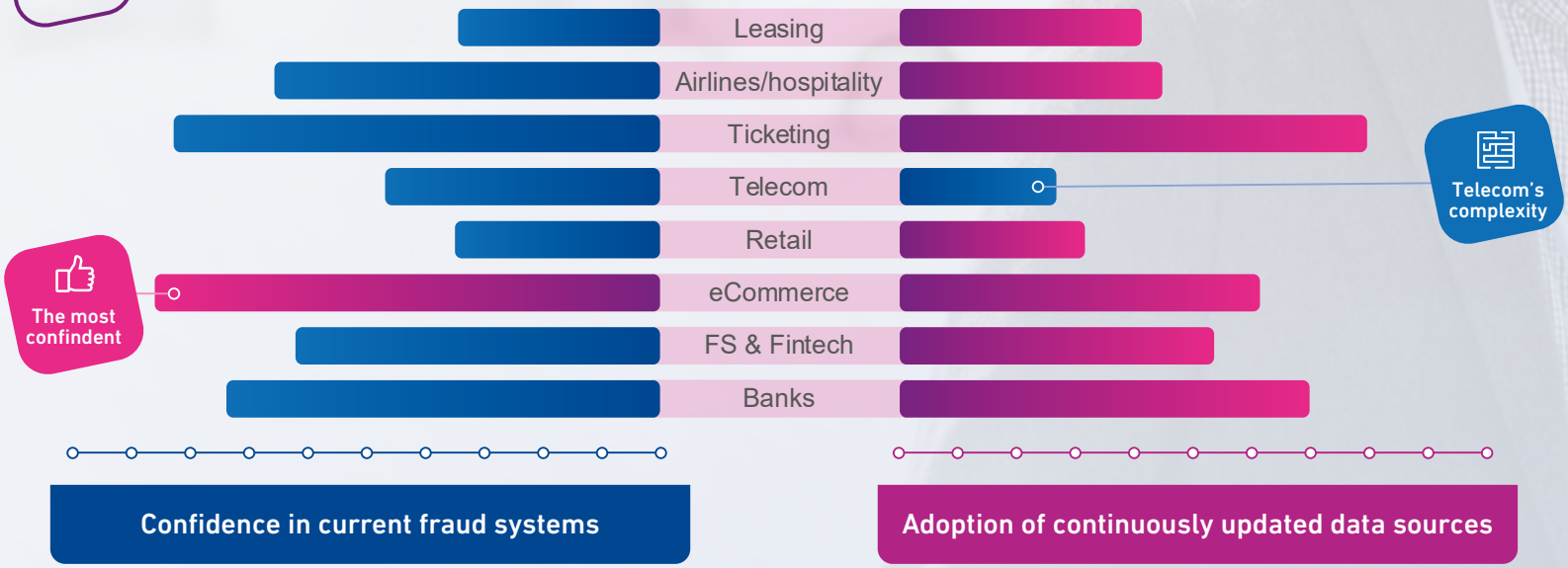
Base: 913 decision makers with responsibility or influence over fraud and risk strategy at businesses in EMEA
Source: A commissioned study conducted by Forrester Consulting on behalf of Experian, June 2019

Efficiency and effectiveness – sector-by-sector

Unsurprisingly, there are disparities in the perceptions of fraud prevention between sectors – particularly among some less mature or fraud-savvy firms within leasing, car rental and retail.

There are also broad variances when compared to eCommerce, which has naturally evolved multiple lines of fraud detection and defence. The sales process leads to a transaction – from the cart / customer fraud assessment, to rules of prevention of regional payment service providers (PSPs), transaction-related authorisation of card schemes and authentication models, to the broad adoption of device intelligence. Elsewhere, telco providers are acutely aware of the extreme complexity posed by their collection and analysis of customer airtime usage, as well as the variety of data models.

Sector-by-sector variances



Perception and impact of fraud types

The top-three most widespread fraud types currently seen are data theft, impersonation and fraudulent entry into digital channels.

But there are huge regional differences of opinion around the ability and effectiveness of fraud-detection. Clearly, there are perceived advantages from data-sharing offered by in-country credit bureaux – as in the UK, Spain and Italy. Spain also offers a more formalised multi-sector prevention scheme via the Spanish Fraud Association), while others have set out to safeguard citizens by championing national digital identity programmes like Denmark's NemID initiative, or the Netherlands' Ideal programme.

The broad perception of the impact of fraud falls into two distinct types – the financial loss and the related legal, regulatory, or perceived reputational impact, which are particularly prevalent following a data theft.

Most prevalent forms of fraud

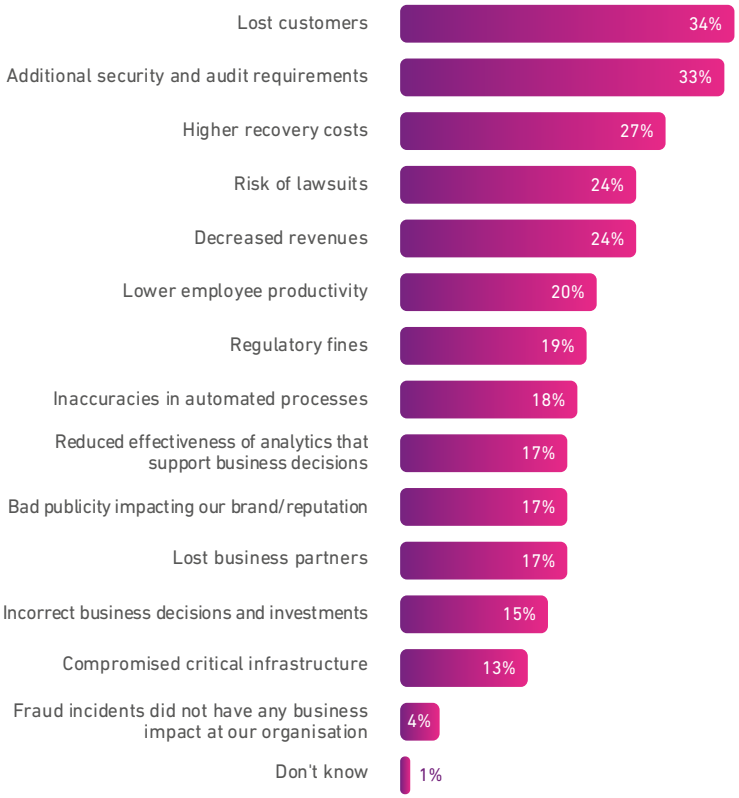
Most prevalent types of fraud by country	Total	A& DE	DK	FR	IT	NO	NL	PL	ZA	ES	TR	UK
Data theft (by malware, social engineering, or hacking)	58%	55%	57%	58%	66%	55%	61%	52%	52%	62%	67%	58%
Identity theft/new account fraud	47%	44%	54%	58%	34%	36%	41%	53%	55%	40%	58%	45%
Account takeover fraud	45%	48%	48%	43%	44%	42%	50%	48%	29%	40%	53%	48%
Internal fraud (employee or retailer)	39%	42%	36%	39%	36%	40%	35%	38%	47%	41%	37%	38%
Wire transfer fraud	36%	38%	31%	43%	25%	28%	31%	47%	42%	37%	48%	34%
Application fraud on digital channels	34%	37%	29%	47%	46%	27%	25%	32%	26%	36%	50%	22%
Card-not-present fraud	28%	29%	22%	27%	30%	21%	26%	30%	31%	27%	35%	33%
Application fraud in physical points of sale	23%	27%	19%	25%	31%	17%	23%	28%	18%	23%	23%	27%
Synthetic identity fraud	22%	26%	22%	25%	33%	17%	13%	33%	15%	29%	15%	11%
None of the above	1%	1%	2%	0%	7%	0%	1%	2%	0%	0%	0%	2%

Base: 913 decision makers with responsibility or influence over fraud and risk strategy at businesses in EMEA

Source: A commissioned study conducted by Forrester Consulting on behalf of Experian, June 2019

Perceived impact of fraud across the EMEA region

Lost customers, the added burden of new security measures and rising recovery costs pose the biggest challenges for one in three (33%) firms. Unsurprisingly, increased risks of fines, regulatory scrutiny, legal action and reputational damage are all close behind, given they are front-of-mind for nearly one in four (24%) decision-makers.



Perceived impact of fraud by country	Total	A& DE	DK	FR	IT	NO	NL	PL	ZA	ES	TR	UK
Lost customers	34%	37%	36%	41%	26%	38%	30%	37%	39%	32%	25%	23%
Additional security and audit requirements	33%	31%	31%	44%	31%	28%	21%	48%	24%	36%	43%	34%
Higher recovery costs	27%	24%	31%	25%	33%	22%	25%	40%	31%	28%	23%	22%
Decreased revenues	24%	32%	23%	22%	16%	21%	20%	32%	26%	30%	18%	22%
Risk of lawsuits	24%	20%	25%	33%	15%	21%	21%	30%	31%	26%	17%	19%
Lower employee productivity	20%	27%	18%	24%	16%	16%	19%	20%	11%	11%	42%	22%
Regulatory fines	19%	20%	18%	27%	18%	20%	15%	17%	16%	14%	30%	14%
Inaccuracies in automated processes	18%	22%	18%	19%	13%	8%	22%	17%	18%	22%	15%	25%
Lost business partners	17%	26%	11%	15%	20%	19%	19%	13%	18%	19%	15%	11%
Reduced effectiveness of analytics that support business decisions	17%	23%	13%	20%	10%	19%	18%	18%	18%	11%	25%	14%
Bad publicity impacting our brand/reputation	17%	23%	18%	20%	18%	11%	16%	10%	26%	13%	13%	19%
Incorrect business decisions and investments	15%	19%	13%	15%	13%	14%	13%	15%	13%	18%	17%	20%
Compromised critical infrastructure	13%	14%	13%	23%	8%	17%	19%	5%	2%	13%	13%	11%
Fraud incidents did not have any business impact at our organisation	4%	5%	9%	1%	13%	5%	1%	3%	0%	4%	7%	3%

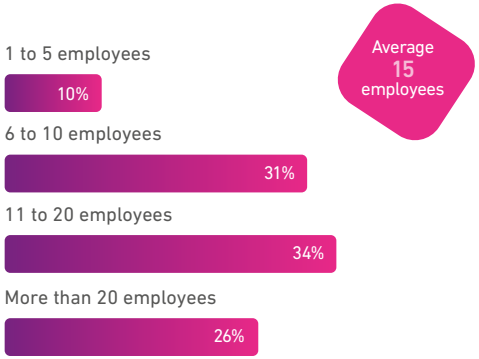
Base: 913 decision makers with responsibility or influence over fraud and risk strategy at businesses in EMEA

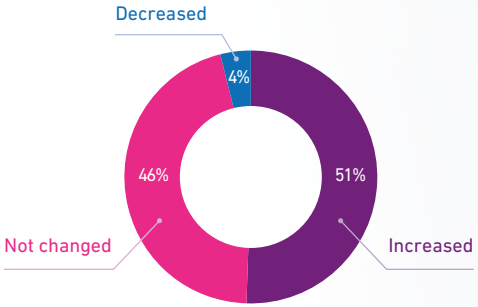
Source: A commissioned study conducted by Forrester Consulting on behalf of Experian, June 2019

Key drivers to fraud strategy and decision-making

Identifying fraud, the volume, scale and types of detected attacks, alongside increased risk of exposure to losses are regarded as the top fraud management challenges for firms' back-offices.

As a result, most plan to increase investment in fraud technology and staff training. But it's worth noting that while many analyse historical customer data to identify fraudulent behaviour, fewer currently rely on predictive models to help reduce fraud. Across business sectors, most fraud prevention initiatives are driven by risk and operations teams.

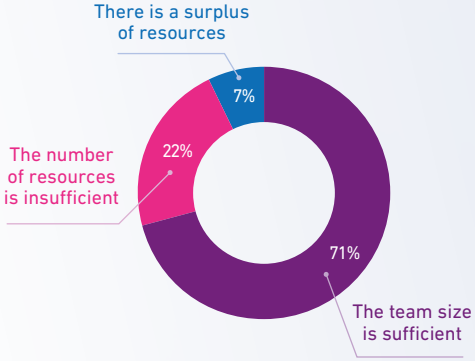


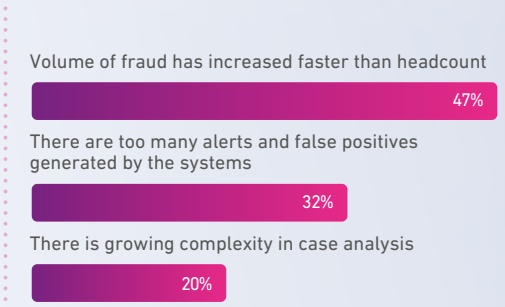


Base: 913 decision makers with responsibility or influence over fraud and risk strategy at businesses in EMEA
Source: A commissioned study conducted by Forrester Consulting on behalf of Experian, June 2019

While the average fraud team has a headcount of 15 staff members, many firms admit to being hamstrung by an acute lack of talent and skilled labour. It's a global challenge, with many businesses obliged to parachute in consultancy expertise and third-party services to fill the gap. In fact, nearly one in four (22%) firms currently believe that insufficient resources are being invested in fraud management. Meeting the demands of emerging fraud trends, the development and adoption of new technology requires new skill sets, is now leaving some businesses with a clear under-representation of fraud data analysts. Short-term investments within the next 12 months to help meet the demand are being earmarked for new technology, increased training and greater external support.

Analysis of teams' size and resourcing challenges



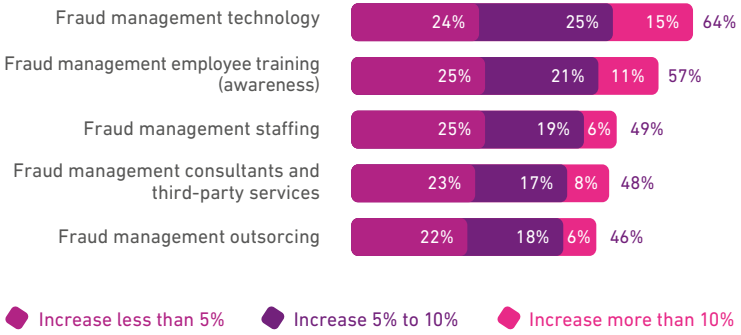


Base: 913 decision makers with responsibility or influence over fraud and risk strategy at businesses in EMEA
Source: A commissioned study conducted by Forrester Consulting on behalf of Experian, June 2019

Scaling the fraud teams – country-by-country analysis

Base: 913 decision makers with responsibility or influence over fraud and risk strategy at businesses in EMEA
Source: A commissioned study conducted by Forrester Consulting on behalf of Experian, June 2019

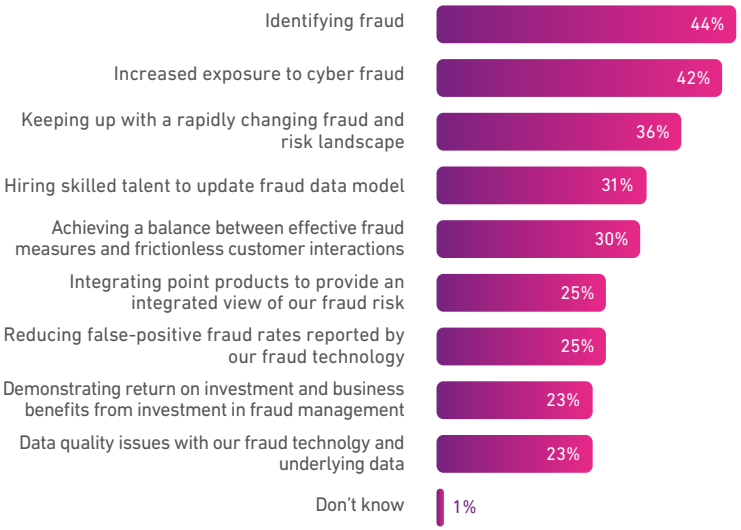
Firms' favoured short-term fraud investments within the next 12 months



Base: 913 decision makers with responsibility or influence over fraud and risk strategy at businesses in EMEA
Source: A commissioned study conducted by Forrester Consulting on behalf of Experian, June 2019

Evolution of top-10 in-house fraud detection indicators and the rising expectations of digital customers

The charts below offer an overview of fraud teams' in-house performance indicators across a diverse mix of territories – but could they be regarded as a little too simplistic given differences in maturity levels? Fraud is a global challenge – particularly given the effort and numerous initiatives in play, while the pressure to safeguardg customers continues to intensify highlighted by the relentless detected attack rate, the volume and rate of fraud losses, as well as their estimated costs to both business and the consumer.



Base: 913 decision makers with responsibility or influence over fraud and risk strategy at businesses in EMEA

Source: A commissioned study conducted by Forrester Consulting on behalf of Experian, June 2019

By country	Total	A& DE	DK	FR	IT	NO	NL	PL	ZA	ES	TR	UK
Identifying fraud	44%	41%	42%	48%	34%	36%	44%	47%	42%	52%	60%	38%
Increased exposure to cyberfraud	42%	51%	40%	48%	38%	33%	31%	50%	40%	36%	60%	36%
Keeping up with a rapidly changing fraud and risk landscape	36%	36%	30%	34%	44%	32%	35%	52%	47%	38%	30%	27%
Hiring skilled talent to update fraud data models	31%	31%	35%	34%	25%	24%	33%	35%	37%	34%	25%	28%
Achieving a balance between effective fraud measures and frictionless customer interactions	30%	25%	35%	32%	31%	27%	24%	45%	21%	29%	32%	33%
Integrating point products to provide an integrated view of our fraud risk	25%	31%	28%	31%	31%	18%	12%	20%	18%	23%	37%	27%
Reducing false-positive fraud rates reported by our fraud technology	25%	30%	18%	26%	34%	23%	19%	18%	29%	31%	20%	20%
Data quality issues with our fraud technology and underlying data	23%	30%	21%	27%	25%	11%	19%	23%	23%	29%	15%	28%
Demonstrating return on investment and business benefits from investment in fraud management	23%	22%	24%	21%	26%	22%	23%	37%	19%	23%	13%	22%

But at the same time, it's worth noting the proportion of respondents highlighting an increase in the level of friction on the customer journey – be it PSD2, the ongoing widespread use of 3DSecure in eCommerce, the demands posed by SCA and document verification in new processes. For more insight into this, please refer to next section.

In fact, only around one in four (25%) believe that false-positives have fallen, suggesting the challenge to successfully optimise the customer experience is continuing and will be an ongoing one.

CASE STUDY

Veepee

How VeePee's adoption of FraudNet helped reduce fraud and improve the customer journey

Demonstrated by a 1% uptick in sales for a business with a +€3bn annual turnover

Vente-privee - now simply known as Veepee - was a pioneer in the concept of flash sales. It offers exclusive designer brands for a limited time, at heavily discounted prices, to a community of savvy online shoppers who often subscribe to get daily sales alerts. Having launched in France in 2001, the company has become a European leader with 72 million customers across eight European countries. It now has more than 6,000 employees and generates around €3.3 billion gross turnover a year.

The challenge

Veepee was confident that it had fraud under control but felt customer conversion rates were impacting overall sales revenues. The company wanted to reduce friction being caused by referrals to 3DSecure (3DS) authentication, which it believed was adversely affecting customer experience and damaging overall sales revenues.

Internal testing showed conversion rates when 3DS was used, were lower than via non-3DS channels. This had an impact on revenues because of interrupted service. Veepee was also very conscious of the impact the interruptions 3DS was having on shoppers – highlighted by subsequent drop-out and basket abandonment. At the same time, the company also wanted to ensure it continued to safeguard genuine customers and maintain its consistently low fraud rates.

Why recognition counts

The challenge Veepee faced hinged on the ability to quickly recognise and serve good customers – whether they were new or returning shoppers. Increasing its customer recognition capabilities were a logical extension of its overall proposition given its exclusive community of shoppers with a shared common interest in high quality, high-value offers.

Research shows consumer desire for recognition within any trust-based relationships are often vital to long-term success. Two thirds of customers also favour security protocols when they go online. But it also emerged that if security measures result in friction, it quickly has an impact. It was also noted that half of consumers said there was nothing worse than an unsuccessful attempt to complete a purchase online simply because of a failure to be recognised.

Experian showed how FraudNet - part of its CrossCore solution - could enable Veepee to enhance shopper recognition in real-time. By integrating device intelligence onto the payments page, it seamlessly collected and analysed hundreds of device attributes along with data from the transaction and payment details. The real-time analysis also built in positive customer behaviour patterns for both returning shoppers and first-time customers. The additional insight also significantly enhanced Veepee's ability to improve its ongoing customer service and consistently deliver a more favourable user experience, bypassing unnecessary 3DS challenges.

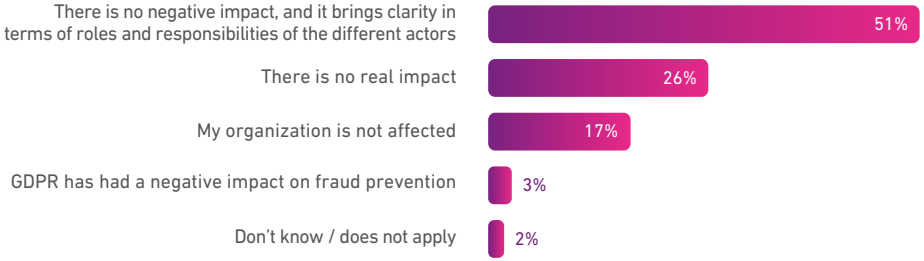
Results

- FraudNet enabled Veepee to reduce 3DS referrals by two thirds.
- It also reduced friction and improved customer experience, helped deliver a 1% jump in conversion rate - a significant sum for a business with a gross annual income of more than €3.3 billion.
- All achieved while ensuring that the overall fraud rate stayed at a consistently low level.

Innovation and the impact of GDPR, PSD2 and emerging regulation

Despite nearly one in five survey respondents suggesting they are not concerned by the impact of General Data Protection Regulation (GDPR) compliance, it has clearly diverted and preoccupied many internal teams' manpower and resources. But surprisingly the regulation has also had a positive impact embraced by most businesses (+50%), which took the opportunity clarify roles, responsibilities, transparency and accountability of stakeholders.

Respondents' views on the impact of GDPR on the day-to-day operation of their business



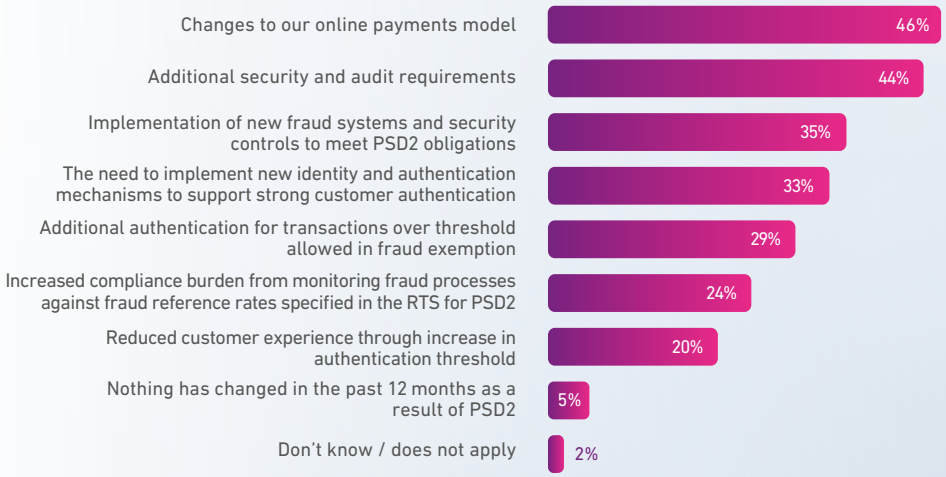
Base: 913 decision makers with responsibility or influence over fraud and risk strategy at businesses in EMEA
Source: A commissioned study conducted by Forrester Consulting on behalf of Experian, June 2019

The regulation also clearly helped move data governance out of the shadows by making its value front-of-mind for many decision-makers and helping create a new generation of engaged and data-savvy customers, who are now developing a true sense of the value of their information.

Respondents' views on the impact of PSD2 on the day-to-day operation of their business

Most in-house fraud specialists also welcome the arrival of the Payment Services Directive 2 (PSD2) with many regarding it as essential in our evolving data economy. Who wouldn't want an extra layer of security on electronic payments, given the directive promotes the creation of Strong Customer Authentication (SCA)? It also now means the new processes must contain at least two of three critical authentication factors. For more, read PSD2 - How the new directive changes the rules of authentication.

How PSD2 drives back-office innovation



Broadly speaking GDPR and PSD2 are genuinely helping drive innovation in favour of the customer, which they were fundamentally created to do. Successful transactions and near real-time risk evaluation now need to be underpinned by far richer information and data sets. Upward of 100 elements relating to shipping addresses, device ID, transaction history, biometric patterns are expected to be the mandatory benchmark.

The customer experience will also need to be safeguarded and continue to be frictionless, because redirections, or additional interventions, simply won't be tolerated by many. Open Banking's arrival is also now removing friction in credit applications right across the Continent, by helping reduce decision times from weeks to minutes.

CASE STUDY

European bank

How FraudNet helped prevent €10.5m of fraud in nine months – equating to €1,615 per hour

The challenge

Our client specialises in consumer credit, online banking and providing credit cards across Europe. In common with other institutions, its anti-fraud team was keen to safeguard customers against the risk of fraud, protect and manage the bank's assets, while maintaining a smooth customer experience for its digital channels.

To achieve these objectives, the lender looked for an easy to implement solution that could quickly and seamlessly analyse online applications to provide alerts to the bank for suspicious behaviour and attempted fraud.

The solution

As a result, our client turned to us, opting for our FraudNet solution, which rapidly proved its value by providing fraud detection rates that are consistently well above the industry average. FraudNet continually monitors all of the bank's online applications to effectively detect and block a high percentage of attacks by fraudsters. FraudNet offered a host of critical capabilities.

- The solution's ability to spot and prevent fraud originating from foreign countries.
- The very rapid platform set-up time and effort required for testing.
- The option of support through one single provider, Experian, without the need for reliance on any third-parties.
- Little impact or on-going dependence on the bank's IT team for solution maintenance and tuning.

Results

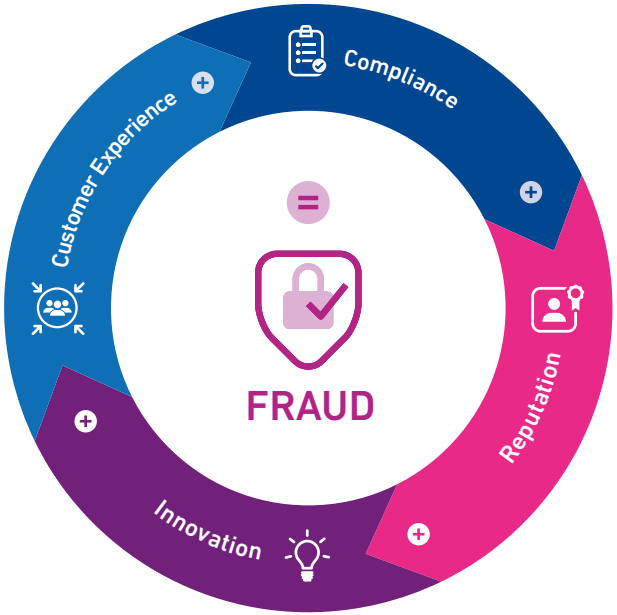
- FraudNet helped prevent €10.5m of fraud within nine months – equating to around €1,615 per hour.
- FraudNet's device intelligence and link analysis proved particularly effective in detecting international fraud rings.
- More than four out of five fraud attempts detected and prevented.
- Prevented €136,000 of attempted fraud made via one device with nine bogus applications during a five-hour period in the same day.
- Shortly followed by six other fraud rings subsequently blocking a further €163,000 of potential losses.
- Fraud detection increased by 21%.
- Identification of an additional 18.7% of fraudulent transactions attributable exclusively to FraudNet and the innovative data it uses.
- Low impact on the day-to-day workload of bank's in-house IT team.
- Improved customer experience.
- Automated decision-making.
- Customers are now better safeguarded from fraud and the bank's reputation is also protected thanks to a direct reduction in losses.
- Reduced operating costs and a fast return-on-investment - in this instance within a matter of days.

Managing the expanding fraud equation = Customer Experience + Compliance + Reputation + Innovation

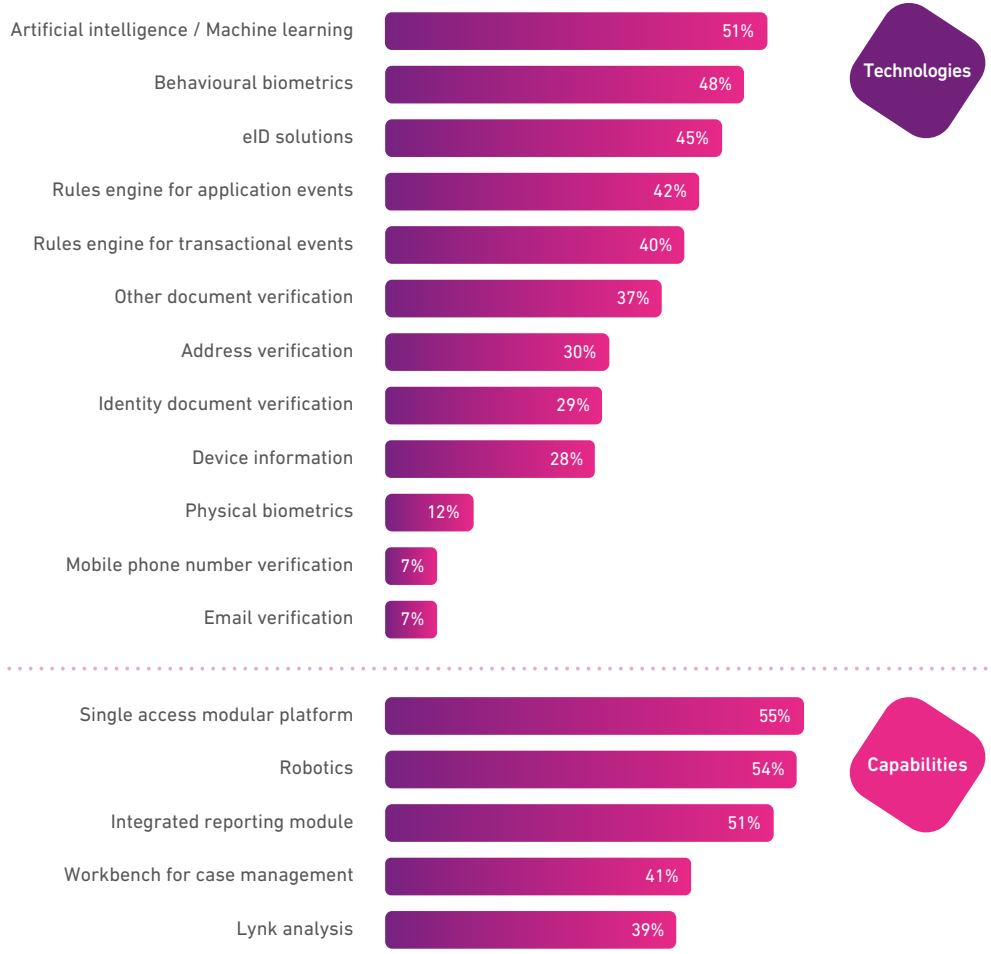
Clearly concerns about fraud no longer hinge wholly on financial losses and rightly extend far beyond to include customer experience, regulatory compliance and reputational matters.

Commercial minds clearly understand the true cost of a lost customer, which in our hyper-connected and accelerated world, extends far beyond just a fraud loss. As a result, top-performing fraud teams have evolved to now encompass compliance, reputation, customer experience and innovation.

But many have also not lost sight of their core mission with fraud prevention and detection still the top priorities. It's clear effective fraud management hinges on speed, flexibility and agility.



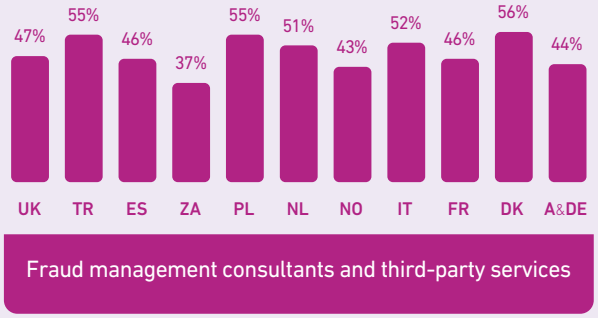
Key areas earmarked for further investment within the next three years



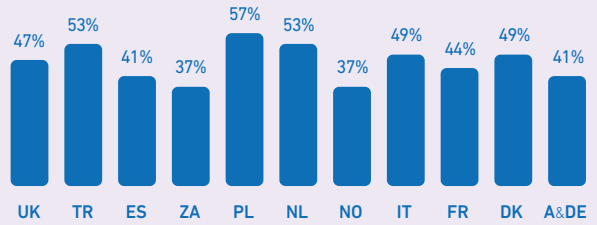
Base: 913 decision makers with responsibility or influence over fraud and risk strategy at businesses in EMEA
Source: A commissioned study conducted by Forrester Consulting on behalf of Experian, June 2019

Investment targets showing country-by-country variances

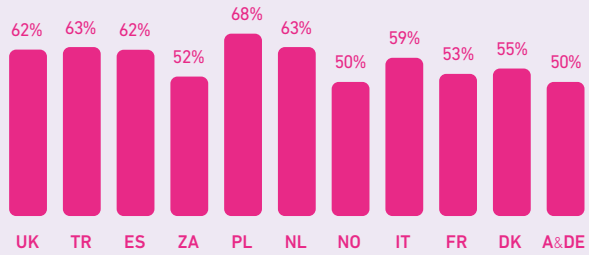
Fraud management technology



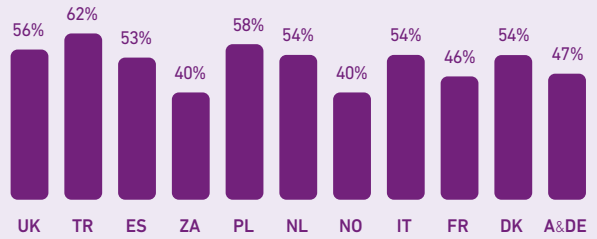
Fraud management consultants and third-party services



Fraud management outsourcing



Fraud management employee training (awareness)



Overall fraud management budget

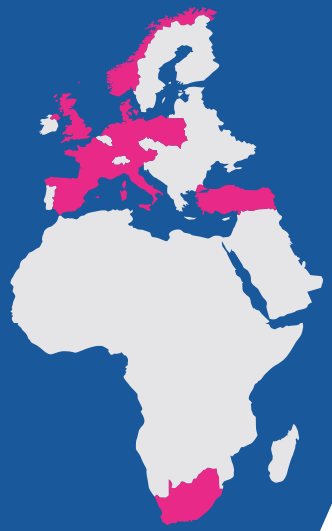
Base: 913 decision makers with responsibility or influence over fraud and risk strategy at businesses in EMEA
Source: A commissioned study conducted by Forrester Consulting on behalf of Experian, June 2019

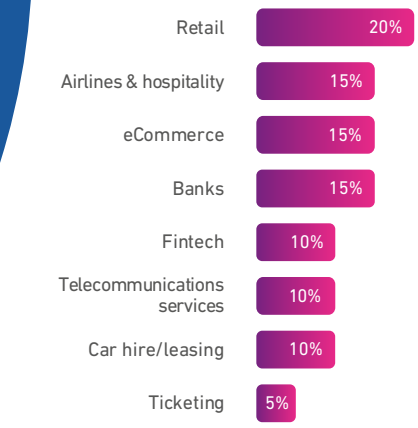
Customers clearly also have great expectations that are continuing to rise. But given the critical tension remaining between CX (customer experience) and fraud solutions that continues to exist, it's expected that the switch away from legacy systems in favour of investing in emerging technology, automation, advanced analytics and biometrics, will pick up pace to help meet the demands of friction-free customer service across every channel.

We're all locked in a digital arms race with fraudsters who operate beyond borders, oversight and regulations. But the challenges will clearly modify and accelerate the pace of technological change in approaches to fraud and risk management. They are areas we already have a proven track-record in successfully delivering for our clients and their customers, thanks to our expertise in biometrics, multi-layered device analysis and geo-location technology.

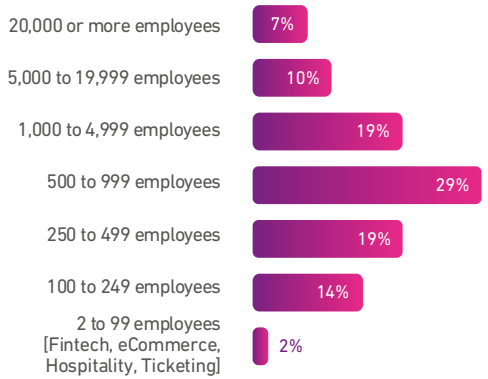
Appendix
About the research

Research findings were compiled from a commissioned study conducted by Forrester Consulting on behalf of Experian, during June 2019. The sample included 913 decision-makers with responsibility or influence over fraud and risk strategy at businesses across Europe, the Middle East and Africa (EMEA).

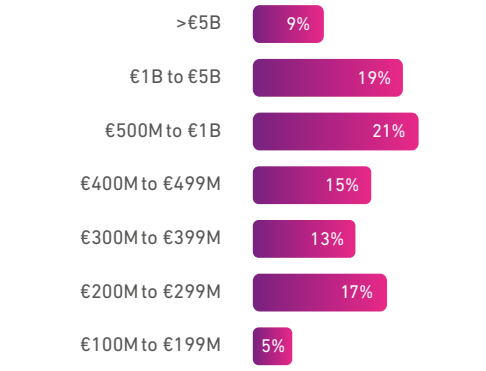




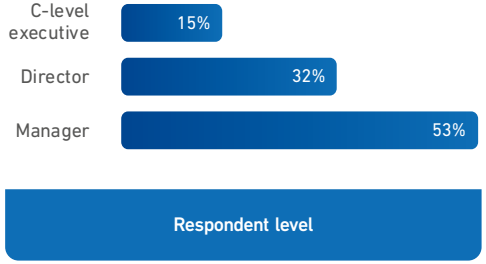
Industry



Company size

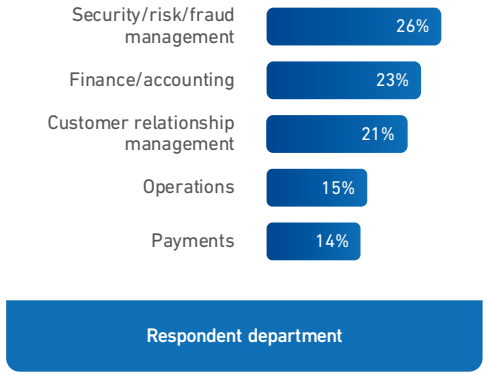


Company revenue



Respondent level

Responsibility on organisation's fraud and risk strategy



Respondent department

Contact your local Experian office

Austria and Czech Republic
Strozzigasse 10/13
1080 Vienna
www.experian.com.pl

Bulgaria
Megapark Office Building
115 G Tzarigradsko shosse boulevard
1784 Sofia
www.experian.com.pl

Denmark
Lyngbyvej 2
2100 Copenhagen
www.experian.dk

France
Tour PB5, 1 avenue du Général de Gaulle
La Défense 8
92074 Paris La Défense Cedex
www.experian.fr

Germany
Speditionstraße, 2 1
40221 Düsseldorf
www.experian.de

Greece and Romania
65 Ag. Alexandrou Street
17561 Paleo Faliro Athens
www.experian.com.pl

Italy
Piazza dell'Indipendenza, 11/b
00185 Roma
www.experian.it

Netherlands
Grote Marktstraat 49
2511 BH, Den Haag
Postbus 13128, 2501 EC, Den Haag
www.experian.nl

Norway
Karenlyst Allè 8B, 0278 Oslo
Postboks 5275, Majorstuen
0303 Oslo
www.experian.no

Poland
Metropolitan Complex
Plac Pilsudskiego 3
00-078 Warsaw
www.experian.com.pl

Russia
5, bldg. 19, Nizhny Susalny lane
105064 Moscow
www.experian.ru.com

Spain
Calle Príncipe de Vergara, 132
28002 Madrid
www.experian.es

South Africa
Ballyoaks Office park
35 Ballyclare Drive
2021 Bryanston, Johannesburg
www.experian.co.za

Turkey
River Plaza, Buyukdere Cad. Bahar Sok.
No: 13 Kat: 8 Levent
34394 Istanbul
www.experian.com.tr

United Arab Emirates
Dubai Islamic Bank Building 01
Office 102, First Floor
Dubai Internet City
www.experian.ae

C-00181