ACCURA

RESEARCH 2016

FIGHTING FRAUD

UNDERSTANDING PEOPLE'S ATTITUDES
TOWARDS THE USE OF PAYMENTS DATA

VOCALINK

EXECUTIVE SUMMARY

JIM WADSWORTH
MANAGING DIRECTOR, ACCURA

This research into people's views regarding the use of transactional data to combat fraud is part of a series of reports from Accura, VocaLink's insight business.

We live in a world with a transactional data landscape. Every minute of every day, simply by going about our normal day-to-day activities, we are generating information through the payments that we make. In the UK, the amount of data created amounts to 11 billion yearly transactions and a total annual payments value of £6trn. VocaLink has therefore created Accura to apply cutting-edge data science techniques to payments data, developing solutions that solve known problems for the benefit of us all – including fighting fraud.

Payments data – that includes transfers of money between bank accounts, or paying a bill by Direct Debit or standing order – is to some extent already being used in the fight against fraud.

Banks and other financial institutions use the data currently available to them to spot irregularities and anomalies that may indicate potential fraud. But there are challenges, especially with non-card payments, where traditional anti-fraud solutions struggle to identify and flag fraudulent transactions before money leaves an account. Additionally, financial institutions currently only have a partial view of the scale problem (i.e. the total value of fraudulent payments), and of fraudulent payments and accounts within the banking system.

Feedback from stakeholders, including banks, financial institutions and credit reference agencies, confirms interest in analysing payments data – but what does the public think about further analysis of their transactions to fight fraud?

Our research suggests that people care more about combating fraud than they fear the misappropriation or misuse of transactional data. That gives the industry confidence to use transactional data to develop stronger protections against fraudulent activity.

This study also shows that people have concerns and suspicions about who is accessing their data and for what purpose. Even where an appropriate reason is declared, people may still lack a clear understanding of what is already happening.

Banks and financial institutions will need to provide an easy-to-understand explanation of the benefits to the public and address any specific concerns in order to ensure that people are comfortable with the analysis of transactions to help fight fraud.

The research gives the industry confidence to use transactional data to develop stronger protections against fraudulent activity, but it is equally clear that communication about the safeguards regarding using data in this way is a vital component in ensuring people's acceptance.

I hope you find this research useful and I encourage you to continue the debate through our online hub VocaLink CONNECT.

This report is the first in a series of three investigations examining people's attitudes towards using transactional data to address problems that affect us all.

Sign up at **connect.vocalink.com** to be alerted to the launch of our future reports.

FOREWORD

SAMANTHA MALONEY
HEAD OF MARKETING, ACCURA

The addition of new and previously untapped data could enable the development of new solutions to help combat fraud as well as improvements to existing ones.

For example, the secure processing of high volume, secure payments in the UK currently accounts for 90% of salary payments and 70% of household bills, and covers 85% of the total UK workforce. This accurate, timely and structured dataset generates 11 billion yearly transactions and could be harnessed to combat fraud as well as for a variety of other beneficial uses.

VocaLink is a critical part of the UK's payments infrastructure and has blazed a trail in innovation and thought leadership in the payments industry for more than 40 years. Building on VocaLink's position as a trusted provider of secure and reliable payments processing, it has created an insights business, Accura, to create innovative solutions that enable better-informed decisions and solve known problems.

As part of this process, Accura conducted research in the first half of 2016 into people's attitudes towards the use of existing transactional data from the payments systems. This looked in detail at a number of possible applications for this data, one of which was to help stop fraud. It explored people's views: their acceptance of the use of transactional data in this way and the reassurances and safeguards that might mitigate their concerns.

ABOUT OUR STUDY

This research was conducted in association with Ipsos MORI and with input from Elaine Kempson, Director of the Personal Finance Research Centre (PFRC) and Professor of Personal Finance and Social Policy Research at the University of Bristol, during the first five months of 2016.

Initial exploratory research was used to identify the range of views, experiences and opinions of 55 adults. Qualitative research is designed to be illustrative and can not only tell us what people think, but why they do so. Ipsos MORI conducted seven two-hour focus groups, the insights from which drove the development of our follow-up quantitative survey, conducted both online and face-to-face.

Ipsos MORI then interviewed 1664 GB adults (aged 16+) between 22nd April and 9th May 2016. A total of 558 people were interviewed face-to-face and 1,106 people were interviewed online. The resulting data was weighted to be representative of the known population by gender, age, region and social grade[1].

Weighting was also applied by access to the Internet to take into appropriate account the 14% of the adult population who do not have such access.

Professor Elaine Kempson provided expert assistance at all stages of the study. Elaine is a recognised international expert on both research and policy analysis on personal finances.

PEOPLE'S VIEWS

WOULD YOU ACCEPT USE OF DATA TO COMBAT FRAUD?

OF PEOPLE SAID THEY WOULD FIND THE USE OF DATA TO COMBAT FRAUD 'ACCEPTABLE'

OF PEOPLE SAID THEY WOULD FIND THE USE OF DATA TO COMBAT FRAUD 'ACCEPTABLE' IF THERE WERE SAFEGUARDS IN PLACE

OF PEOPLE SAID THEY WOULD FIND THE USE OF DATA TO COMBAT FRAUD 'UNACCEPTABLE'

SAID THAT THEY DID NOT HAVE A VIEW ONE WAY OR THE OTHER

The majority of people interviewed accepted the principle of using transactional data to combat fraud, if there were safeguards in place.

Among those who found this use of transactional data acceptable, or who would do so with safeguards in place, it is the frequent internet users - those who use the internet several times a day - who have the highest level of acceptance (74%) compared to 63% of those who access the internet less frequently and just 32% of those who don't use the internet at all[2].

Similarly, social grades ABC1 (73%)[3] are more accepting than social grades C2DE (60%)[3]. Men and women have broadly the same attitude towards data use to combat fraud. Likewise, attitudes towards data use show very little variation across the country.

However, there is a core of people, 16%, who said that even if safeguards were in place they would find this use of transactional data unacceptable. This proportion was highest among the retired and the self-employed (both 19%) and people from social grades C2 and D (19% and 18% respectively).

To understand this reluctance, we looked more closely at why they were opposed to the idea. The main objections centered on concerns about:

- Security and the threat of hacking and criminal exploitation of data – which was likely heightened by high-profile cases of mobile phone hacking at the time of the survey;
- Whether anonymity would be assured;
- With whom the data might be shared;
- A perceived 'major invasion of privacy'.

Indeed, some people were aware or believed that this type of data is already being used in this way and the prospect of further data sharing served to heighten their misgivings.

> I suppose the only downside is a lack of privacy, because obviously your records are there. But in a way I guess it is already happening, because for example your bank protects you from fraud.

London, 31-60, female

When talking to people in the qualitative research groups, it was clear that suspicion exists about 'ulterior motives' concerning the use of data, and people queried whether data collected to fight fraud might also be used for other purposes.

For example, some raised whether it would subsequently be made available to government departments for more wide-ranging 'snooping' – with particular reference to undeclared taxable income – and voiced concerns about protecting the data from misuse.

People will require assurance that their anonymity and privacy will be protected. Our research suggests that simple clarity around safeguards – many of which are already in place – would provide such reassurance.

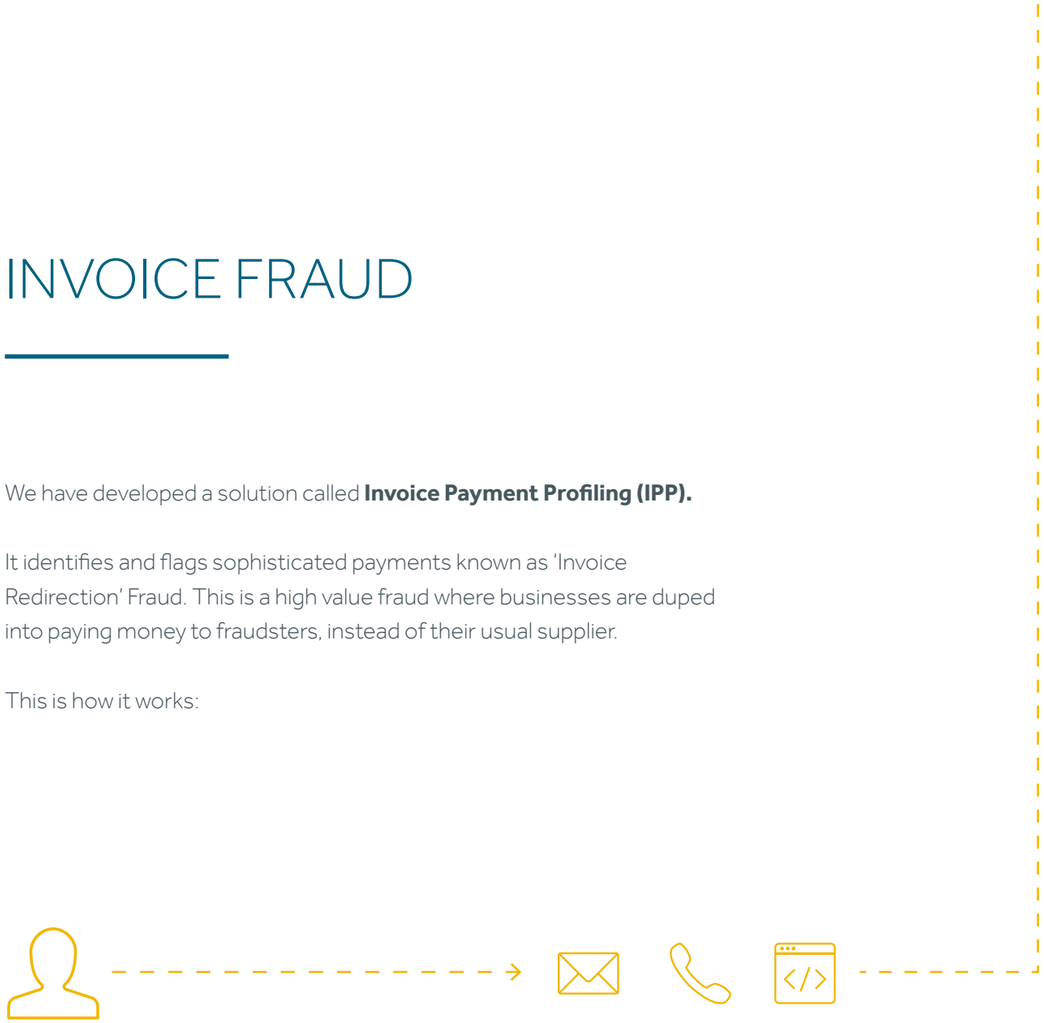
ACCURA

INVOICE FRAUD

We have developed a solution called **Invoice Payment Profiling (IPP).**

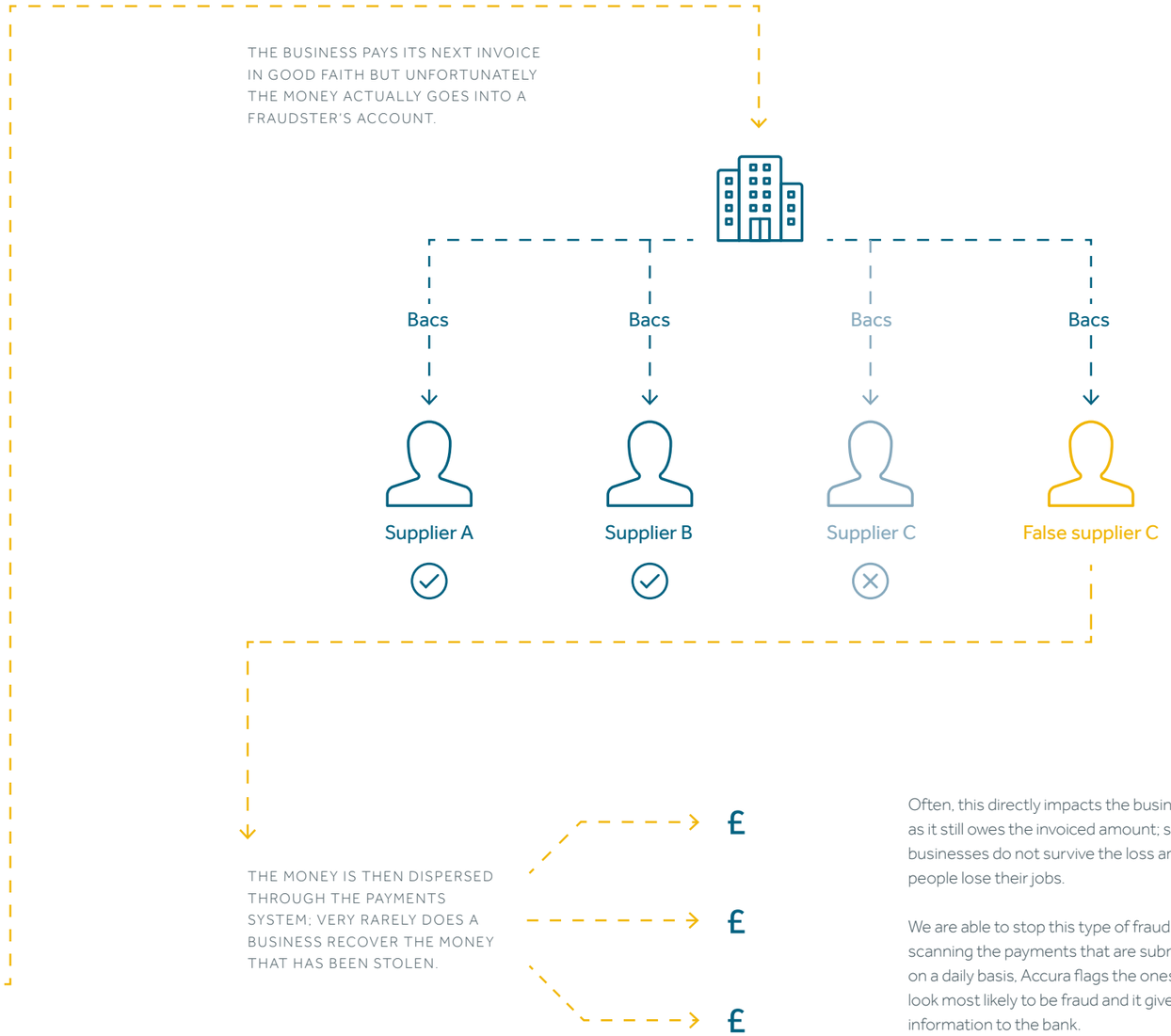
It identifies and flags sophisticated payments known as 'Invoice Redirection' Fraud. This is a high value fraud where businesses are duped into paying money to fraudsters, instead of their usual supplier.

This is how it works:



A FRAUDSTER CONTACTS A BUSINESS, PRETENDING TO BE ONE OF THEIR SUPPLIERS, TELLING THEM THAT THEIR BANK DETAILS HAVE CHANGED.

THE FRAUDSTERS ARE SOPHISTICATED AND MAKE THEIR COMMUNICATIONS CONVINCING - FOR EXAMPLE, SETTING UP DUMMY WEBSITES AND EVEN MANNING PHONE LINES.



Often, this directly impacts the business as it still owes the invoiced amount; some businesses do not survive the loss and people lose their jobs.

We are able to stop this type of fraud. By scanning the payments that are submitted on a daily basis, Accura flags the ones that look most likely to be fraud and it gives that information to the bank.

The bank then has time to contact their customers to either verify that the transaction is real and should go through, or whether their customer has been duped into sending money to a fraudster's account, in which case they can stop the payment before it is made and that money disappears forever.

This service is now live and is already protecting business customers of a major UK bank as we speak.

MAKING DATA USE MORE PALATABLE

If people are broadly open to the idea of their transactional data being used for this purpose, provided there are safeguards in place, what kinds of safeguards are they looking for? What would it take to convert them from being cautiously accepting to become enthusiastic advocates?

In our survey we outlined a series of possible safeguards — including ones that are either already in place through existing regulation and legislation, or which are reflective of sensible, commonplace behaviour. The results highlight once again that people are not really looking for anything new in terms of safeguards, just reassurance that familiar protections are in place and that they work.

Perhaps unsurprisingly, the broadest reassurances give the greatest comfort: 71% of those who had initially either said the principle of data use was unacceptable, or that they would require additional safeguards for it to be acceptable, said they were more likely to accept transactional data use for anti-fraud purposes if **'I knew exactly what the information would be used for and that it would only be used for these purposes'**. Providing that level of reassurance should not be a major challenge for financial institutions since that is what they already do, albeit with seemingly limited public awareness.

More specific reassurances attracted nearly the same level of response. From our list, people said they would be more likely to accept the use of transactional data if:

- 'It was covered by legislation e.g. the Data Protection Act' — 70%;
- 'It was overseen by the appropriate authority, such as the FCA' — 70%;
- 'They knew exactly who would have access to the information' — 70%;
- There were 'guarantees that the information could not be used to identify an individual's data' — 70%.

TABLE 1

This last point raises a paradox: those looking for safeguards around the use of their data do want to be protected from fraud, but seven in ten of these people also want to remain anonymous when their data is analysed for this purpose.

At personal level that simply may not be possible, so the financial services industry needs to develop a robust narrative around this covering what is possible, what is required and why it is important.

The references to legislation and appropriate authorities are particularly interesting, suggesting that people are willing both to defer responsibility and to trust an 'official' agency, were such a stamp of assurance to be offered. This may indicate that, for a significant number of people, the issues of data security and anonymity are more to do with presentation and protection than principle: if the protections above were to be actively promoted when the use of transactional data for fraud prevention were presented, then many objections would melt away. Of the respondents who said they would find transactional data use acceptable if safeguards were in place, between 77% and 86% indicated that those four safeguards would indeed make data use more acceptable. This says loud and clear that safeguards are persuasive and work to build engagement and acceptance.

Most powerfully of all, however, it demonstrates that safeguards, even robust ones, only provide reassurance when they are clearly communicated. If the financial services industry wants to use transactional data to more effectively combat fraud, it will need to engage customers in the process: reassurances only succeed if they are well known and fully understood.

THE POWER OF ASSURANCES

64%

SAID THEY WOULD BE MORE LIKELY TO ACCEPT DATA USE 'IF THE WORK WAS UNDERTAKEN BY A WELL-KNOWN, REPUTABLE ORGANISATION'

64%

SAID THEY WOULD BE MORE LIKELY TO ACCEPT DATA USE 'IF THE COMPANY OR ORGANISATION USING THE DATA WAS ONE I KNEW AND TRUSTED'

63%

SAID THEY WOULD BE MORE LIKELY TO ACCEPT DATA USE 'IF THERE WERE SAFEGUARDS THAT THE DATA COULD ONLY BE USED FOR A FINITE PERIOD OF TIME'

FROM 'NO' TO 'MAYBE'

People who initially said "no" but were persuaded by the prospect of safeguards (see Table 1):

30%

OF PREVIOUS 'NO'S' SAID THEY WOULD BE MORE INCLINED TO ACCEPT DATA USAGE TO COMBAT FRAUD IF 'IT WAS COVERED BY LEGISLATION E.G. THE DATA PROTECTION ACT'

27%

OF PREVIOUS 'NO'S' SAID THEY WOULD BE MORE INCLINED TO ACCEPT DATA USAGE TO COMBAT FRAUD IF 'IT WAS OVERSEEN BY THE APPROPRIATE AUTHORITY, SUCH AS THE FCA'

29%

OF PREVIOUS 'NO'S' SAID THEY WOULD BE MORE INCLINED TO ACCEPT DATA USAGE TO COMBAT FRAUD IF 'THEY KNEW EXACTLY WHO WOULD HAVE ACCESS TO THE INFORMATION'

So, if the principle is established, who should be analysing the data? Responses (64%) suggest that this use of data would best be carried out by organisations that **'I knew and trusted'** or by a **'well-known, reputable organisation'**. Quite who fits into that category lies outside the scope of this study, but trusting the organisation in charge of the data collection and use was less important to people than the nature and rigour of the safeguards they might put in place.

REFERENCES

1

Social grades provide a useful and established framework for analysing the behaviours and opinions of people with differing socio-economic profiles. For the purposes of this piece of research, we have used Ipsos MORI's own structure:

- A High managerial, administrative or professional
- B Intermediate managerial, administrative or professional
- C1 Supervisory, clerical and junior managerial, administrative or professional
- C2 Skilled manual workers
- D Semi and unskilled manual workers
- E State pensioners, casual or lowest grade workers, unemployed with state benefits only

2

Less frequent internet users and those who don't use the internet at all are far more likely to answer don't know to this use of data.

3

74% of As, 76% of Bs and 71% of C1s were accepting of data use outright or with safeguards. This compares to just 59% and 56% of C2s and Ds who were accepting of data use outright or with safeguards.

CONCLUSION

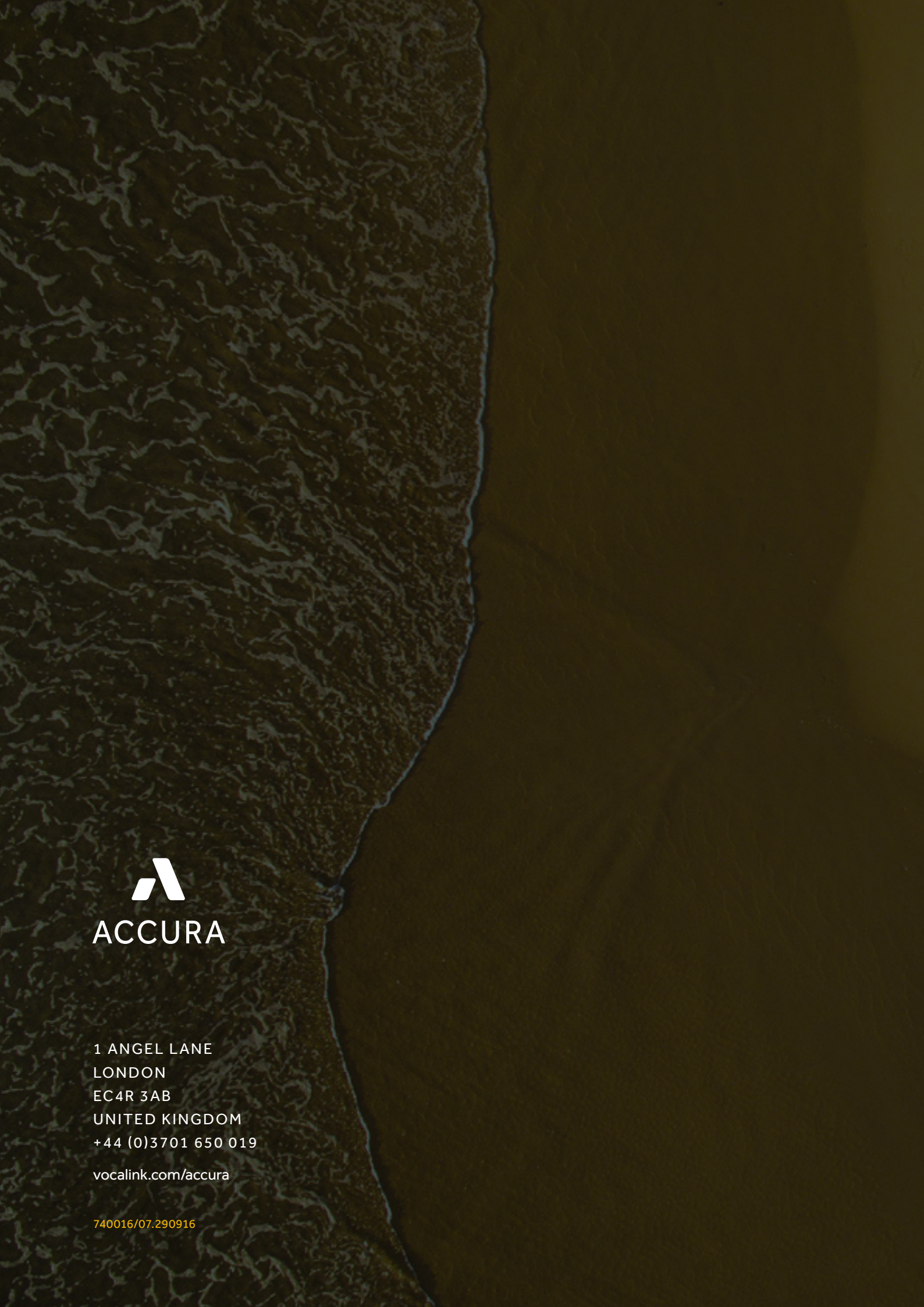
Transactional data already plays a vital role in helping to combat fraud and - provided certain safeguards are in place – the majority of the people we interviewed accepted the principle of using this kind of data in this way.

Reassuringly for both the public and the industry, in many instances these safeguards already exist; it is therefore a question of making it clear to people that they are robust, effective and overseen by organisations they feel they can trust.

Accura's insights, based on timely and fact-based payments data, offer the prospect of an enhanced understanding of the financial behaviours of people and businesses and consequently more effective tools to combat fraud. However, people need clarity and reassurance around who is accessing transactional data and why.

> "Someone overseeing it just to make sure that everything is being handled correctly and obviously in a non-fraudulent way. That would kind of give me a bit of a peace of mind."

Glasgow, 31-60, male



ACCURA

1 ANGEL LANE
LONDON
EC4R 3AB
UNITED KINGDOM
+44 (0)3701 650 019

vocalink.com/accura

740016/07.290916