The rise of B2B fraud

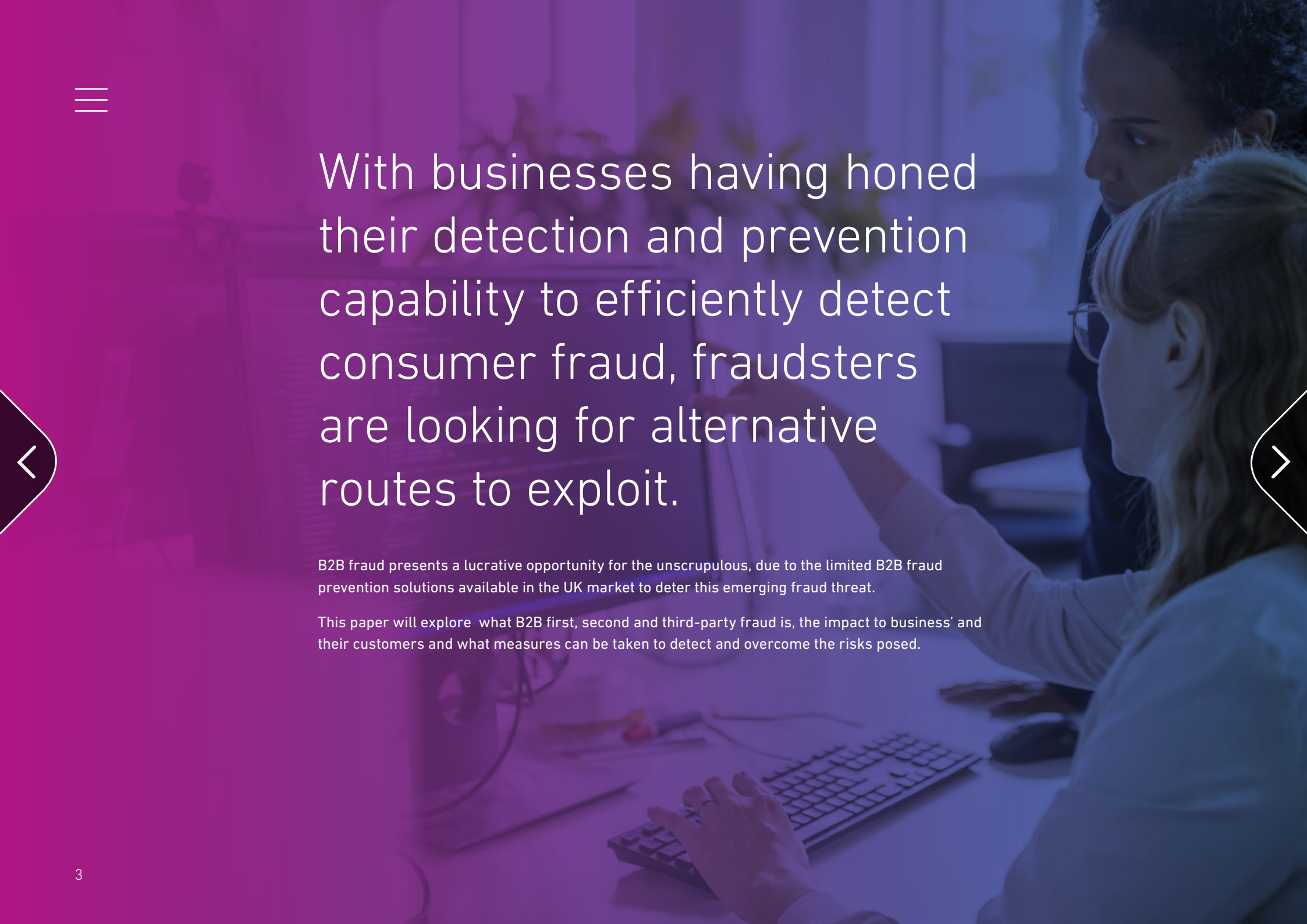
EXPERIAN INSIGHTS

Using the power of data to help you

ADAPT, SURVIVE AND THRIVE

experian™

Contents



With businesses having honed their detection and prevention capability to efficiently detect consumer fraud, fraudsters are looking for alternative routes to exploit.

B2B fraud presents a lucrative opportunity for the unscrupulous, due to the limited B2B fraud prevention solutions available in the UK market to deter this emerging fraud threat.

This paper will explore what B2B first, second and third-party fraud is, the impact to business' and their customers and what measures can be taken to detect and overcome the risks posed.

What is B2B first, second and third party fraud?

1. **FIRST** PARTY FRAUD

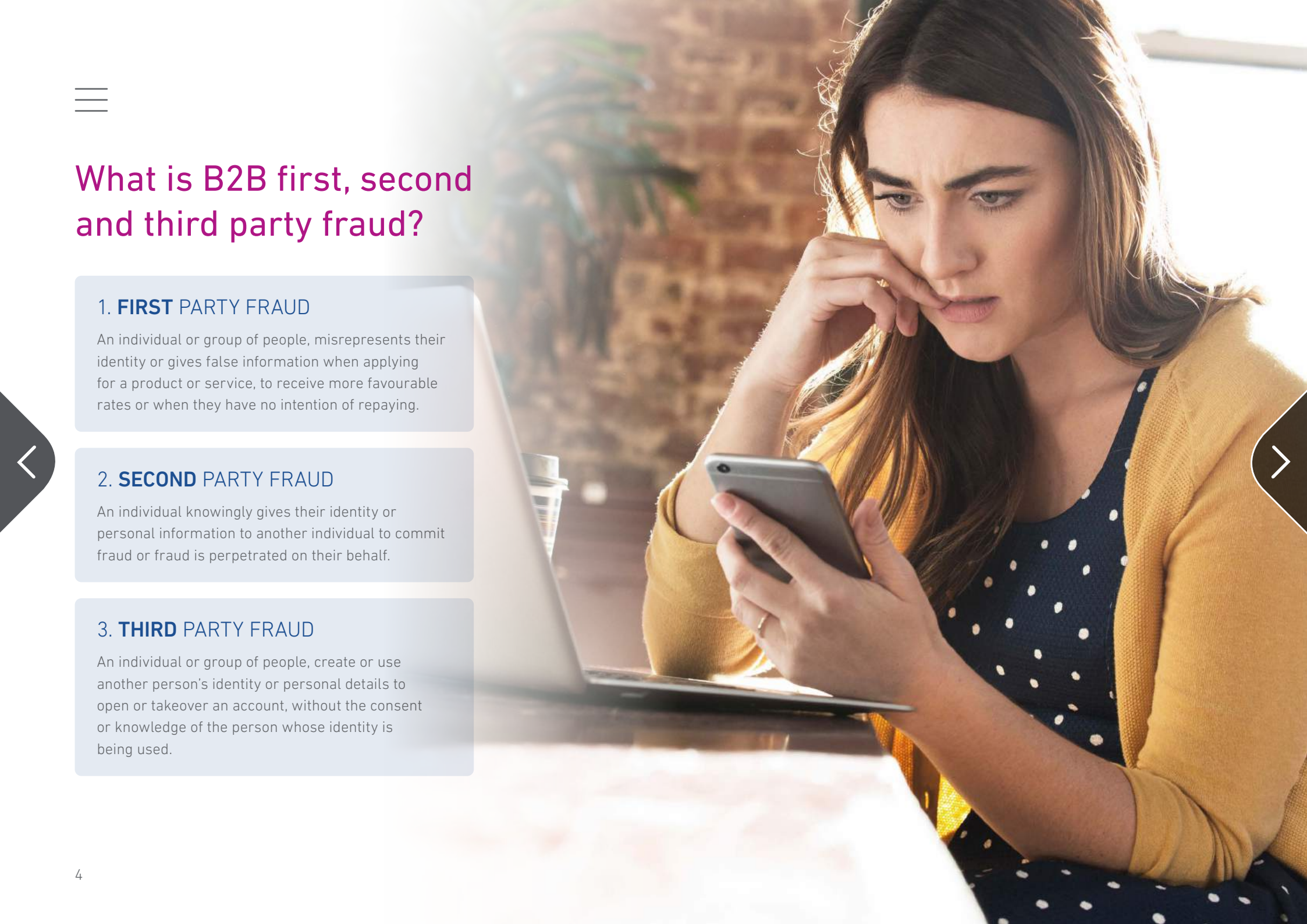
An individual or group of people, misrepresents their identity or gives false information when applying for a product or service, to receive more favourable rates or when they have no intention of repaying.

2. **SECOND** PARTY FRAUD

An individual knowingly gives their identity or personal information to another individual to commit fraud or fraud is perpetrated on their behalf.

3. **THIRD** PARTY FRAUD

An individual or group of people, create or use another person's identity or personal details to open or takeover an account, without the consent or knowledge of the person whose identity is being used.



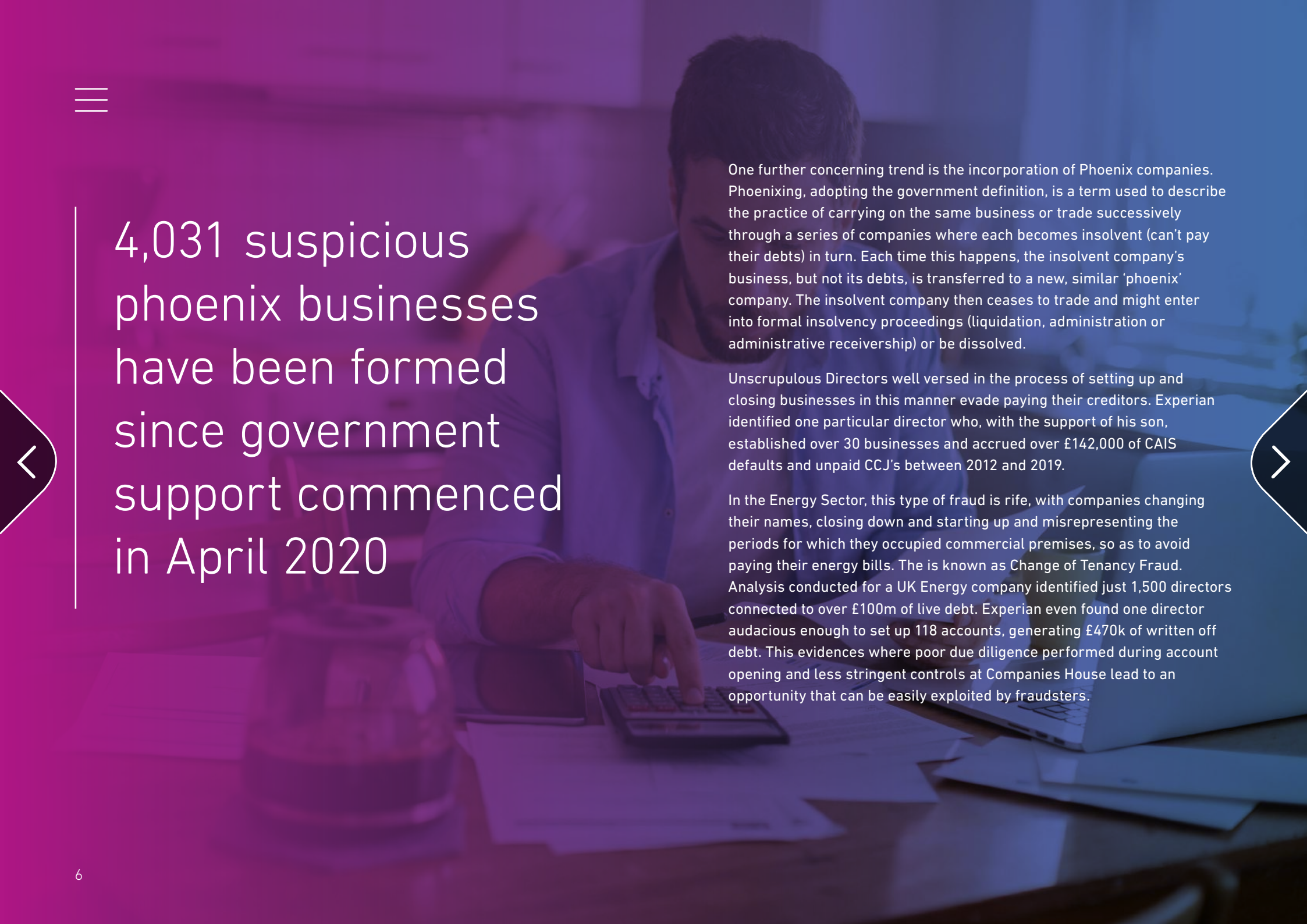
First party commercial fraud

First party Commercial fraud is where a business or its owner misrepresent their identity or give false information. This is usually done when applying for a product or service to receive more favourable rates, a better product or if they have no intention of meeting their commitments. Another example could be if a business makes a false claim against an insurer to obtain a payment they are not eligible for or misrepresents their trading activity to obtain a reduced premium.

Experian analysis shows that more people are committing fraud across the board. In the consumer world, people are being dishonest to get a mortgage they might not otherwise be eligible for, by not being truthful about their employment or financial circumstances. Sadly, the same is true with businesses. Company turnover values or income and expenditure data is amended to portray a more favourable picture of the business performance. Trading statuses or formation dates can be manipulated. The motivation for such dishonesty is clear; the want to gain access to a product or service the applicant is not eligible for or obtaining a line of credit greater than what the applicant would otherwise get than if their true credentials were presented.

Another interesting trend is that during major events there tends to be a short-term increase in first party fraud cases detected. For example, during the current pandemic, analysis conducted for a leading UK Bank identified that 0.7% of Bounce Back Loans had been granted by them and by another major bank, a breach of the eligibility rules whereby only one government backed loan is permitted per company. Additionally, Bounce Back Loan applications should not exceed a request for a credit limit greater than 25% of a company turnover, with a maximum loan amount permitted of £50,000. Despite this, Experian identified instances where small businesses falsely claimed a turnover of exactly £200,000 to obtain that maximum loan value available.

> 0.7% of Bounce Back loans a UK bank awarded had also been given by another bank, a breach of the one loan only rule



4,031 suspicious phoenix businesses have been formed since government support commenced in April 2020

One further concerning trend is the incorporation of Phoenix companies. Phoenixing, adopting the government definition, is a term used to describe the practice of carrying on the same business or trade successively through a series of companies where each becomes insolvent (can't pay their debts) in turn. Each time this happens, the insolvent company's business, but not its debts, is transferred to a new, similar 'phoenix' company. The insolvent company then ceases to trade and might enter into formal insolvency proceedings (liquidation, administration or administrative receivership) or be dissolved.

Unscrupulous Directors well versed in the process of setting up and closing businesses in this manner evade paying their creditors. Experian identified one particular director who, with the support of his son, established over 30 businesses and accrued over £142,000 of CAIS defaults and unpaid CCJ's between 2012 and 2019.

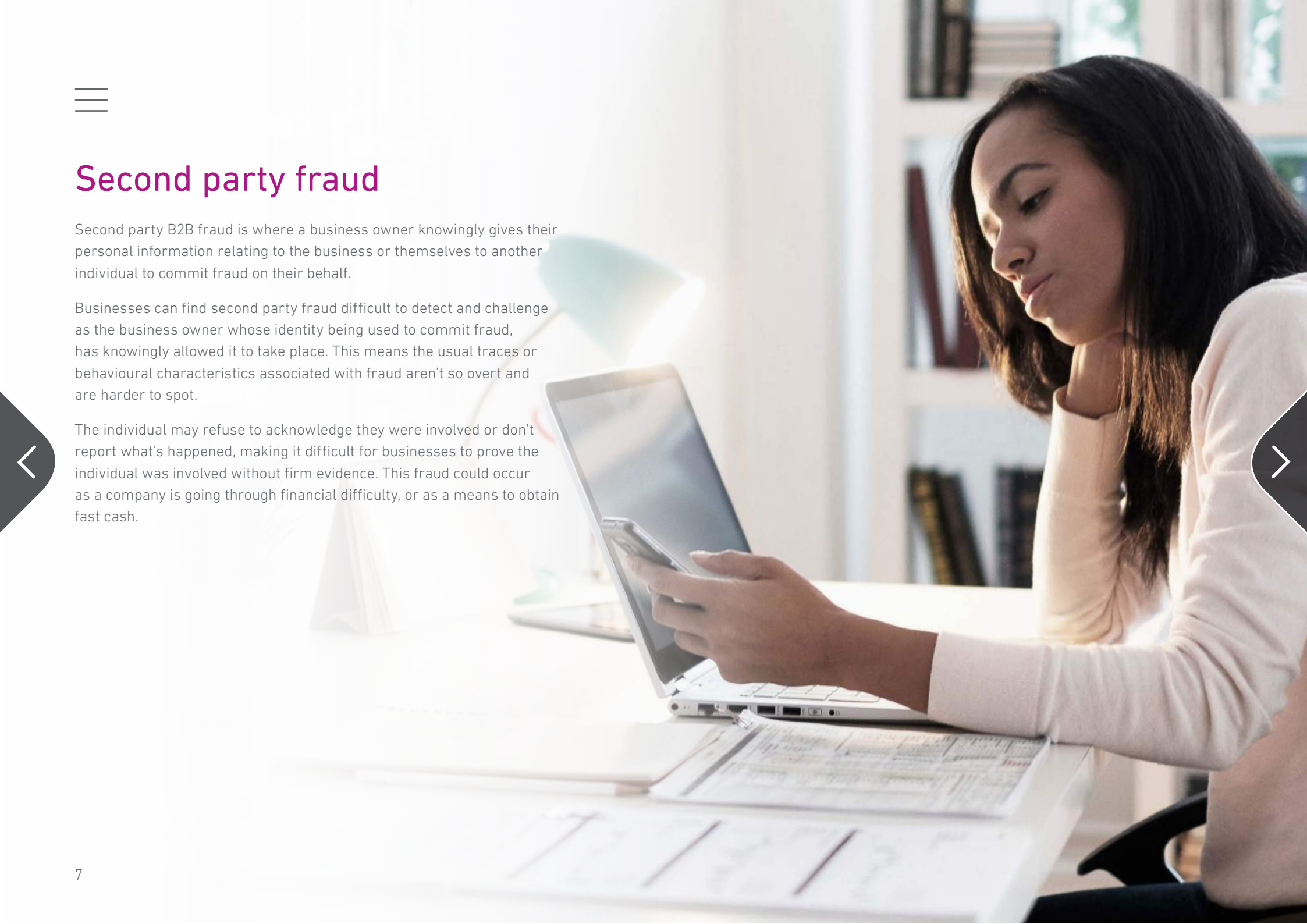
In the Energy Sector, this type of fraud is rife, with companies changing their names, closing down and starting up and misrepresenting the periods for which they occupied commercial premises, so as to avoid paying their energy bills. The is known as Change of Tenancy Fraud. Analysis conducted for a UK Energy company identified just 1,500 directors connected to over £100m of live debt. Experian even found one director audacious enough to set up 118 accounts, generating £470k of written off debt. This evidences where poor due diligence performed during account opening and less stringent controls at Companies House lead to an opportunity that can be easily exploited by fraudsters.

Second party fraud

Second party B2B fraud is where a business owner knowingly gives their personal information relating to the business or themselves to another individual to commit fraud on their behalf.

Businesses can find second party fraud difficult to detect and challenge as the business owner whose identity being used to commit fraud, has knowingly allowed it to take place. This means the usual traces or behavioural characteristics associated with fraud aren't so overt and are harder to spot.

The individual may refuse to acknowledge they were involved or don't report what's happened, making it difficult for businesses to prove the individual was involved without firm evidence. This fraud could occur as a company is going through financial difficulty, or as a means to obtain fast cash.



Third party fraud

There are two types of third party business fraud. The first is where an individual, or group of people, use another person's identity or personal details to open up a new business, using the stolen identity to present themselves as a director. This same approach can be taken to steal the identity of an existing company director. Conducting identity and verification checks on the business owners is critical to identifying that the director does exist and that they are who they say they are.

The second form of third party business fraud is known as 'manufactured identities' where an individual adapts the identity of an existing business. Fraudulent parties seek out older established businesses with a strong credit score and a weak data footprint to steal and enhance their credentials, presenting themselves as if representing a reputable business.

This activity not only causes financial disruption to the small businesses falling victim to the fraud, but also results in untold mental stress for its owners.

The preferred profile of a business to be used by the impersonators is clear; they like small limited companies, established for many years with strong financials but a weak online presence. This affords them the opportunity to carefully build the online profile of an already credit worthy business, introducing critical fraudulent details such as address, employee and contact details.

These previously invisible companies will be set up on directories (Yell and 118), with new web domain details and a trading address that is not the registered office. Mailbox companies and Serviced Offices are a natural choice to quickly convey a professional image, although residential addresses are also a common choice.

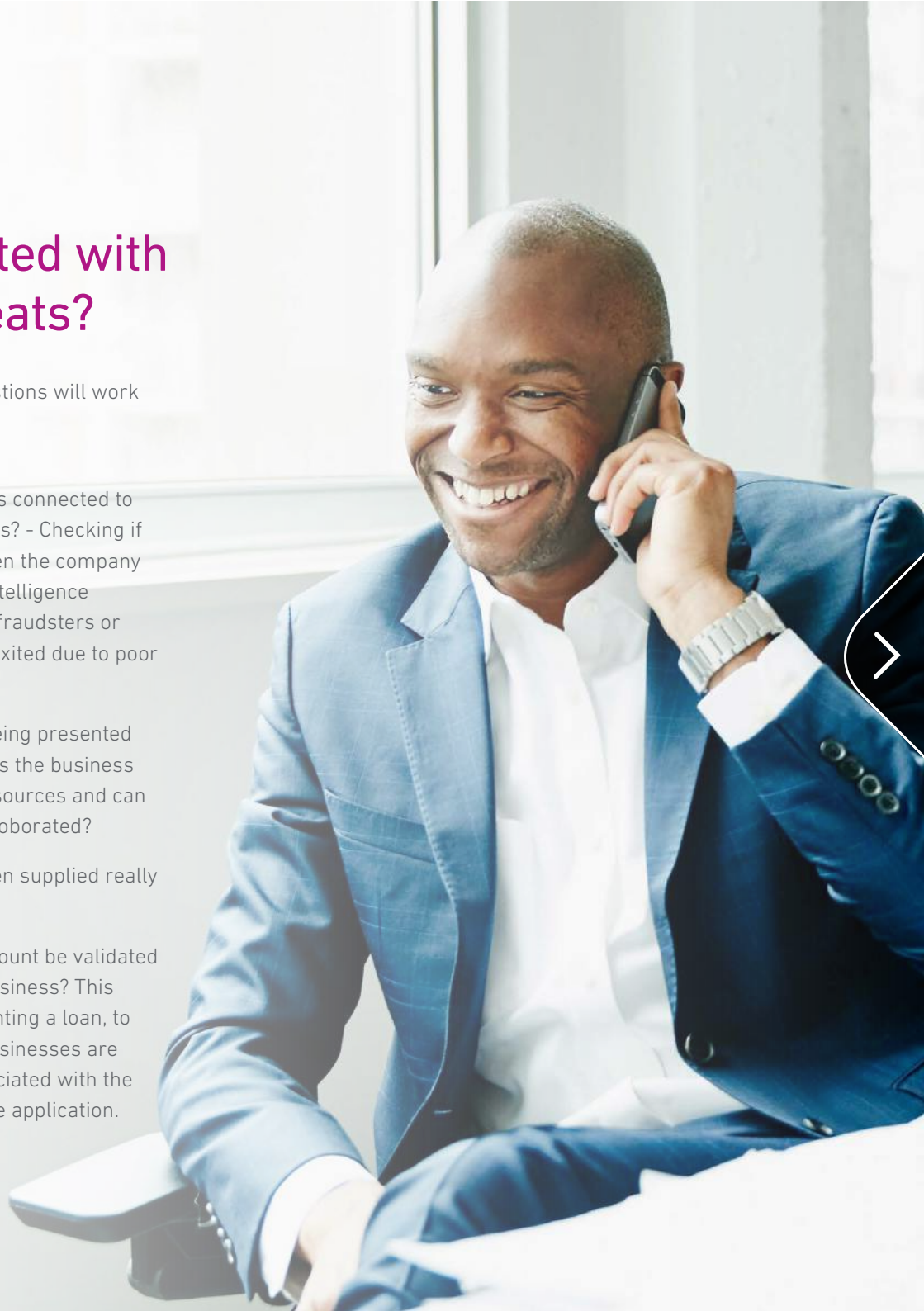
Mobile and Landlines are activated and become out of service in quick succession and new Hotmail and Gmail accounts are common practice.

How can you mitigate the risk associated with first, second and third party fraud threats?

The first step is knowing how to detect your level of exposure. Asking the following questions will work towards understanding the existing position and work towards earlier detection:

1. Can I validate the existence of the business, verify it is trading and confirm that the contacts presented are associated with that business?
2. Am I able to confirm the identity of the key people owning or controlling the business? – understanding the directors and who the ultimate beneficial owner (UBO) is
3. Am I able to authenticate the Business Owners? – do they exist and are they who they say they are?
4. Is the Business or its owners connected to known frauds? - Ensuring a business and its directors are not connected to known fraudulent databases- e.g. National Hunter or CIFAS
5. Are the business or owners connected to internal 'suspect' databases? - Checking if a connection exists between the company and any historic internal intelligence gathered, such as historic fraudsters or customer who have been exited due to poor credit behavior
6. Are the business details being presented honest and accurate – Does the business turnover align to external sources and can the trading activity be corroborated?
7. Is the address that has been supplied really linked to the company?
8. Can the business bank account be validated and associated with the business? This is important if you are granting a loan, to ensure the account that businesses are paying funds into are associated with the business that is making the application.

Let's now review each question and see where Experian can help.



Q1: Validating that the business exists, is trading and that the contacts presented are associated with that business

For years Experian has been leading the market in individual electronic identity and verification through our Identity Authenticate product offering. Many of the building blocks present in this solution have now been extended to help validate that a business exists and is actively trading. Using a combination of Companies House data, Open data and Bureau data (including CAIS and CCDS), we can produce a score out of 90 which offers confidence around the validity of an organisation.

We are also able to confirm where the applicants match to our Key Party data, denoting where they are a Director, Ultimate Beneficial Owner or Person of Significant Control.

Q2: Understanding who owns and controls a business

Determining the Ultimate Beneficial Owner (UBO), the individual that owns and controls a business, can be extraordinarily complex and time consuming.

Experian capture data from each document filed by companies at Companies House, capturing Shareholders, Shareholding, Share Value, Share Types, Currency, etc.

Capturing this data over time, provides a dynamic picture of the ownership structure that updates in line with new documents being filed.

Completing this manually for companies with multiple tiers in the corporate structure can take hours.

The below table illustrates the composition of the UK business universe broken down by corporate complexity, using shareholders and the number of tiers in a business. Whilst determining the Ultimate Beneficial Owner for the segment in green (low number of tiers and low number of shareholder) can be calculated in a few minutes, the segment highlighted in pink can take in excess of half a day. Using the Experian UBO algorithm all complexities can be handled providing a more accurate instant decision.

> For complex corporate frauds, understanding ownership and control is key for determining the extent of your exposure.

	Shareholders									
Tiers	1	2	3	4	5	6-9	10-25	26-50	50+	Total
1	2,170,888	1,082,129	179,082	112,079	40,183	47,287	27,225	6,330	3,061	3,668,264
2	16	74,195	56,162	29,477	24,061	34,859	16,303	4,213	3,175	242,461
3	-	3	21,133	9,581	6,998	16,341	10,788	2,684	1,978	69,506
4	-	-	-	10,662	3,072	6,695	6,851	2,001	1,631	30,912
5	-	-	-	-	6,007	4,590	4,473	1,204	1,704	17,978
6-9	-	-	-	-	-	10,243	7,336	2,820	4,642	25,041
10-25	-	-	-	-	-	-	2,341	1,249	3,928	7,518
26-29	-	-	-	-	-	-	-	76	10	86
Total	2,170,904	1,156,327	256,377	161,799	80,321	120,015	75,317	20,577	20,129	4,061,766

Q3: Authenticating that the Business Owners exist and are who they say they are

Once Experian has established all Key Parties (Directors, Ultimate Beneficial Owners and Persons of Significant Control), Experian can leverage restricted Usual Residential Address (URA) data to enable frictionless authentication. The URA is key for delivering a seamless customer experience. Without this, Ultimate Beneficial Owners who are not captured in application forms will need to be contacted separately to obtain residential address details to enable electronic identity verification. An Authentication Score is calculated using the results of consumer bureau matches and public data, including recency of data sources matched to and any high-risk flags.

Our identity questioning service, Identity IQ, then offers a solution to support customers in further confirming their identity using information that only they would know. This can remove the need for business owners to provide documentation and confirm with certainty that they are indeed the authenticated business owner.

Q4: Business or Business owners' connections to known Fraud Databases and Datasets

Once the Business and its owners have been authenticated, we can start to assess where connections exist to fraud data sets.

Firstly, we check the business against the following four business fraud flags:

- Suspicious Phoenix companies – flagging questionable directors and companies identified as habitually opening and closing businesses to evade paying creditors
- Zombie Director's – denoting directors appointed after their date of death
- Stolen and duplicated accounts – where a company passes another companies set of accounts off as their own
- Inaccurate reporting – identifying businesses where financials presented to Companies House may be misleading. For example, where the companies liability position is lesser than that calculated by Experian.

Company Details, including any bank accounts or contact details collected at point of application can be additionally checked against:

- Geo-Detect Index
- National Fraud Intelligence Bureau
- CIFAS (if a member)
- National or Insurance Hunter (if a member)

Once the business fraud risk has been established, we can assess the risk associated with the Business Owners. Directors and UBOs with approximate Date of Birth and Service Addresses, combined with restricted Usual Residential Address (URA) data and full Date of Birth, can be leveraged to check against the following traditionally used data sources:

- **Suspicious Activity Score File**
- **Geo-Detect Index**
- **Mosaic Risk Index**
- **Mortality (GRO, CAIS, Bona Vacantia)**
- **Victims of Fraud**
- **Prison List**
- **Previous Credit Application Data**
- **Disqualified Directors**
- **Never Paid Defaults (for CAIS Members Only)**
- **Gone Aways (for CAIS Members Only)**
- **CIFAS (if a member)**
- **National or Insurance Hunter (if a member)**

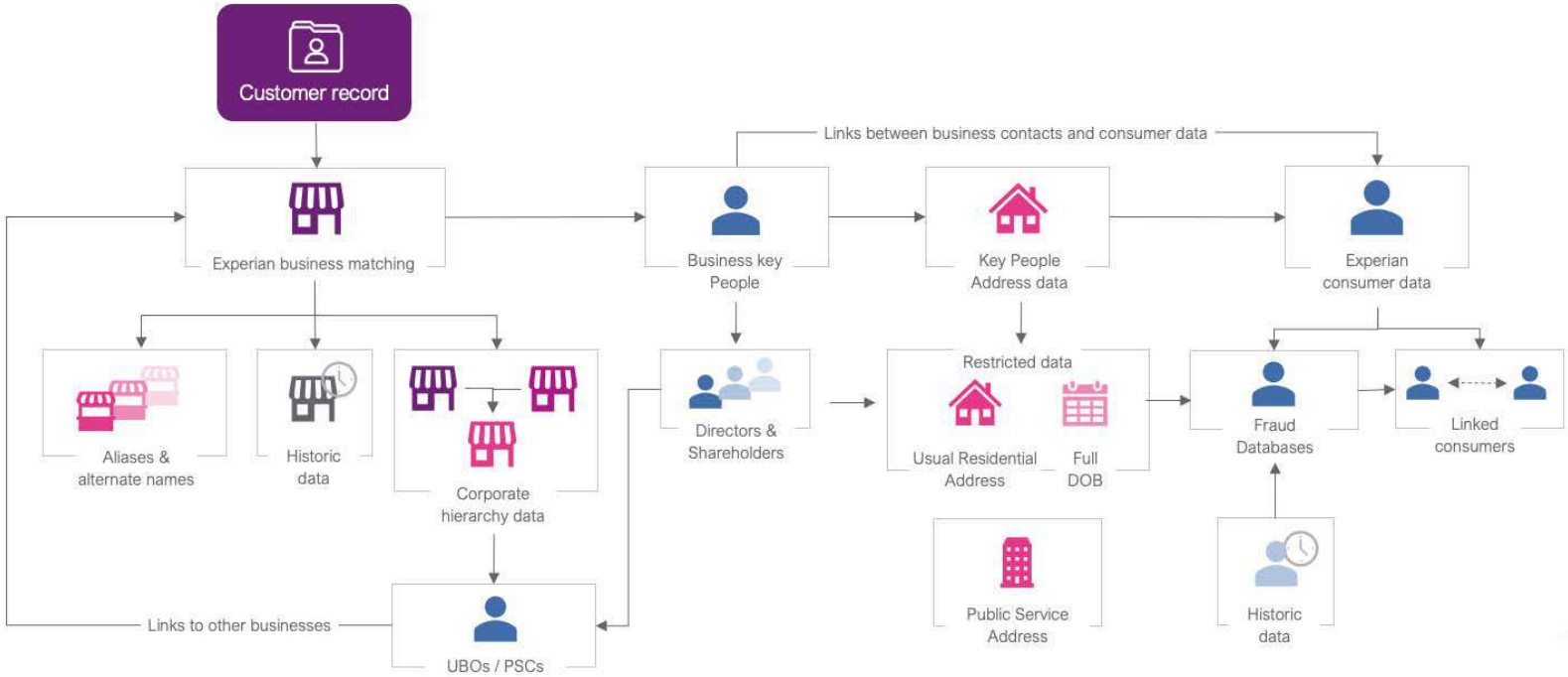
Q5: Leveraging your own internal data to identify suspicion

Experian recognise that many businesses will have accumulated vast amounts of intelligence on historic attempted or successful frauds. Being able to connect this invaluable wealth of information to existing customers and new applicants is essential for developing a solution that encompasses all internal and external fraud insights.

Businesses however are much more complex to navigate when investigating fraud than consumers.

Businesses can be hierarchical. Companies have parent companies, ultimate parent companies, subsidiaries and sites. If you have a bad experience with one or many parts of the group, how can you identify where new and existing accounts are potentially linked. Furthermore, Directors can own multiple companies not part of the same group. If you have a bad experience with the Director 'John Smith', how can you identify whether Mr Smith is a Director of a company applying for new services or is hidden in your portfolio under a different company.

The below diagram illustrates Experian's unique ability to link companies together connecting companies to their owners and these owners to consumer fraud datasets held in our bureau.



Q6: Validating the accuracy and integrity of the data being presented

When onboarding a new customer, honest and accurate contribution of information from the applicant is key to determining risk. Experian can support this process by highlighting inconsistencies between the data provided on the application and what's held on the bureau. Examples of this include:

- Overstating turnover - By comparing application values, management accounts, Companies House filings and Current Account Turnover data that is being shared by the banks, Experian can flag overstated income and issues within accounts
- Claiming to be VAT registered when not - Experian has access to the VAT register and can flag if an organisation is VAT registered or not and if the VAT number is correct
- Misrepresenting the age of the business - Length of time in business is a powerful risk scoring attribute and a good measure of the solidity of the business, which can often be misrepresented. Using credit, payment and current account data, alongside directory data assets, Experian is able to see how long a business has been actively trading and flag inconsistencies with what has been stated
- Not revealing credit facilities. Using Commercial CAIS data, Experian can show a true picture of a business's current credit commitments and reveal hidden facilities
- Providing a misleading trading activity – This is common issue in the insurance sector where different trading activities will result in a different premium calculation. For example, a roofer may claim to be a builder, knowing that roofers tend to incur higher insurance premiums. This is also common in serious and organised crime where certain business types are more commonly used to launder money. Experian's ability to understand and corroborate trading activity risk is truly unrivalled, with over 20 data sources utilised to accurately discern the principal activities of an organisation.

Q7: Validating that the address provided is associated with the business

Google, and other internet search engines, continue to be the most common choice for verifying that a trading address is associated with a business. As mentioned above, this is well understood by fraudsters when manufacturing and adapting the identity of an existing and established business. To address this, Experian have dedicated large amounts of our focus and resources to source the following data sources to enable unparalleled trading address verification for registered and non-registered businesses.

Experian's unique access to restricted Companies House Usual Residential Address (URA) data and a proprietary Ultimate Beneficial Ownership algorithm, provides the capabilities that enable the required connection of businesses to business owners and business owners to consumer fraud databases.

Data Source	LTD	Non LTD
Companies House	✓	
PAF	✓	✓
Market Location	✓	✓
Thomson	✓	✓
Local Data Company	✓	✓
Local Data Company - Closed Premises	✓	✓
Local Data Company - Vacant Premises	✓	✓
Jersey Financial Services Commission	✓	
Email movers	✓	✓
Experian	✓	✓
Corpfin	✓	✓
Open Government Licence	✓	✓
Companies House API	✓	
Charity Commission for England and Wales	✓	✓
Care Quality Commission	✓	✓
Edubase (Department for Education) Schools Register	✓	✓
Food Standards Agency	✓	✓
Gambling Commission	✓	✓
Licenced Premises	✓	✓
Ministry of Transport (MOT) Test Stations	✓	✓
Charities Commission for Northern Ireland	✓	✓
Organisation Data Service (ODS) of the Health & Social Care Information Centre	✓	✓
HM Revenue & Customs Trade Statistics	✓	✓
Scottish Charity Regulator	✓	✓
Driver & Vehicle Standards Agency	✓	✓
FCA Financial Services Register	✓	✓
VAT Register	✓	✓

Q8: Confirming the Bank Account Details are associated with the Business

When making payments to another business you need to confirm that the account you intend to make the payment into belongs to your customer. By making the link between the businesses you deal with and their bank account you will ensure that you only make payments to the correct beneficiaries. Experian's Bank Wizard Absolute service now includes CCDS business current account data to further increase match rates.

Bringing it all together

To tackle all of the B2B fraud typologies outlined in this paper it is clear that only a multifaceted, coordinated and comprehensive fraud prevention strategy can truly protect your organisation from potential B2B fraud losses resulting from these emerging trends. However, the age-old challenge of protection versus reducing friction within a customer journey must be considered in any approach taken. The use of external services and datasets can help to streamline the checks and validations to enhance the customer experience.

Businesses must employ a combination of Business, Consumer and Identity and Fraud capabilities to administer robust KYB and KYC checks. These fall into the following two broad categories.

- Business and Business Owner Authentication – determining that a business is active, trading, addresses are verified and that the owners are who they say they are
- Business and Business Owner Fraud Checks – confirming that the business and its owners are not connected to internal and external fraud databases and datasets.

The war against the fraudsters ever evolving exploitation of weaknesses in existing processes is becoming progressively greater. Therefore, it is imperative that in order to win the battle companies look to utilise the available tools in market.

If you'd like to talk to us about how we can help you to combat commercial fraud we're here to help.

Just call us on **0844 481 5873**
or email **businessuk@ experian.co.uk** and find out how we can help you take a new approach to fighting fraudsters.

About the author

Grant MacDonald Director of FinCrime Market Engagement

For over 20 years, Grant MacDonald has been pioneering the creation and delivery of market insights across the identity, fraud, financial crime and credit landscape. Having held roles as Head of Enterprise Markets, Sales Director Identity & Fraud and now Director of Financial Crime Market Engagements, Grant is now responsible for coordinating Experian's marketing, product, delivery and consultancy efforts to deliver market leading Financial Crime insights and services to UK businesses.

Contact us:
businessuk@experian.com

Stay up to date with our latest thinking,
by bookmarking our thought leadership portal:
www.experian.co.uk/latest-thinking

The insight contained within this report is prepared using research performed on both Experian data and external data sources, in addition to market research. All sources, unless referenced, are from Experian insight.

The information contained within this report is designed to help businesses manage the complexity brought by a national crisis - and is a summary of key areas and capabilities. To understand more about the breadth of market-leading capability Experian has, or to access further detail on the impact of Covid-19 on consumers, business and lending portfolios - please contact us.

Registered office address:
The Sir John Peace Building, Experian Way,
NG2 Business Park, Nottingham, NG80 1ZZ

T: 0844 481 5873
www.experian.co.uk

C-01067