EXPLORING THE TRENDS AND TRAITS OF FRAUD

Looking at UK fraud volumes and global fraud trends

2019 edition
Exploring trends between 2014 and 2019

CONTENTS

INTRODUCTION

Fraud shows no sign of abating, and it's affecting more people than ever.

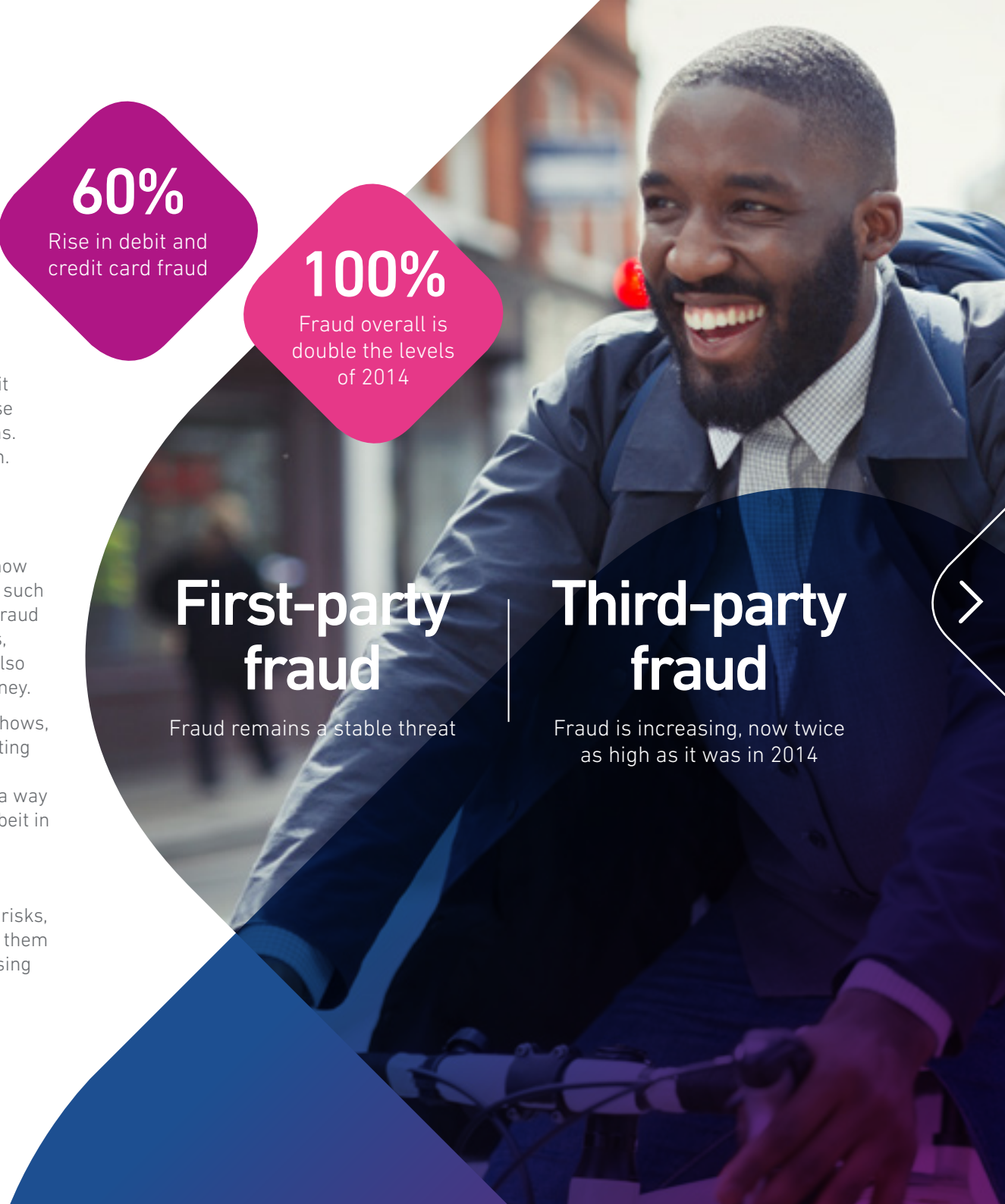
Over the last year we have seen a significant rise in credit card fraud; it is now twice as high as four years ago. There has also been an increase in first-party loan fraud - equating to 70% of all fraud on personal loans. Current account and asset finance fraud have also seen overall growth. Fraudsters are also relentlessly testing new ways to commit financial theft, with more fraud attacks against older people and more women committing fraud.

In terms of how the fraud is being carried out, account takeovers are now one of the biggest challenges facing organisations, while technologies such as AI and machine learning – typically used by businesses to combat fraud – are being used by fraudsters themselves. Man-in-the-middle attacks, synthetic identities, mules, phishing, Trojan Horses and ransomware also remain popular methods for tricking people into parting with their money.

Businesses are aware that fraud is a serious threat. As our research shows, they know the importance of looking after their customers and cultivating trust with them. And they also understand that data breaches and associated fraud can be damaging to customer trust. Few have found a way to entirely stop fraud, and instead we see year-on-year levels rise – albeit in different ways, and with different products targeted.

One thing is certain with fraud: it changes fast.

From the consumer point of view, building trust is the key. Despite the risks, consumers continue to depend on digital interactions, and they expect them to be secure. Businesses are coming around to this idea, and are realising that creating frictionless relationships with robust security cannot be achieved without the latest technology and authentication methods. That's why we're seeing a commitment to increasing budgets and adopting new controls.



FRAUD TRENDS

ANALYTICS ON FRAUD DATA 2014-2019

THE FRAUD LANDSCAPE

Fraud trends by product

Current account fraud is twice as high as it was in 2014.

4x

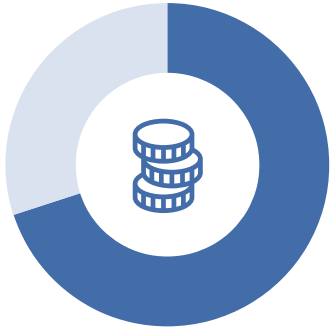
Consumers who are indebted are four times more likely to commit fraud

71%

Third-party savings fraud remains the dominant threat over first-party

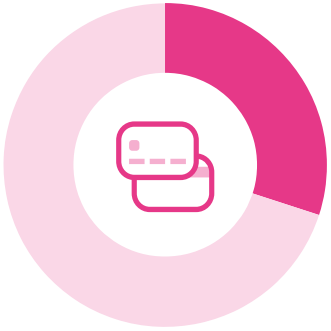
60+

Those who are nearing pensionable age are seeing an emerging threat, with an 11% growth YoY



70%

of fraud on personal loans is first-party



30%

Rise in credit card fraud, making it four times as high as it was in 2014

10%

greater than a year previous, growing at a rate of **22%** YoY

Fraud trends by age and gender and demographic

35%

rise in fraud against first-time buyers aged 25-34, living in suburbs

19%

of fraud is against those aged 25-29

2014

2019 **+45%**

rise in women committing fraud since 2014

<20

Those under 20 see the largest relative increase in first-party fraud

88%

higher than the levels seen in 2014

x2

Municipal Challenge are twice as likely to commit fraud, seeing annual rises

93%

of fraud against Rental Hubs is on current accounts and credit cards

249%

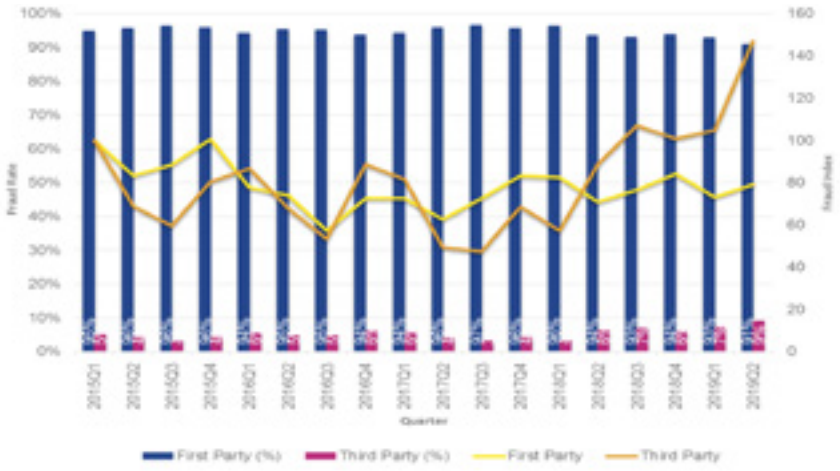
The Rental Hub Mosaic group is 249% higher than expected to be a victim of fraud

ANALYSING THE RISE

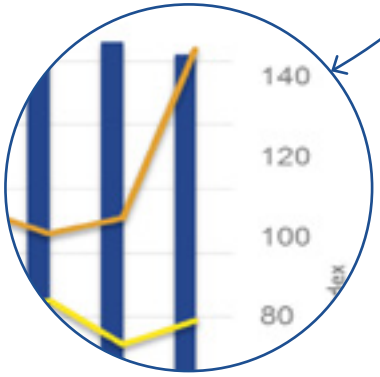
Rise in third-party mortgage fraud – but is all as it seems?

Third-party mortgage fraud saw the largest increase from 2017-2018, compared to all products, and after an initial dip in Q1 2018, levels have begun to rise again.

Fraud type distribution
mortgages (indexed where 2015 Q1 = base)



Rise in 2018 to 2019
in third-party fraud



14%

Mortgages are the most targeted product in Urban Cohesion relative to the total fraud in this group, accounting for over 14% of first-party fraud

33%

The increase in victim of fraud rates is mainly driven by mortgages and cards, with rates on these products 43% and 33% higher than last year respectively

91%

The majority of fraud, 91%, on mortgage applications is first-party as expected

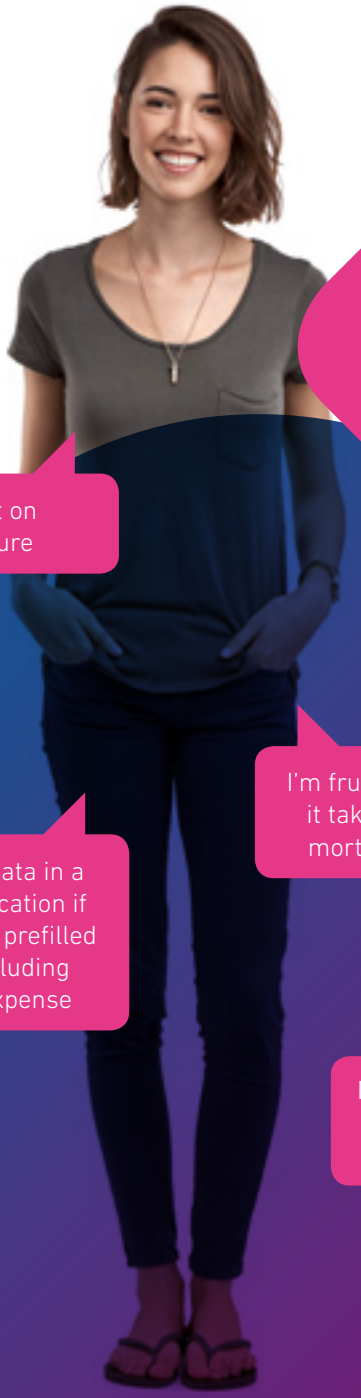
IS ALL AS IT SEEMS?

Fraud in mortgages is not reported accurately by lenders, simply because it's difficult to classify.

Consequently, while it looks like there are more victims of mortgage-related identity theft, these applications could actually be first-party frauds from people giving false information to get a mortgage.

Even then, it's important to consider whether the false applications are deliberate. Are people aware that giving false information could classify them as fraudsters – or do they simply not have accurate data to input?

If it's the latter, new data sources such as bank account transaction data delivered by open banking can help with accurate form-filling, as it can prepopulate income and expenditure. Meanwhile, new analytics such as categorisation can instantly validate and verify income based on a person's current account transactions. Together, technologies such as this can better classify applicants and eradicate inaccurate fraud measurements.



80%
of people got their financial commitments wrong in actual versus perceived

50%
I overcommit on my expenditure

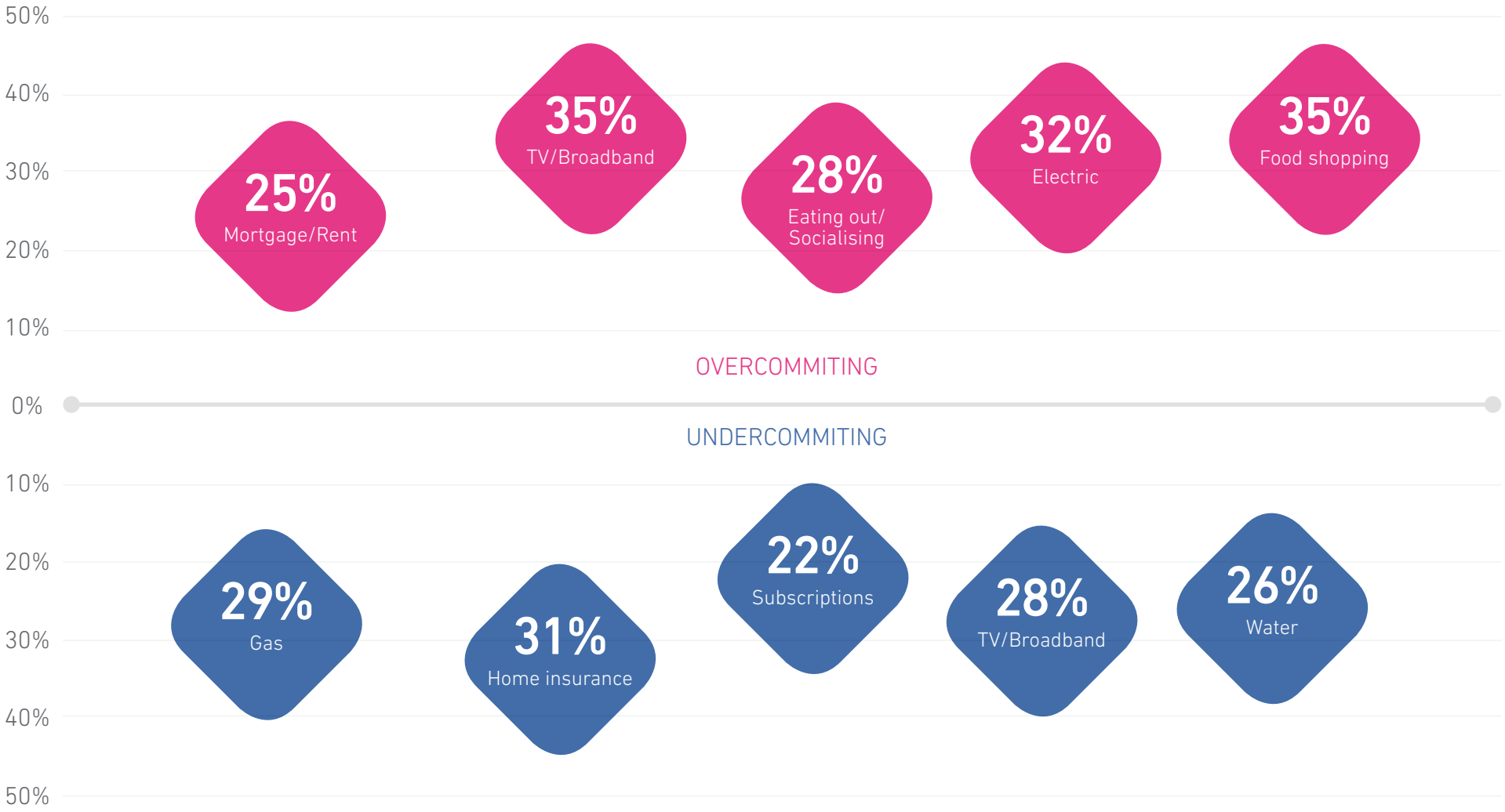
76%
I'm frustrated in the time it takes to complete a mortgage application

80%
I would share data in a mortgage application if meant data was prefilled for them – including income and expense

15%
I have increased my salary on a mortgage application to get a better rate

The reality of unawareness

Most people (80%) are unaware of how much they pay per month on static bills. The graph highlights the key areas where most consumers are inaccurate in assumptions.



More personal loan fraud

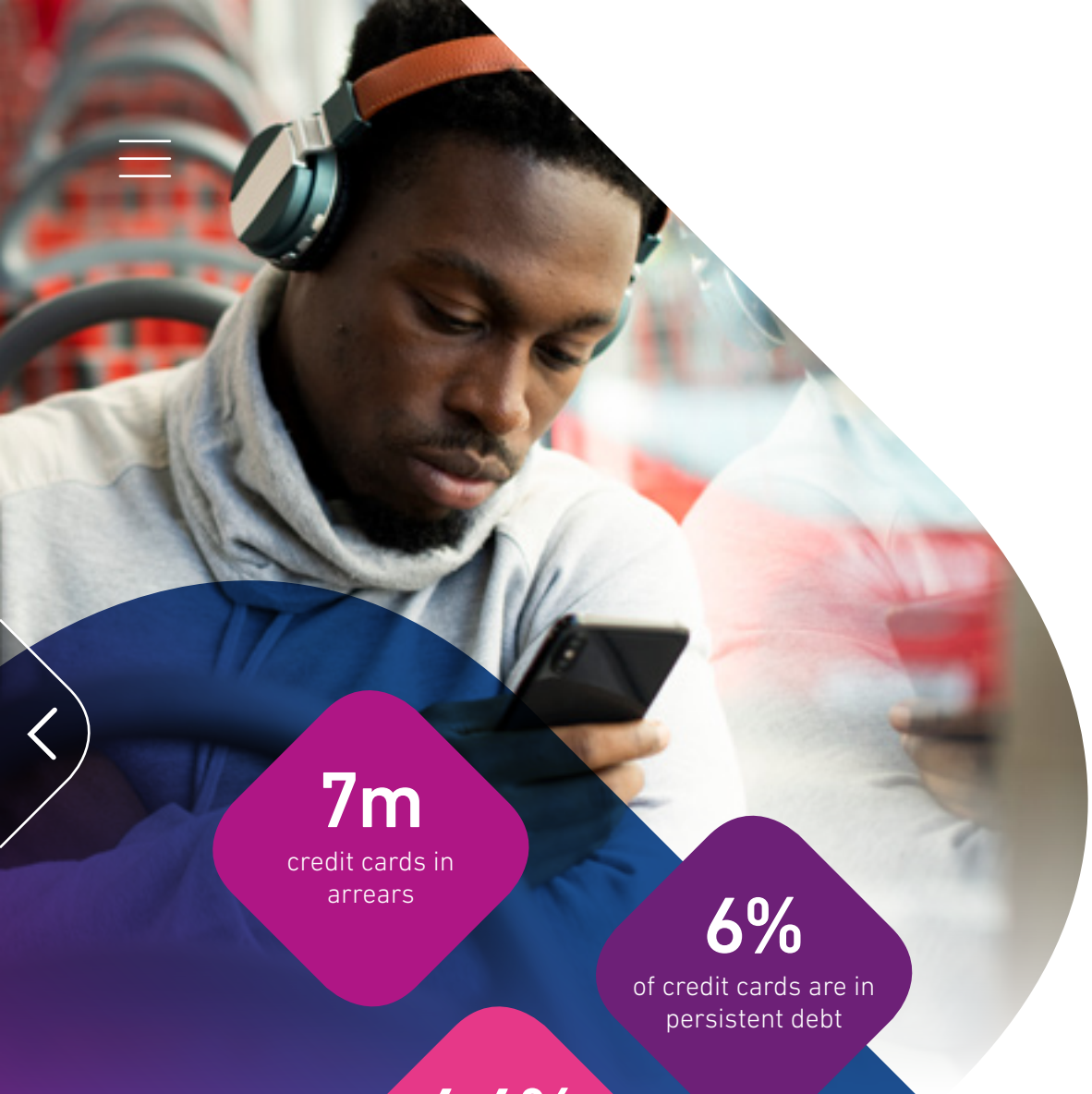
The amount of first-party fraud on personal loans has grown 21% compared to the levels seen in 2014. There is also a rise in applications for high value loans (£20k - £40k) spread over longer terms (7-10 years).

This could be fraudsters targeting instant high value gains, and spreading payments over a longer time period in order to qualify for the affordability checks.

Fraud type distribution
loans (indexed where 2015 Q1 = base)

28%
rise in arrears on personal loans, particularly seen in values of £20-40k

6.3%
new personal loans increase since 2017



7m
credit cards in arrears

6%
of credit cards are in persistent debt

4.4%
growth in new credit card lending

More third-party credit card fraud

Third-party credit card fraud rose by almost 31% from 2017 to 2018. However, first-party credit card fraud has reduced, with Q3 2018 starting to show an incline once again. With a higher proportion of credit cards today with revolving credit balances and persistent debt, this change could be a result of fraudsters not getting access to the amount they seek, and therefore switching efforts. The trends support this switch.

Fraud type distribution
cards (indexed where 2014 Q1 = base)

More women committing first-party fraud

The majority (66%) of first-party fraud is from men, it has been reducing year on year.

The number of women committing fraud has grown a staggering 62% over the same timeframe; thats double the growth, and makes women committing fraud stand 45% higher than 2014 (compared with 26% for men).

Increase in third-party fraud against new groups

Fraud is ever fluid, and the increase in fraud against new groups of people is proof of this. Fraudsters are casting their net wider, typically to older communities, and to those in more rural locations.

The Country Living Mosaic group, for example, is defined as well-off homeowners in rural locations enjoying the benefits of country life. This group is actually the least likely group to be victims of fraud, being 70% below what would be expected for their population size.

Nevertheless, they saw a 29.5% increase in incidents of fraud over 2018. The Suburban Stability Group – mature suburban owners living settled lives in mid-range housing – also suffered 7.5% more incidents of fraud in the same timeframe. Perhaps most worryingly of all, elderly people reliant on support to meet financial or practical needs (the Vintage Value group) saw an increase in fraud of 16%.

Older ages see an emerging threat

As to why this is this happening, it could be general vulnerability brought about by a host of changing behaviours. Those aged 50 and over, for example, were last year more at risk of being a victim of fraud. This could be a consequence of the former pension release, but equally as they typically have more accessible savings and available credit funds, compared to other age groups.

Education is needed, across all age groups

The younger victims in these demographics, meanwhile, are a bigger target for fraud given their willingness to live their lives online and share data through apps and wearables. This data can help a fraudster impersonate an identity much more effectively today than it could even just few years ago.

To tackle this increase, the people within each group need more education on steps they can take to protect themselves. It's vital that older people, especially, are reminded not to write down or share passwords or account details. Everyone should also check their credit file regularly for signs a fraudster is using their identity.

From a business viewpoint, the answer is to identify points of vulnerability and sharpen your defences by bringing in real-time fraud analytics.

140,000

people aged 55 and over have been reached through our financial education programme to help prevent fraud

£91k

On average, victims of pension scams lost £91,000 each to fraudsters in 2017

Source: Action Fraud

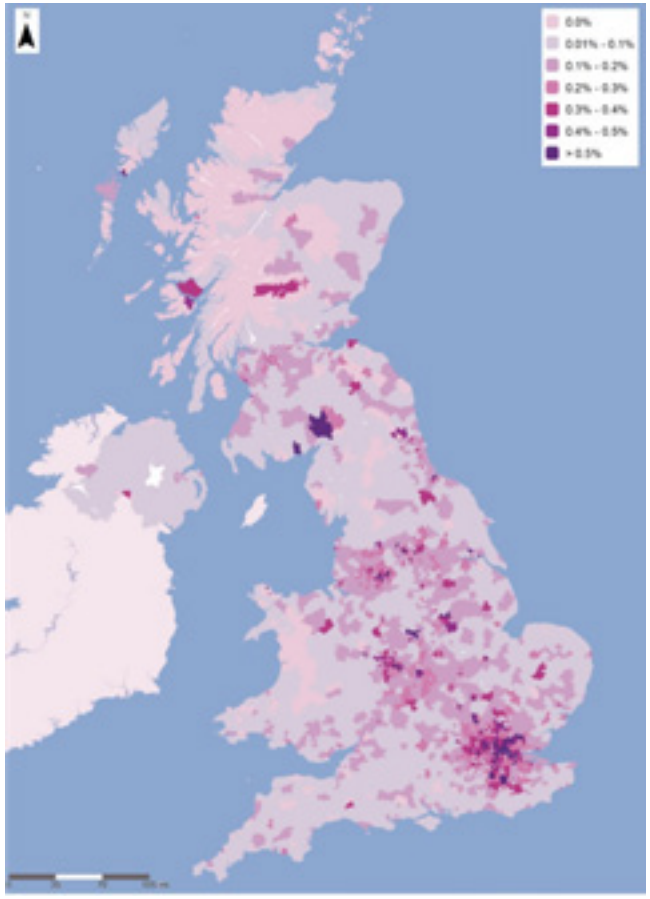
70%

Country Living are the least expected to be fraudulent

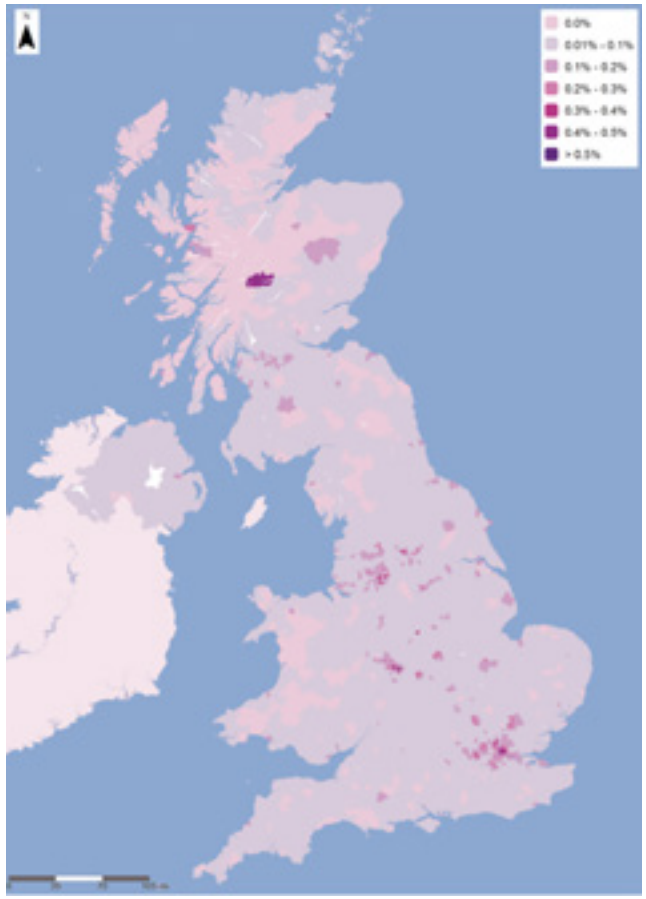
FIRST-PARTY FRAUD BY GEOGRAPHY

London is the overall hot spot for fraud in the UK, and has been for some time. Glasgow, the Midlands, Liverpool and Manchester also show highly concentrated areas of fraudulent activity.

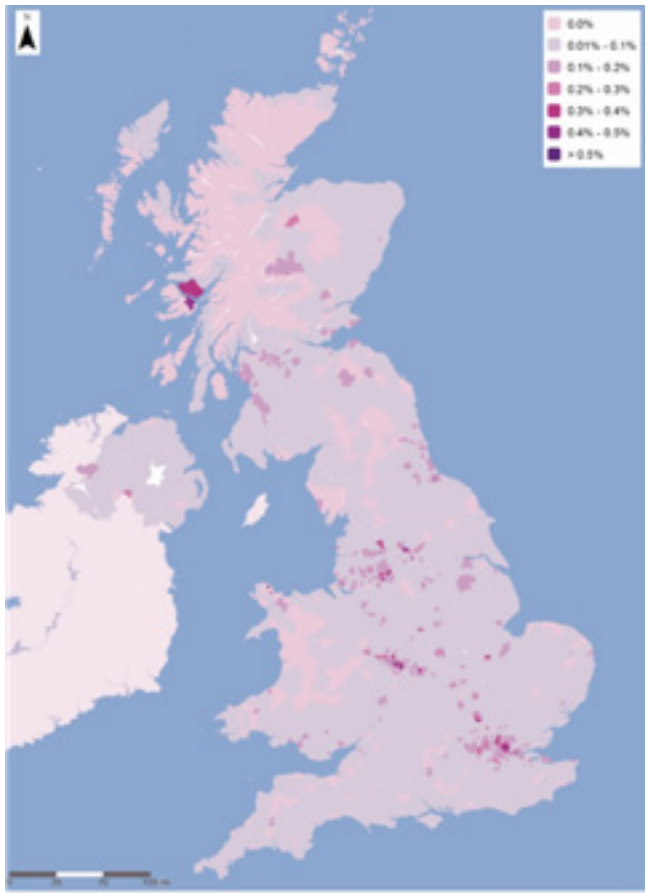
Total fraud



2018 First-party fraud



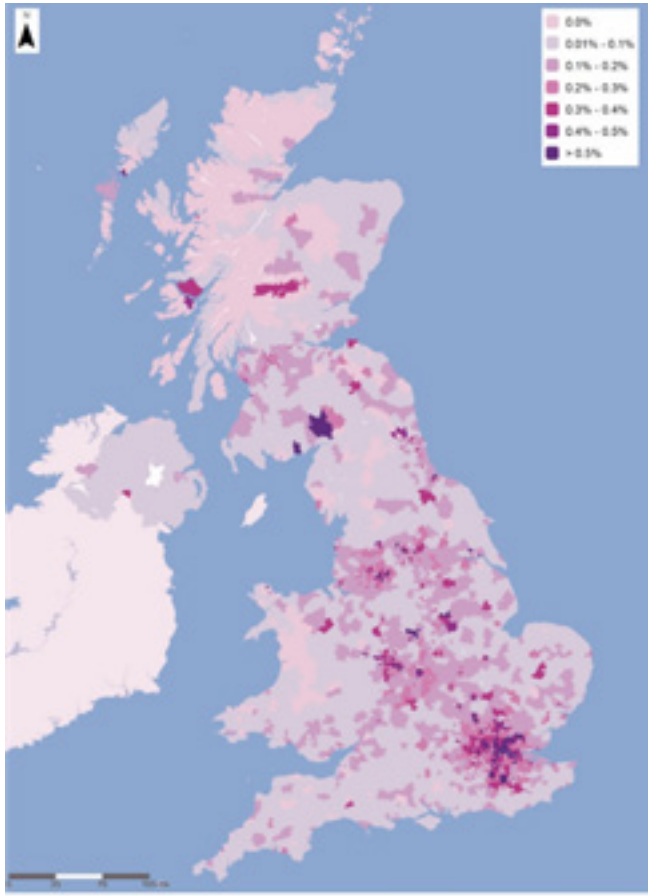
2019 First-party fraud



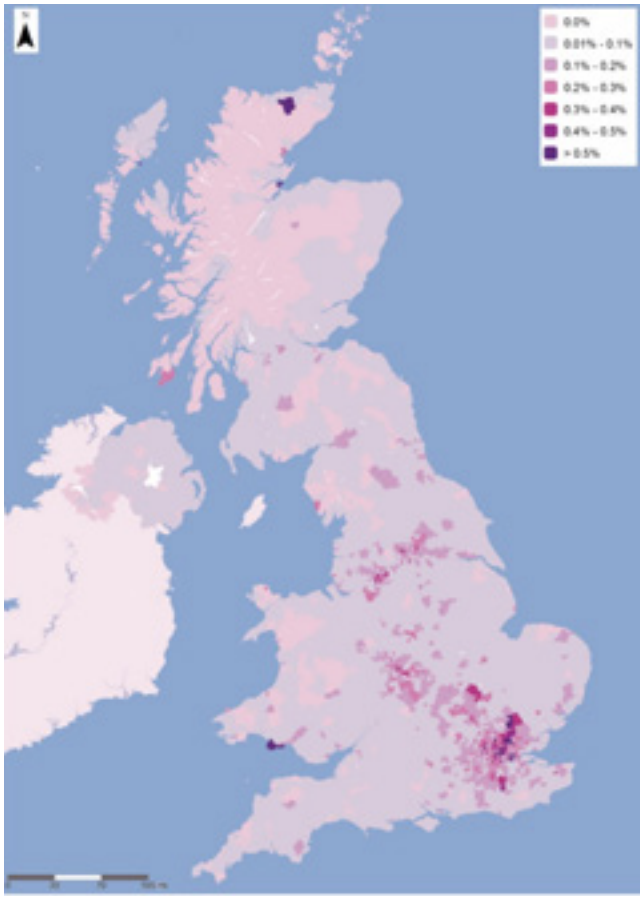
† 2019 Fraud shown for H1 only

THIRD-PARTY FRAUD BY GEOGRAPHY

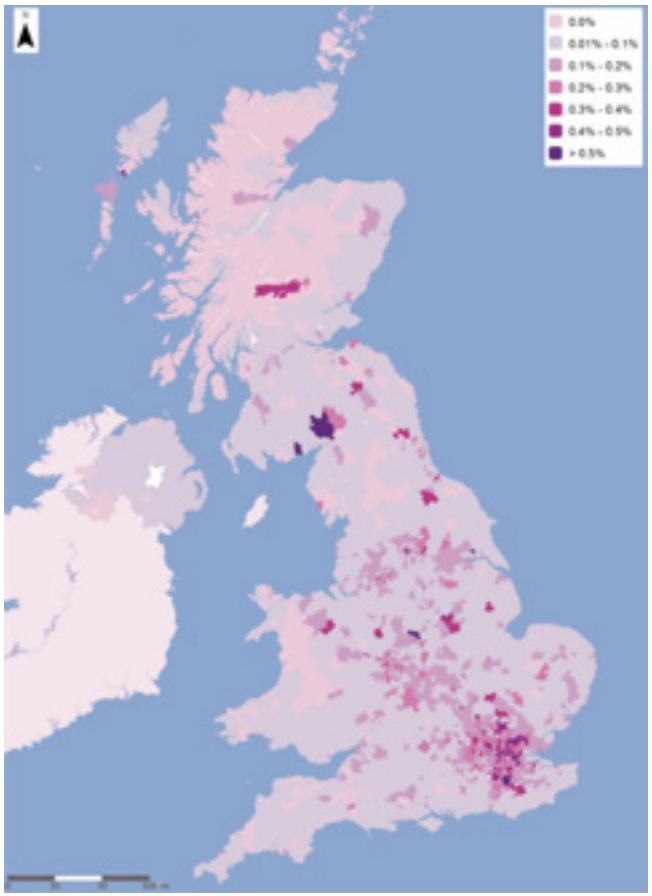
Total fraud



2018 Third-party fraud



2019 Third-party fraud



† 2019 Fraud shown for H1 only

CASE STUDY: SAGA SERVICES

Application fraud and Ghost Broking were specific significant challenges for Saga and contribute towards the rising losses they faced. In addition to this fraudsters using compromised identities and/or stolen identities.

By integrating FraudNet at the point of a quote, Saga could benefit from reducing the costs incurred from fraud losses at the point of a policy purchase and better automate fraud cases. Within the first 30 days, FraudNet helped Saga detect a sizeable Ghost Broking ring.

> "The FraudNet system has proved its worth even in the short term and now we understand how we can continue to expand on this, but not impact our other objectives such as customer experience."
>
> Ste Teeling, Head of Financial Crime, Saga

FraudNet detects 25% to 400% more instances of device fraud than traditional tools

With more devices than ever being used to carry out transactions online, the opportunities for device fraud are increasing.

FraudNet from Experian identifies every device visiting a site and highlights fraud indicators, including inconsistencies, transaction volume and velocity from a single device. Research suggests that finance providers implementing FraudNet are seeing a consistent downward trend in attack rates – likely because fraudsters are realising that the business is protected.

FRAUD TRAITS

HOW FRAUD IS CHANGING

FRAUD: HOW IT'S BEING DONE

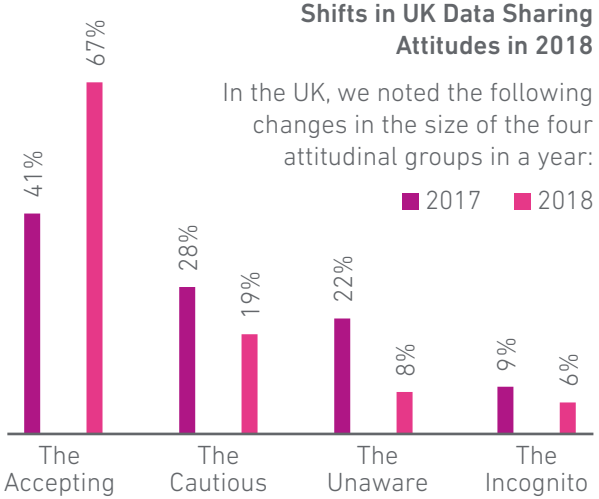
Fraud attacks can be very fast, and methods change constantly. What's more, when new fraud methods enter the landscape, they are rarely easily overcome, instead compounding the existing problem.

This constantly shifting threat is fuelled by the huge volumes of data today's customers share on social media sites, online shopping sites or by email. It's also fuelled by fraudsters' relentlessness: they are continually testing systems to understand potential gaps in defences, which are common where no multi-layered fraud prevention strategy exists.

Year on year, more people, across all ages, are more accepting of sharing data online – trust in who they share with remains a crucial factor.

Shifts in UK Data Sharing Attitudes in 2018

In the UK, we noted the following changes in the size of the four attitudinal groups in a year:



Below are the most common ways in which fraud is carried out today.

Account takeovers

In our 2019 Global Identity and Fraud Report, 55% of businesses reported an increase in online fraud-related losses over the past 12 months. Account takeover attacks were a major cause of this.

Account takeovers are now one of the biggest challenges facing organisations. They happen when fraudsters use a victim's personal information to take control of an existing bank or credit card account, and to carry out unauthorised transactions. Often this is possible because of previous security breaches, such as fraudsters taking over customers' email addresses or SIM cards, which allows them to sneak through the usual security checks.

Artificial Intelligence

While there has been a rise in the use of AI and machine learning to fight fraud, in certain specific scenarios these tools can also be used to commit fraud.

For example, AI can be used to commit machine-to-machine fraud, where AI bots disrupt production processes or interfere with customer communications; this is often referred to as Dedicated Denial of Service attacks (DDoS).

Man-in-the-middle or man-in-the-browser attacks

Criminals take over a genuine customer's device to commit fraud, thereby side-stepping device identification and authentication defences.

Synthetic identities

Criminals combine real customer data with fake information to create entirely new identities, and use them to open accounts and commit fraud.

55%

of businesses reported an increase in online fraud related losses over the past 12 months

57%

Of businesses plan on increasing budgets for AI, with fraud prevention being a top priority

Use of 'mules'

Through second-party fraud, a person or 'mule' willingly gives their identity to be stolen for fraudulent use.

This type of fraud is common in a range of industries, including financial services and telecommunications. Customers sometimes take out phone contracts that include devices, and cash-in their devices – later claiming that they never took out the contract in the first place.

Hyper-personalized fraud – including phishing

Criminals use personal information available in the public domain – on social media accounts, for example – to create elaborate, highly personalised fraud attacks; for example, phishing scams directed at individuals responsible for making payments in a business.

Trojan Horse – the stallion of fraud

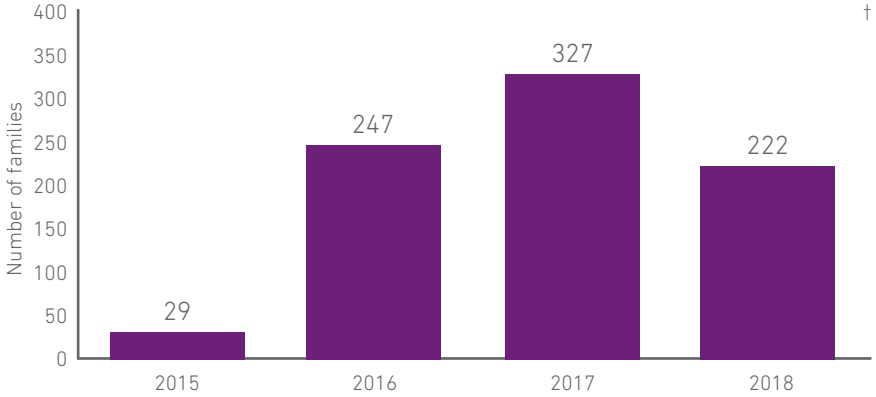
Disguised as legitimate software, Trojans can be employed by cyber-thieves and hackers trying to gain access to users' systems. Users are typically tricked by some form of social engineering into loading and executing Trojans on their systems. Once activated, Trojans can enable cyber-criminals to spy on a customer, steal sensitive data, and gain backdoor access to systems.

93%
of all phishing emails contained encryption ransomware
(end March 2018)

56%
of 1,379 reported malware incidents involved ransomware

Ransomware

According to Verizon's 2018 Data Breach Investigations Report, 93% of all phishing emails contained encryption ransomware as of the end of March 2018. Additionally, the report shows that ransomware was the most common type of malware reported during the year with 56% of 1,379 reported malware incidents involving ransomware.



This statistic depicts the total number of newly added ransomware families worldwide from 2015 to 2018. In the most recently measured period, there was a total number of 222 newly discovered ransomware families. Comparing it to 2017, this was a decrease, to which there was a total of 327 newly discovered ransomware families.

†www.statista.com/statistics/701029/number-of-newly-added-ransomware-families-worldwide/

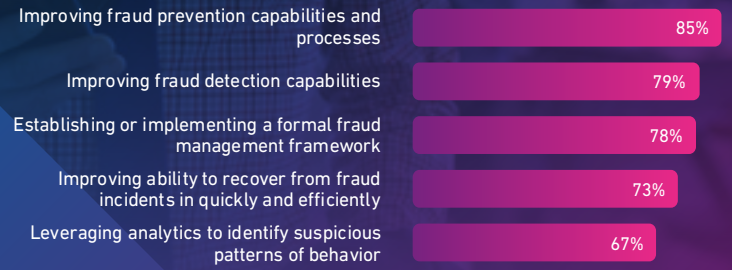
ARE BUSINESSES TAKING FRAUD SERIOUSLY?

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.

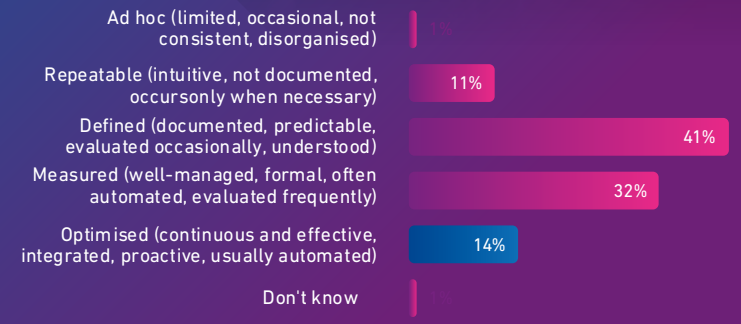
Businesses recognise the growing risk fraud presents and its direct impact. In an effort to tackle the rising challenges it poses and minimise the impact, firms are investing more time and resources into fraud management.

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, while also managing budgetary constraints, recruitment, talent retention and related manpower challenges.

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



Firms' ability to prevent fraud



THE CUSTOMER IMPACT

HOW FRAUD IS ERODING TRUST

THE CUSTOMER IS KING

When Forrester surveyed 702 global managers on our behalf about their organisations' business priorities for the coming year, improving the customer experience was their top response. This was closely followed by the desire to improve data/information security across the organisation, and also the desire to improve customer trust and satisfaction.

However, 32% of the same respondents said that increased exposure to fraud is prohibiting them from accomplishing these initiatives. The only thing they believe to be holding them back more is the threat from new and existing competitors.

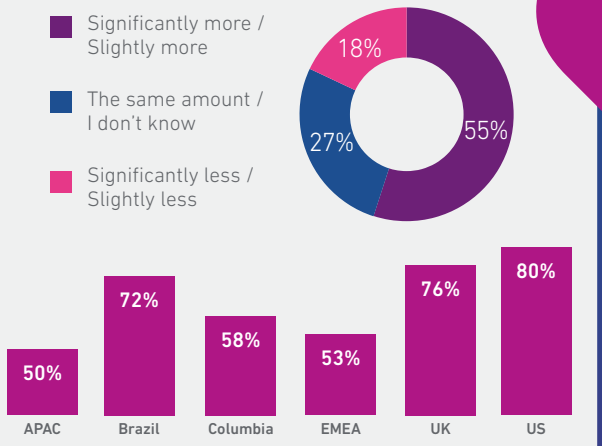
It's true that fraud prevention and customer satisfaction are not, on the surface at least, natural bedfellows. In order to prevent online fraud, for instance, traditional online fraud checks with lengthy or multiple forms to fill are 'high friction', and result in abandoned transactions and lost business. What's more, they're not even effective. According to the Experian Global Fraud and ID Report 2018, more than 70% of business leaders admit to blocking far more genuine transactions than they should, simply because they cannot authenticate them effectively.

It's heartening to see that 50% of businesses report an increase in their fraud management budgets. However, 55% of the same businesses report that online fraud losses are slightly or significantly more than they were in 20186. Arguably, businesses are therefore investing their growing budget into the wrong fraud prevention capabilities.

"Arguably, businesses are investing their growing fraud budgets into the wrong fraud prevention capabilities."

Online fraud losses have increased in the past year

In the past 12 months, has your business experienced more, less or the same in fraud losses?



APAC countries surveyed include: Australia, China, Hong Kong, India, Japan, New Zealand, Singapore, Indonesia, Malaysia, Thailand and Vietnam

EMEA countries surveyed include: Germany, Austria, France, Spain, The Netherlands and South Africa

50%
Half of businesses are increasing budgets for fraud controls

55%
Yet more than half have experienced more online fraud

CX
Improving customer experience is the top priority for businesses in the UK and EMEA regions

32%
Yet a third have increased exposure to fraud

How to tackle fraud while boosting customer service

To win, retain and safeguard genuine customers, you need to give them fast, secure access to your business via multiple channels. Typically, this has meant reducing onerous security controls, often positioning IT, marketing and fraud at odds with one another.

However, our research with executive business leaders has shown that when the brand was put first (i.e. reputational risk), stakeholders expanded from IT to include both marketing and fraud prevention teams. This suggests that the tension between customer experience and data security can give way to cross-functional alignment and integration among teams to deliver both security and convenience.

By shifting business attitudes to fraud, and adopting more sophisticated authentication strategies and tools, your business can start to combat fraud more effectively while delivering the online experiences your customers expect. Analytics can also help you get more out of the information you already own, enabling you to build comprehensive 360-degree views of each of your customers. Through this data-led approach you can design friction-free customer journeys that authenticate your genuine customers while mitigating your exposure to risk.

A frictionless journey looks like this:

1. The lender validates the customer based on pre-qualification and initial fraud checks.
2. The lender completes credit bureau, affordability, and/or existing customer behaviour checks.
3. The lender approves and accepts the application and the customer is verified and authenticated.
4. The lender screens the applicant against PEPs lists, sanctions lists and watch lists as appropriate.
5. The lender releases the funds into the customer's bank account within five minutes.

"Nearly half of decision makers expect machine learning and AI to be far more prevalent in risk management and fraud prevention in the next three years."

THE CHALLENGE FOR BUSINESSES

THE BARRIERS TO OVERCOME, AND THE OPPORTUNITIES TO IMPROVE

MACHINE LEARNING: THE KEY TO BETTER CUSTOMER SERVICE AND FRAUD RISK MANAGEMENT

Nearly half of all decision-makers say they expect the use of machine learning and AI to be far more prevalent in risk management and fraud prevention over the next three years.

In financial services, for instance, banks can use machine learning to analyse applicants' existing bank transactional data in order to assess affordability. The resulting models can then be added into automated decision-making processes, to not only reduce default risk but also remove friction from customer journeys, and enhance the bank's reputation for responsible lending.

Advanced analytics and machine learning can add the power and flexibility of being able to ingest various kinds of third-party partner data, resulting in a more comprehensive, single decision process flow – which is equally powerful for fraud detection and identity verification.

CrossCore, our award-winning fraud platform

The industry's first 'plug and play' award-winning fraud platform, CrossCore, brings together all the fraud and identity services you need to detect and prevent fraud across your business. With simple ways to connect into our partners' fraud solutions, you can create a sophisticated, multi-layered frontline fraud defence and adopt new fraud solutions quickly to counter emerging threats. And because our platform integrates with systems across your business, it provides centralised authentication, helping you minimise friction in your customer journeys across all your contact channels.

THE CONSUMER PERSPECTIVE: SEARCHING FOR TRUST

Despite the risk of fraud facing consumers and businesses, we continue to depend on the digital world. And we expect our digital interactions to be both secure and to instil confidence.

In other words, we want to trust the companies we do business with. To that end, consumers are looking for visible signs of security.

Building trust through advanced authentication

Consumers will willingly work through friction-inducing security methods such as password resets, PIN code push notifications to smartphones, and security questions – simply because they inspire confidence. However, that confidence is likely perpetuated by having no other choice than using these methods.

When exposed to more advanced authentication, such as physical biometrics, our research suggests that consumer confidence increases significantly. In fact, the use of physical biometrics seems to have the largest positive impact on trust, particularly in Colombia and the United States.

Businesses are coming around to this, and realising that consumer desire for convenience and security is unachievable without the latest technology and authentication methods.

74%

of consumers have more confidence in a business that uses physical biometrics for security

Physical biometrics inspire most trust in Columbia and USA

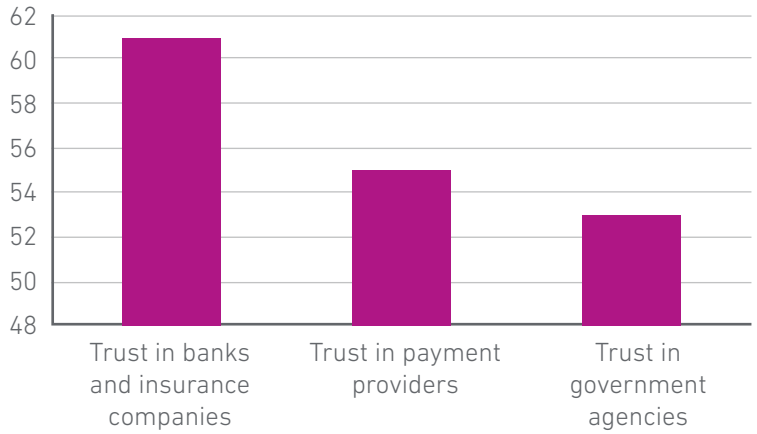
Most important elements of a consumers' online experience

Which of the following services is most important to you when it comes to your online experience?

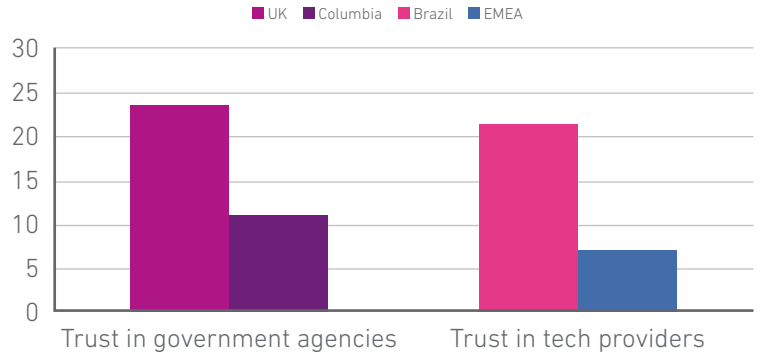
Different countries, different organisations, different levels of trust

Trust in an organisation's ability to safeguard customer data varies considerably according to the country and the type of business.

Overall consumer trust by industry (%)



When this data is broken down, however, some gaps in trust grow more transparent. For example:



The reasons for this are probably a heady mix of social, political, cultural and historical factors. But understanding that there are differences can empower organisations to tailor their fraud management strategies according to their market.

EXPLORING CONSUMER TRUST

Consumer adoption of digital channels has skyrocketed in recent years due to increased convenience and accessibility to greater product selection and personalisation.

90%

of consumers would be willing to go through a more thorough identity verification process upfront in exchange for seamless access to their accounts later.

76%

of consumers have more confidence in a business that uses physical biometrics over passwords, and they trust a business using physical biometrics to better protect their information.

86%

of consumers said engaging with a business that is protecting them from online fraud and/or identity theft is the top factor in their online experience.

76%

Consumers who have greater trust and confidence in businesses that give them control over the use of their personal information — how much, with whom it's shared and a clear understanding of the tradeoffs for sharing more (or less).

66%

Consumers who conduct their online banking on their smartphone, followed by 59% who use their laptop. However, when asked which they prefer, 45% said smartphone (up 16% from 2017) and 28% said laptop (up 9% from 2017).

MEASURING UP

The world may be round but trust is relatively flat.

In our survey, 4 out of the top 5 countries where businesses are most trusted – include: India, Thailand, Vietnam, Indonesia and Brazil. These higher levels of trust may be the result of digital transformation initiatives such as digital IDs, e-commerce payment infrastructure and social payments being led by government and businesses in those countries.

76% of countries included in the survey fell in the low range, including the United States, the United Kingdom, Colombia and China. No country scored high or very high for trust, putting pressure on those in the moderate range to improve their own standings and also serve as the beacon for other countries to follow.

List of countries in descending order of trust

India 47	Thailand 46	Vietnam 45	Indonesia 43	Brazil 40	US 37	Columbia 36	Malaysia 35	Spain 34	South Africa 33	UK 33
Australia 33	Austria 32	New Zealand 31	Singapore 31	Netherlands 28	Germany 28	Hong Kong 28	France 27	China 27	Japan 21	

CONCLUSION: TACKLING THE FRAUD PROBLEM

A higher number of attacks. Attacks of different types and using new technologies. New criminals, new targets and new geographies. While organisations are spending more money on fraud, the fluidity of the fraud landscape shows that current efforts are not solving the problem. New methods are needed to protect consumers from threats while working to gain their trust.

The first part of the solution is data

Data based on consumer biometrics, channel preferences, and the devices they use can massively simplify customer authentication. Data can also identify potentially fraudulent behaviours, such as toggling between websites and spreadsheets to input stolen customer information.

Importantly, you should not only rely on data from within your business. Organisations must be willing to share their fraud data with others in the industry, to help everyone improve their defences. This is no time to be protective; quite simply, if one company suffers the fallout from fraud, it affects the reputation of all.

Simply owning the data is not enough

It must be joined up, analysed and constantly refreshed, and the insight must be deployed across all channels and customer touchpoints – fast, and at scale – in order to be effective. That's why the second, key part of the solution is the creation of an integrated environment, which uses the latest technologies such as AI and machine learning, to turn that information into insight and action company-wide.

Inspire trust through a multi-layered agile strategy

By adopting a risk-based authentication approach through a multi-layered, agile strategy, you can both inspire consumer trust and deter fraudsters. You can showcase your security measures to your customers at appropriate points in their journey – introducing just the right amount of friction that they expect – and hidden at other points, so that fraudsters remain unaware.

Through risk-based authentication, company-wide data analytics and constant, industry-wide data refresh and exchange, you can give yourselves the best chance of protecting your customers and your business – all in the hope that one day, we can report that fraud is not increasing, but decreasing.

Key ingredients for fighting fraud include:

Data | Analytics | Technology | Collaboration

HOW EXPERIAN'S AWARD-WINNING FRAUD AND IDENTITY PLATFORM CAN HELP YOU

Introducing CrossCore™

CrossCore™ is the first smart, open, plug-and-play platform for fraud and identity services. It delivers a future-proof way to modify strategies quickly, catch fraud faster, improve compliance, and enhance the customer experience.

It does so through a modern technology approach that combines a flexible and scalable API with powerful workflow and decisioning functions, allowing you to connect, access, and orchestrate decisions across multiple systems more effectively. In addition, because no single system will ever have all the answers, CrossCore is open. This means it supports a best-in-class approach to managing a portfolio of services that work together in any combination — including Experian solutions, third-party services and client systems — to deliver the level of confidence needed.

Key benefits

- A future-proof way to manage fraud and identity services.
- Reduce risk across fraud and compliance by speeding the time-to-market with new tools and strategies.
- Drive top-line growth by reducing the friction and false
- positives that cause customer fallout.
- Increase operational efficiency by avoiding needless referrals and driving down the cost to deploy new tools and strategies.

What CrossCore™ delivers:

A future-proof way to manage fraud and identity services.

- Start quickly by turning on Experian services through a single integration.
- Connect to services quickly with a common, flexible API.
- Act quickly to adapt to changing conditions and new risks with built-in strategy design and workflow capabilities.

Strategies that deliver the level of confidence required at a transaction level.

- Specify which services are needed in which order based on the workflow logic and decision criteria for each transaction.
- Call services all at once or in sequence based on decision logic.
- Precisely tailor strategies based on transaction type.

Capability to optimise decisions across services.

- Orchestrate decisions across disparate systems.
- Control the data being used in decisions.
- Apply client-specific data and analytics to decisions.

Ability for risk-management teams to take control and move at the speed of fraud.

- Create, deploy, and manage strategies more easily.
- Reduce burdens on IT and Sciences teams.
- Make strategy changes dynamically, with no downtime

ABOUT THE RESEARCH AND INSIGHT CONTAINED WITHIN THIS REPORT

Research insights

Research contained within this paper, unless sourced otherwise, is an extraction from Experian research commissioned through 2018 and 2019. This includes research with third-parties including Forrester Consulting, as well as consumer research conducted on Experian's behalf through C Space. Additional data insights are derived from data sources such as National Hunter and the credit bureau.

- Read from our research commission to Forrester Consulting **here**
- To read insight from our Global Data Management trends, **click here**
- For a full view of the UK Fraud trends, please view our **fraud stats** and **fraud map** – also see our Global Fraud and Identity report **here.**

For more information on any specific quotation, **please contact us**.

About Experian

Experian unlocks the power of data to create opportunities for consumers, businesses and society.

At life's big moments – from buying a home or car, to sending a child to college, to growing a business exponentially by connecting it with new customers – we empower consumers and our clients to manage their data with confidence so they can maximise every opportunity.

We gather, analyse and process data in ways others can't. We help individuals take financial control and access financial services, businesses make smarter decision and thrive, lenders lend more responsibly, and organisations prevent identity fraud and crime.

For more than 125 years, we've helped consumers and clients prosper, and economies and communities flourish – and we're not done. Our 17,200 people in 44 countries believe the possibilities for you, and our world, are growing. We're investing in new technologies, talented people and innovation so we can help create a better tomorrow.

C-00279

Learn more at **www.experianplc.com**

To find out more about our services, visit our website: **www.experian.co.uk/business**