FRAUD

HOW TO MANAGE THIS INCREASINGLY COMPLEX THREAT

HUNTSWOOD

> THIS REPORT HIGHLIGHTS THE NEED FOR GOOD RISK MANAGEMENT AND EFFECTIVE PROCEDURES TO DEAL WITH FRAUD. IT ALSO COMES AS NO SURPRISE THAT SOME OF THE MOST PREVALENT FORMS OF FRAUD ARE LINKED TO TECHNOLOGY APPLICATIONS AND ACCESS. AS FIRMS PROGRESS WITH THEIR DIGITAL OFFERING AND COMMUNICATIONS THIS COULD BECOME EVEN MORE PREVALENT

PERSONAL INVESTMENT MANAGEMENT &
FINANCIAL ADVICE ASSOCIATION
(PIMFA)

CONTENTS

FOREWORD

If a firm is vulnerable to fraud, it should expect to become a victim of fraud. Fraud is an ever present and destructive threat that confronts firms, individuals and society at large. It can be committed by trusted persons, unknown individuals, experts, opportunists and by the truly skilled and motivated. It is carried out for a broad range of reasons, from financial gain to a desire to cause harm, and may or may not involve the use of technology. Combating such a broad range of variables therefore demands specialised skills and focus. If these are applied effectively, firms will experience significant operational efficiencies (when compared against less effective fraud control models), customers will receive improved service and fraudsters will less likely benefit from their dishonest conduct.

In this report, we provide readers with comparative insights into fraud risks and controls as well as suggested enhancements, using primary research collated from a diverse range of financial services and utilities firms, as well as our first-hand experience of working with clients to help them manage fraud risk.

SOME KEY INSIGHTS HIGHLIGHTED BY OUR RESPONDENTS INCLUDE:

- Company boards should set out a robust and proportionate anti-fraud governance framework, where accountability and oversight are clear, and consolidated information is produced to provide a comprehensive view of the firm's fraud risk and control environment
- Fraud risk assessments should be continuously refreshed, benchmarked and individually consider both:
  - The risk of specific fraud typologies occurring (e.g. application fraud)
  - The risk that fraud disrupts key business process (e.g. customer servicing)
- Firms benefit from implementing a holistic approach to fraud risk management. In practice, this means having clear sight of fraud risks and controls across end-to-end business processes (e.g. customer journey) rather than maintaining segregated fraud controls within several business areas (e.g. application, onboarding, underwriting, claims, customer servicing and payments)
- Technology advances provide firms with an opportunity to improve fraud control, operational efficiencies and quality

We are grateful to everyone who has contributed to this research – and hope the insight in this report supports you in your continued endeavours to effectively manage fraud.

STEVE ELLIOT
MANAGING DIRECTOR
FINANCIAL CRIME, FRAUD,
INFORMATION SECURITY AND
PAYMENTS

STEVE ELLIOT
MANAGING DIRECTOR
FINANCIAL CRIME, FRAUD, INFORMATION
SECURITY AND PAYMENTS

> FRAUDSTERS ARE HIGHLY MOBILE AND WILL EXPLOIT WEAKNESSES IN FIRMS' CONTROLS.
>
> THIS REPORT PROVIDES KEY INSIGHTS WHICH WILL ENABLE INSURERS AND OTHERS TO REVIEW AND STRENGTHEN THEIR FRAUD DEFENCES. IT WILL ALSO HELP TO SATISFY THE REGULATOR THAT THE INDUSTRY TAKES APPROPRIATE CONTROL MEASURES TO MANAGE THE RISK PRESENTED BY FINANCIAL CRIME

ASSOCIATION OF BRITISH INSURERS
(ABI)

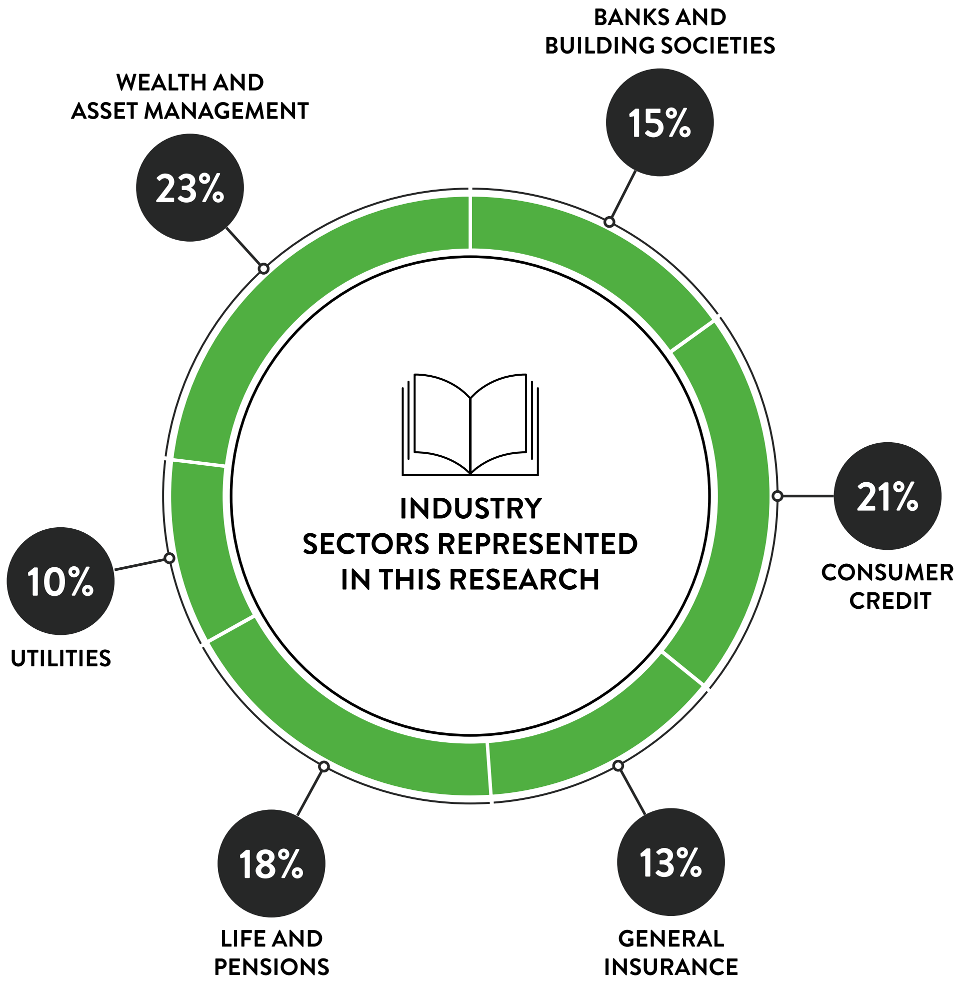
RESEARCH METHODOLOGY

THE INSIGHT WITHIN THIS REPORT IS BASED ON ORIGINAL RESEARCH UNDERTAKEN BY HUNTSWOOD

Our research involved interviews with 43 firms across financial services and utilities. Specifically, it incorporated:

QUALITATIVE AND QUANTITATIVE RESEARCH AND ANALYSIS

of in-depth interviews with senior operational, compliance / risk and financial crime management on their fraud risk management practices. We also engaged with board members and NEDs to understand their views on fraud risk management.



THE FRAUD LANDSCAPE

THE FRAUD THREAT

Fraud is acknowledged as a significant threat to firms' infrastructures, where the public opinion has shifted, with a growing expectation on firms to protect their customers from fraud. However, the problem of fraud is not a simple threat to address. The scale of fraud is accelerating at the same rate as technology growth and a recent survey from the Office of National Statistics showed that, of an estimated total of 10.8 million crimes in the UK, 5 million offences were categorised as fraud and computer misuse.

> FRAUD SHAMES OUR FINANCIAL SYSTEM. IT UNDERMINES THE CREDIBILITY OF THE ECONOMY, RUINS BUSINESSES AND CAUSES UNTOLD DISTRESS TO PEOPLE OF ALL WALKS OF LIFE. FOR TOO LONG, THERE HAS BEEN TOO LITTLE UNDERSTANDING OF THE PROBLEM AND TOO GREAT A RELUCTANCE TO TAKE STEPS TO TACKLE IT
>
> THERESA MAY

The growing importance of fraud is also highlighted by the numerous domestic and international initiatives which have been introduced:

LEGISLATION AND REGULATION

In 2007, the Fraud Act 2006 came into force which categorises the level of offending with dishonest behaviour to gain, cause or expose a loss into three main offences:

1. Making a false representation (untrue or misleading behaviour)
2. Failing to disclose information
3. Abusing a position of trust

Whilst there is currently no corporate liability offence for failing to prevent fraud (unlike bribery and facilitating tax evasion), there was a Call for Evidence in January 2017 for considering a new offence of corporate liability of economic crime. The proposed offence is designed to prevent financial crimes such as fraud, false accounting and money laundering when committed on behalf, or in the name of, companies. Ministers are currently reviewing the evidence, and we are expecting to hear an announcement in 2018.

The General Data Protection Regulation (GDPR) also comes into force in May 2018, which provides a requirement for firms to report data breaches within 72 hours or face the consequences of significant fines. Failure to notify of a breach, can result in fines of 10 million euros, or 2% of the firm's global turnover, as well as associated reputational damage.

FRAUD CONTROL ORGANISATIONS

A number of industry bodies and initiatives have also been established to assist in the fight against fraud, some of which include:

ENFORCEMENT AND REGULATION

- **FINANCIAL CONDUCT AUTHORITY (FCA) -** the FCA, a financial regulatory body in the UK, has a strategic objective to reduce the risk of fraud and financial crime to mitigate the impact on consumer protection. The FCA requires firms to submit an annual financial crime return (REP-CRIM) which captures a firm's top three most prevalent frauds and identifies whether they are increasing, decreasing or unchanged
- **PAYMENT SERVICES REGULATOR (PSR) -** the PSR is an economic regulator for the £81 trillion payment systems industry in the UK. At present, it is proposing a scheme to improve standards to victims of fraud by reimbursing customers who have been deceived to transfer money and a new 'contingent reimbursement model' is to be introduced by September 2018
- **LAW ENFORCEMENT AND THE SERIOUS FRAUD OFFICE (SFO) -** reported fraud investigations are divided across numerous law enforcement agencies such as local police forces, the National Crime Agency (NCA), the Department for Work and Pensions (DWP) or HM Revenue and Customs (HMRC). However, the specialist prosecutor for tackling the most serious fraud offences are investigated and prosecuted by the SFO

INDUSTRY BODIES

- **FRAUD ADVISORY PANEL (FAP) -** the FAP are an organisation governed by a board of trustee directors that aim to provide best practice on fraud prevention, detection, investigation and prosecution. Members are drawn from all sectors such as public, private and voluntary with a common goal to mitigate fraud
- **CREDIT INDUSTRY FRAUD AVOIDANCE SYSTEM (CIFAS) -**
  CIFAS is a not-for-profit fraud prevention membership organisation who manage the largest confirmed fraud database in the country. Members, who are from various sectors, share data to reduce and mitigate instances of fraud and financial crime
- **INSURANCE FRAUD BUREAU (IFB) -** The IFB is a not-for-profit organisation established to lead the insurance industry's collective fight against insurance fraud. It has two primary objectives, to help insurers identify fraud and avoid the financial consequences and to support police, regulators and other law enforcement agencies in finding fraudsters and bringing them to justice
- **FINANCIAL FRAUD ACTION (FFA) UK -** now part of the UK Finance trade association. In 2018, FFA UK will continue their work with the Joint Fraud Task Force and law enforcement agencies to tackle the issue of payment fraud

FRAUD CONTROL INITIATIVES

JOINT FRAUD TASKFORCE

The taskforce, a partnership between banks, law enforcement and the government, was set up in 2016 with three main objectives – firstly, to protect the public and businesses from financial fraud, secondly, to reduce the effects of fraud on victims and thirdly, to increase prosecution of fraudsters

THE BANKING PROTOCOL

This protocol enables staff at banks and building society branches to alert the police if they suspect a customer is vulnerable to a scam. It is a collaboration between the finance industry, police, and Trading Standards to mitigate the risk of fraud to customers

TAKE FIVE TO STOP FRAUD

Take Five is a national awareness campaign led by UK Finance and backed by Her Majesty's Government. The campaign is delivered through the UK payments industry, financial services firms, law enforcement agencies and telecommunication providers to offer an overarching message to stop and think about the risks of fraud

INSURANCE FRAUD TASKFORCE

Set up in 2015, the taskforce investigates the causes of fraudulent behaviour and recommends solutions to reduce the level of insurance fraud

THE HIDDEN COST OF FRAUD

Fraud is reported to Action Fraud, hosted by the City of London Police, or in some cases, reported to local police forces, with other confirmed frauds and intelligence fed into the CIFAS internal database. However, there is not a general regulatory requirement for all firms across all industries to report fraud and the total cost to businesses is, therefore rarely recorded. The hidden nature of fraud also provides a challenge for calculating its cost to the private and public sector. This is made more difficult as the assessment cannot identify the cost of any frauds that have gone undetected. From the data available, the Association of Certified Fraud Examiners (ACFE) estimated that firms typically lost 5% of their annual revenue to fraud in 2017 and the future is just as bleak, with the NCA stating that fraud losses in the UK are likely to increase.

FRAUD CASES

> "THE POTENTIAL REPUTATION IMPACT OF FRAUD IS HUGE. YOU ARE NOTHING WITHOUT YOUR REPUTATION. IF YOUR REPUTATION IS DAMAGED, THE RESULT OF THIS IS CUSTOMER LOSS, DISTRUST AND LOSS OF BUSINESS. THE BUSINESS REVOLVES AROUND THE CUSTOMER, SO THE MOST IMPORTANT THING IS TO PROTECT OUR CUSTOMERS"
>
> NED, RETAIL BANK

Several recent high-profile cases highlight the financial and reputational consequences of fraud:

2012

KWEKU ABODOLI - convicted for fraud following the 2011 UBS rogue trade scandal

2013

YAHOO - three billion accounts compromised in a cyber attack

2015

RBS AND NATWEST - cyber attack on online services

TOM HAYES - a former trader at UBS and Citigroup sentenced to 11 years imprisonment for manipulating the Libor rate

2016

TESCO - cyber attack which resulted in the loss of £2.5 million

BANK OF BANGLADESH - cyber payment fraud where bank hackers stole $81 million

2017

NHS - ransomware attack

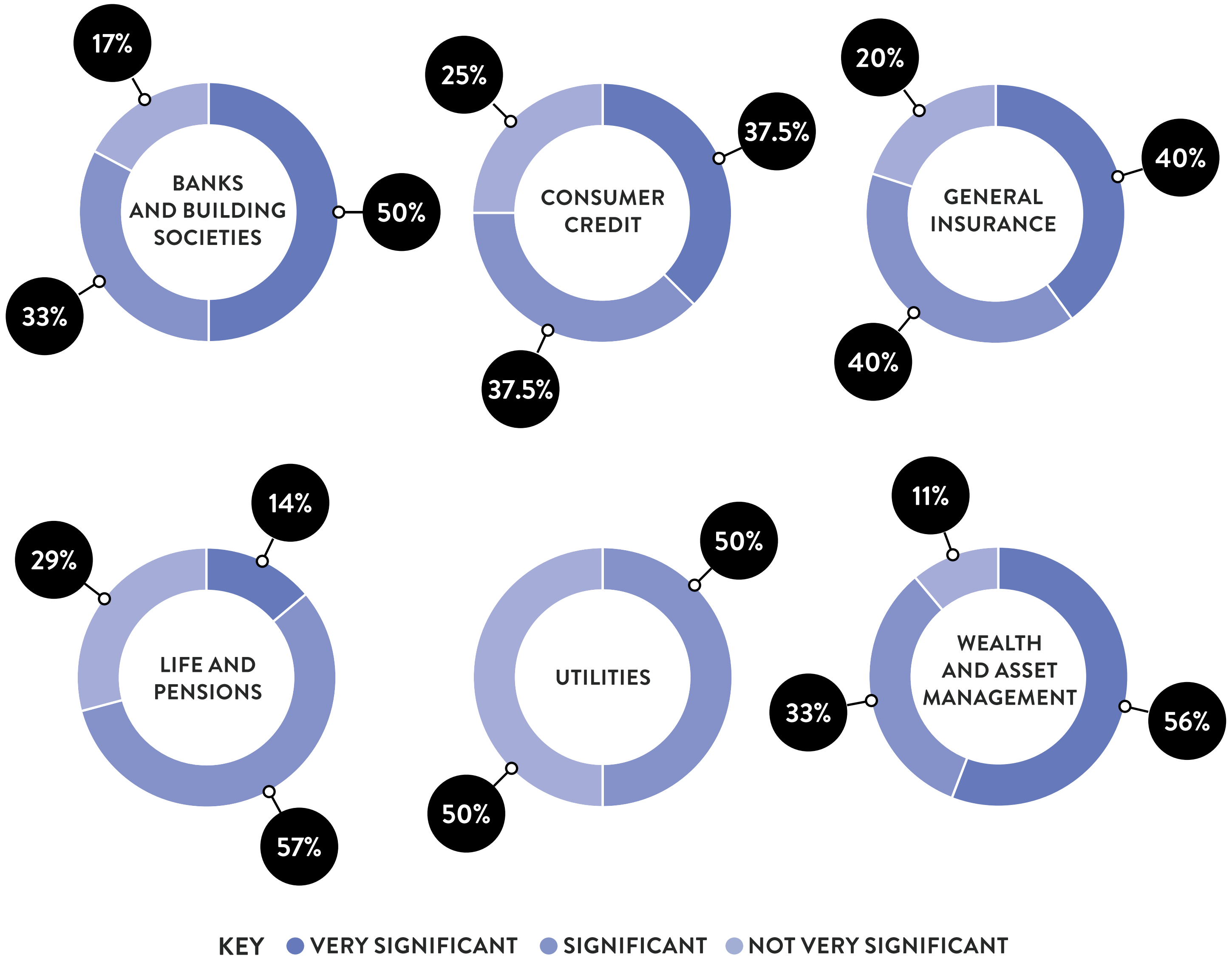
TALK TALK - fined £100,000 for failing to protect customers data

EQUIFAX - data breach affecting 145 million people

FRAUD ARRANGEMENTS

When asked to rate the relative importance of reputation in driving the firm's anti-fraud activity, the responses provided by firms varied significantly. Wealth and asset management firms weighted their responses toward reputation being very significant, which may be due to many of those firms having a close relationship with the individuals they serve, and the fact that clients place a higher than average weight on the reputation of the firm they engage with to manage their wealth. Alternatively, utilities weighted towards not very significant.

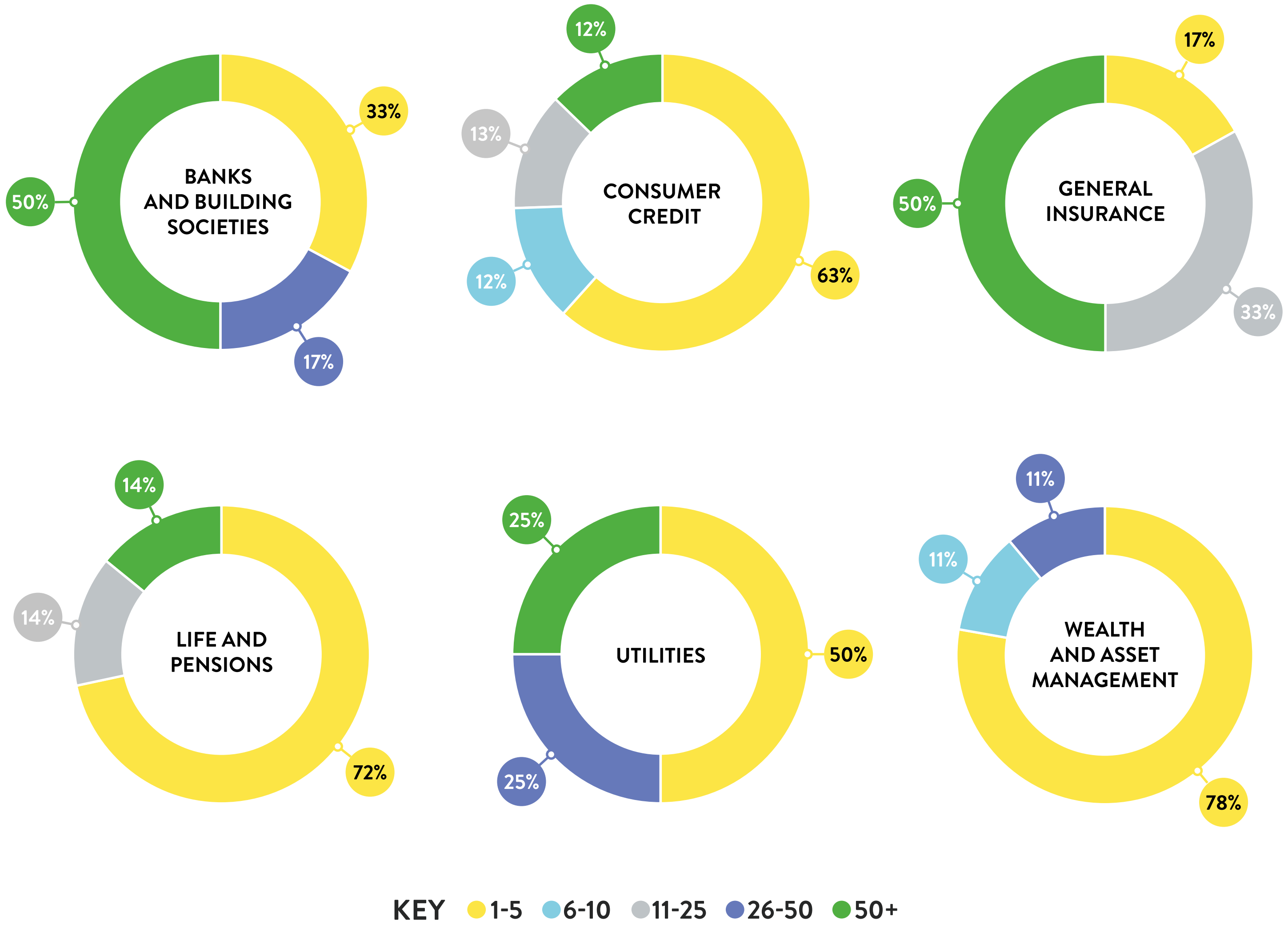
HOW SIGNIFICANT IS REPUTATION IN DRIVING YOUR ANTI-FRAUD ACTIVITY?



Our research also highlighted that a variety of approaches are taken when defining and measuring fraud loss and a range of metrics and management information (MI) are utilised. 52% of firms surveyed only consider direct financial loss as the cost of fraud whereas the remaining 48%, also consider the wider financial impact on operations, brand, consumer and resource - in fact, just over a half of respondents had between one to five resources dedicated to fraud control activity.

BRIONY RIPPINGTON-BOND
CONSULTANT
FINANCIAL CRIME AND FRAUD

HOW MANY OF YOUR EMPLOYEES ARE DEDICATED TO FRAUD CONTROL ACTIVITY?



WHAT DO YOU CONSIDER WHEN YOU ASSESS THE COST OF FRAUD?

FINANCIAL LOSS

- Net value
- Reimbursing the customer
- Compensating the customer
- Value of fraudulent applications
- Fines / enforcement action

IMPACT ON THE BRAND

- Reputational damage
- Market share

OPERATIONAL COST

- Impact on internal processes
- Controls
- New systems
- Investigation
- Litigation
- Asset recovery
- Cost of insurance
- Capital adequacy

IMPACT ON THE CUSTOMER

- Customer experience
- Customer complaints
- Customer awareness

COST OF RESOURCE

- The impact of reduced morale on productivity
- Training and awareness
- Referencing and vetting
- Increased headcount
- Time

33% OF OUR PARTICIPATING FIRMS ESTIMATED THAT THE COST OF FRAUD WAS GREATER THAN £500,000 IN THE PREVIOUS 12-MONTH PERIOD. WITH 41% OF ALL PARTICIPATING FIRMS STATING THEY EXPERIENCED OVER 250 FRAUD EVENTS IN THE SAME PERIOD

FRAUD RISKS

THE FRAUD RISKS FACED BY FIRMS ARE MANY AND VARIED - FIRMS WE SURVEYED IDENTIFIED 146 INDIVIDUAL FRAUD RISKS REQUIRING THEIR ATTENTION. HAVING REVIEWED THESE, WE HAVE CATEGORISED THE RESPONSES INTO SEVEN GENERIC FRAUD RISKS:

IDENTITY (ID) FRAUD

IMPERSONATING A GENUINE OR FAKE IDENTITY TO ACCESS A SERVICE OR PRODUCT

In 2017, CIFAS reported the highest recorded number of identity frauds (173,000 reports) which accounted for a staggering 53% of all fraud. ID fraud is a key challenge for firms, particularly in light of the recent cyber-attacks, where vast amounts of identity information was released onto the dark web for fraudsters to exploit.

INSIDE FRAUD

FRAUDULENT LOSS AND CORRUPTION BY EMPLOYEES AND OTHER AGENTS CONNECTED TO THE BUSINESS

Employees who hold a position of trust and act dishonestly can severely disrupt the organisation and lead to financial and reputational loss. Often, insiders are equipped with the requisite knowledge of the company and its processes to cover their tracks. According to the Annual Fraud Indicator report, £16.6 billion was lost through payroll expenditure and £134 billion for procurement expenditure.

"THE MOST COMMON PERPETRATORS OF FRAUD, CYBER, AND SECURITY INCIDENTS OVER THE PAST 12 MONTHS WERE CURRENT AND FORMER EMPLOYEES"

KROLL ANNUAL GLOBAL FRAUD AND RISK REPORT 2016 / 2017

FALSE CLAIMS FRAUD

KNOWINGLY USING DISHONEST INFORMATION TO MAKE CLAIMS

False claims fraud is where the identity is known, and the claimant exaggerates to gain a payment - an area that is well known with the insurance industry. The fraud could also include the provision of false information to a company to obtain a service or benefit.

CYBER - ENABLED FRAUD

USING COMPUTERS, COMPUTER NETWORKS OR OTHER FORMS OF INFORMATION AND COMMUNICATIONS TECHNOLOGY TO INCREASE THE SCALE OR REACH OF TRADITIONAL CRIMES

Cyber-dependant crime is where devices are both the tool for committing the crime and the target of the crime. However, in this report we are focusing on cyber-enabled fraud, which is an area that continues to overlap in most fraud typologies, with technology now being the main enabler. Our respondents highlighted the prevalence of phishing that can lead to losses for both customers and organisations. One in every 131 emails sent in 2016 contained malware – the highest rate in five years. Spear-phishing, a more targeted attack, led to a loss of £3 billion from businesses in the last three years.

ORGANISED SCAMS

TARGETING CUSTOMERS, PARTICULARLY THE VULNERABLE, USING ORGANISED CRIME SCAMS (E.G. BOILER ROOM / INVESTMENT SCAMS)

To help combat this type of fraud, the FCA has introduced the ScamSmart campaign – an initiative to raise awareness of investment scams - and is asking relevant firms to help educate the consumer by placing information on their website. Similarly, the 'Take Five' campaign also aims to raise awareness. Notwithstanding these initiatives, firms themselves can be targeted by organised scams such as CEO fraud.

PAYMENTS FRAUD

FRAUDULENTLY DIVERTING PAYMENTS OR ACCESSING PAYMENT SYSTEMS TO TRANSFER FUNDS

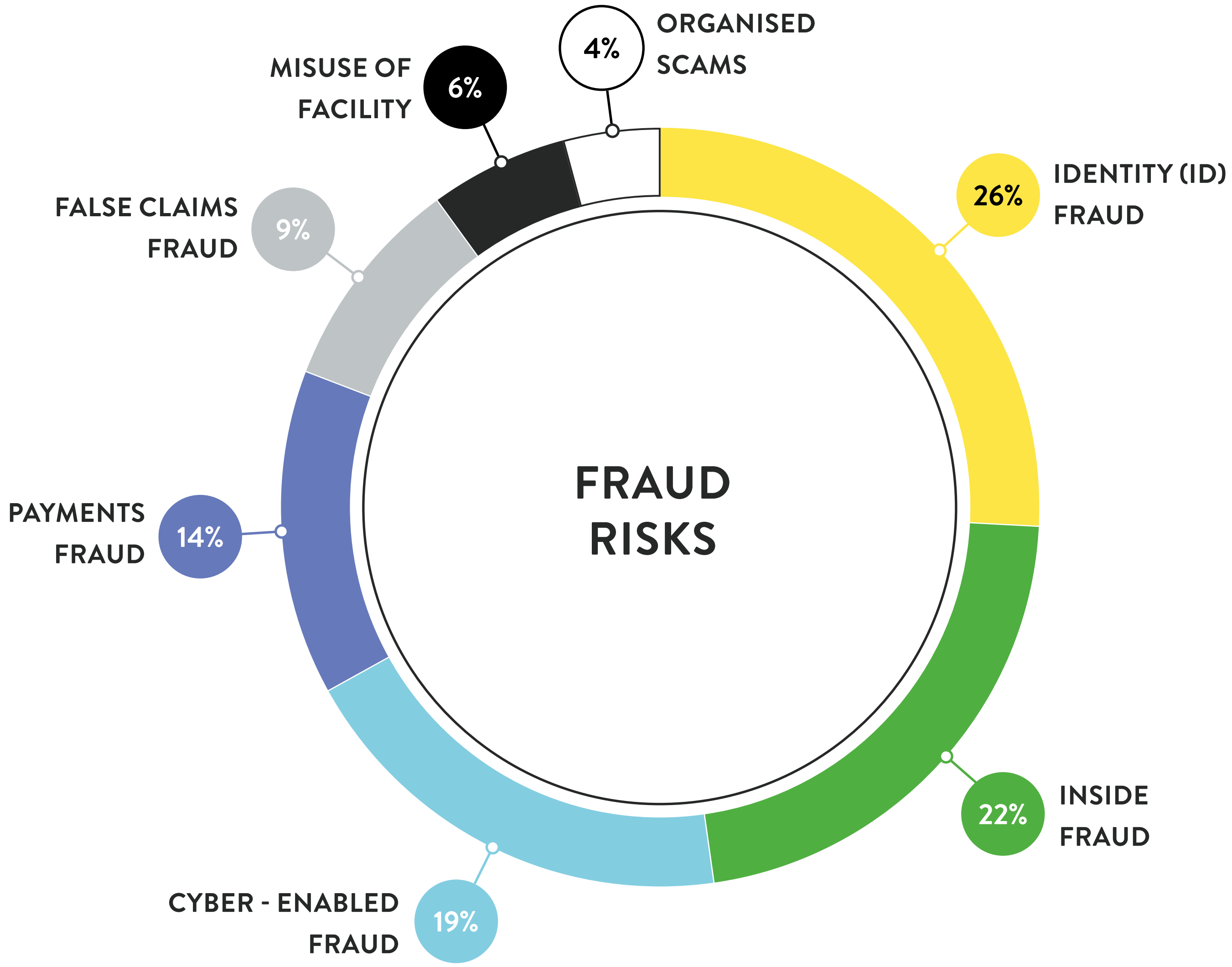
Payments fraud across remote banking and cheques totalled £768.8 million in 2016, an increase of 2% compared to 2015. This increase has been attributed to impersonation, deception and online attacks from recent data breaches, whereas the theft of card data, which has also been increasing year-on-year, has been attributed to the rise in remote ('card not present') fraud. Push payments i.e. authorised by the customer, are also a growing trend in scams.

MISUSE OF FACILITY

MISUSING A PRODUCT OR SERVICE FOR A FRAUDULENT PURPOSE, SUCH AS A BANK ACCOUNT OR POLICY

A common theme in this area is money mules and the 2017 CIFAS Fraudscape report underlined that money mule activity increased by 9% on the previous year, with young adults being targeted, while bank accounts impacted by the misuse of facility fraud rose by 7%.

OF THESE SEVEN RISKS, IDENTITY FRAUDS WERE THE MOST FREQUENTLY IDENTIFIED INDIVIDUAL RISK TYPES, FOLLOWED BY INSIDER FRAUDS AND CYBER-ENABLED FRAUDS.



WHEN ASSESSING THE HIGHEST PRIORITY RISKS FOR EACH SECTOR, BOTH IN TERMS OF INTERNAL RISK ASSESSMENTS AND REGULATORY ATTENTION IN THE COMING YEAR, THE COMBINED RESULTS OF THE RESPONSES REVEALED, THAT NO TWO INDUSTRY SECTORS SHARED THE SAME RISK PRIORITISATION.

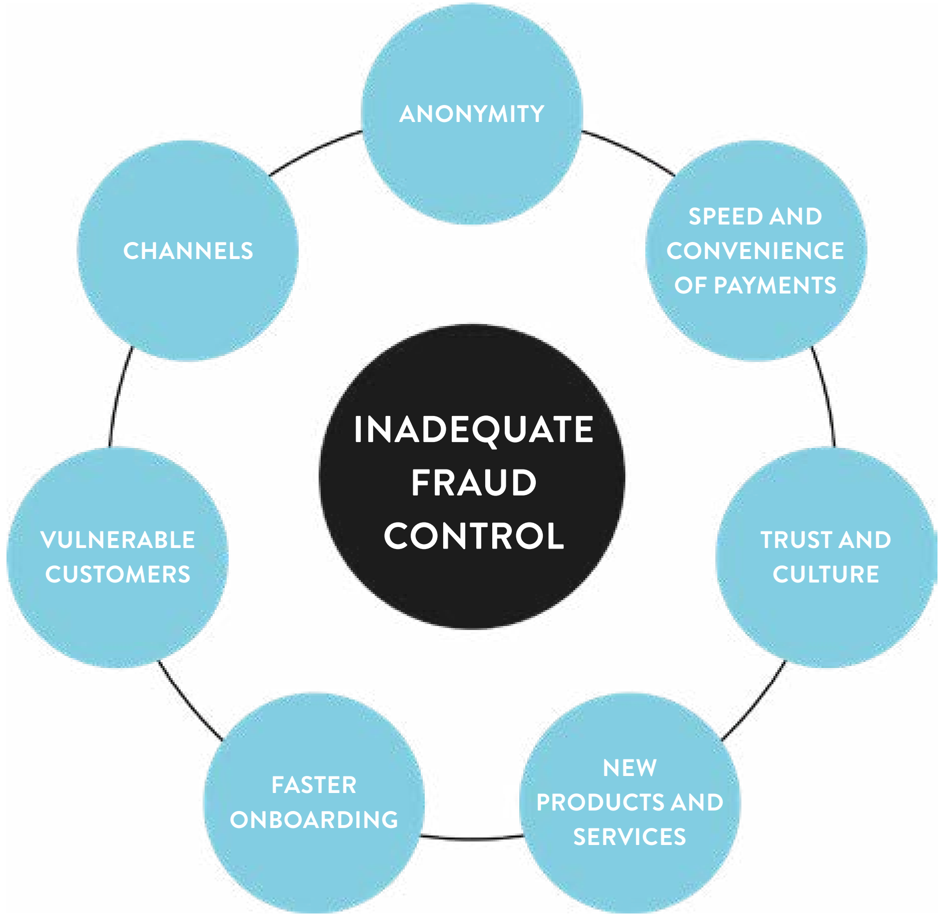
	BANKS AND BUILDING SOCIETIES	CONSUMER CREDIT	GENERAL INSURANCE	LIFE AND PENSIONS	UTILITIES	WEALTH AND ASSET MANAGEMENT
1ST	PAYMENTS FRAUD	ID FRAUD	INSIDE FRAUD	ID FRAUD	INSIDE FRAUD	CYBER - ENABLED FRAUD
2ND	ID FRAUD	INSIDE FRAUD	FALSE CLAIMS FRAUD	CYBER - ENABLED FRAUD	FALSE CLAIMS FRAUD	PAYMENTS FRAUD
3RD	CYBER - ENABLED FRAUD	MISUSE OF FACILITY	ID FRAUD	INSIDE FRAUD	CYBER - ENABLED FRAUD	INSIDE FRAUD

CHARACTERISTICS OF A FRAUD

INDIVIDUALS COMMIT FRAUD FOR A VARIETY OF REASONS HOWEVER, THE LIKELIHOOD OF THEM BEING SUCCESSFUL IN COMMITTING THE FRAUD WILL BE DEPENDENT ON BOTH THE OPPORTUNITY PROVIDED TO THEM AND THE SKILLS AND EXPERIENCE THEY POSSESS.

OPPORTUNITY

Our analysis identified seven key organisational and operational characteristics that provide fraudsters with an opportunity to commit fraud which, if not controlled, could create an inadequate fraud control environment.



MOTIVE

Any existing opportunities for fraud will be exploited where an individual is motivated to do so. When asked to explain the fraud risks facing each firm, few responders drew attention to the motivations or the impact that motivation will have on the rigour that the fraudster will apply to defrauding their target. This critical component of any fraud risk should be considered when assessing the risk, as it will assist in establishing the strength of the control that will need to be applied.

As an example, the insider, who sets out to defraud their employer as a consequence of serious upset at work, will likely have their focus set on just their employing organisation, whereas an external fraudster will be searching for an easy target and will quickly transfer their focus to whichever firm they identify as having the weakest controls.

> THE KEY TO MANAGING FRAUD IS BEING BETTER THAN YOUR PEERS: FRAUDSTERS AREN'T STUPID – THEY TARGET THE WEAKEST LINK
>
> BOARD MEMBER, SHORT TERM, LOW COST LENDER

SKILLS AND COMPETENCE

For a fraudster to succeed, they will require specific skills and competence to enable them to carry out the particular type of fraud they are seeking to commit. As an example, the skill set and level of competence for an opportunist is likely to vary significantly to that of the organised fraudster and, although it is not possible to prevent the most skilled and organised fraudsters from committing every fraud, all fraud leaders should be ready to prevent frauds being committed by the most likely perpetrators of that fraud.

Controls that are effective at preventing fraud by an opportunist are less likely to be effective at deterring a skilled or organised fraudster. In practice, this means that the fraud risk assessment will need to reflect the skills required to commit the fraud that is being evaluated and have a control model that is appropriate for preventing that skill set from being effective.

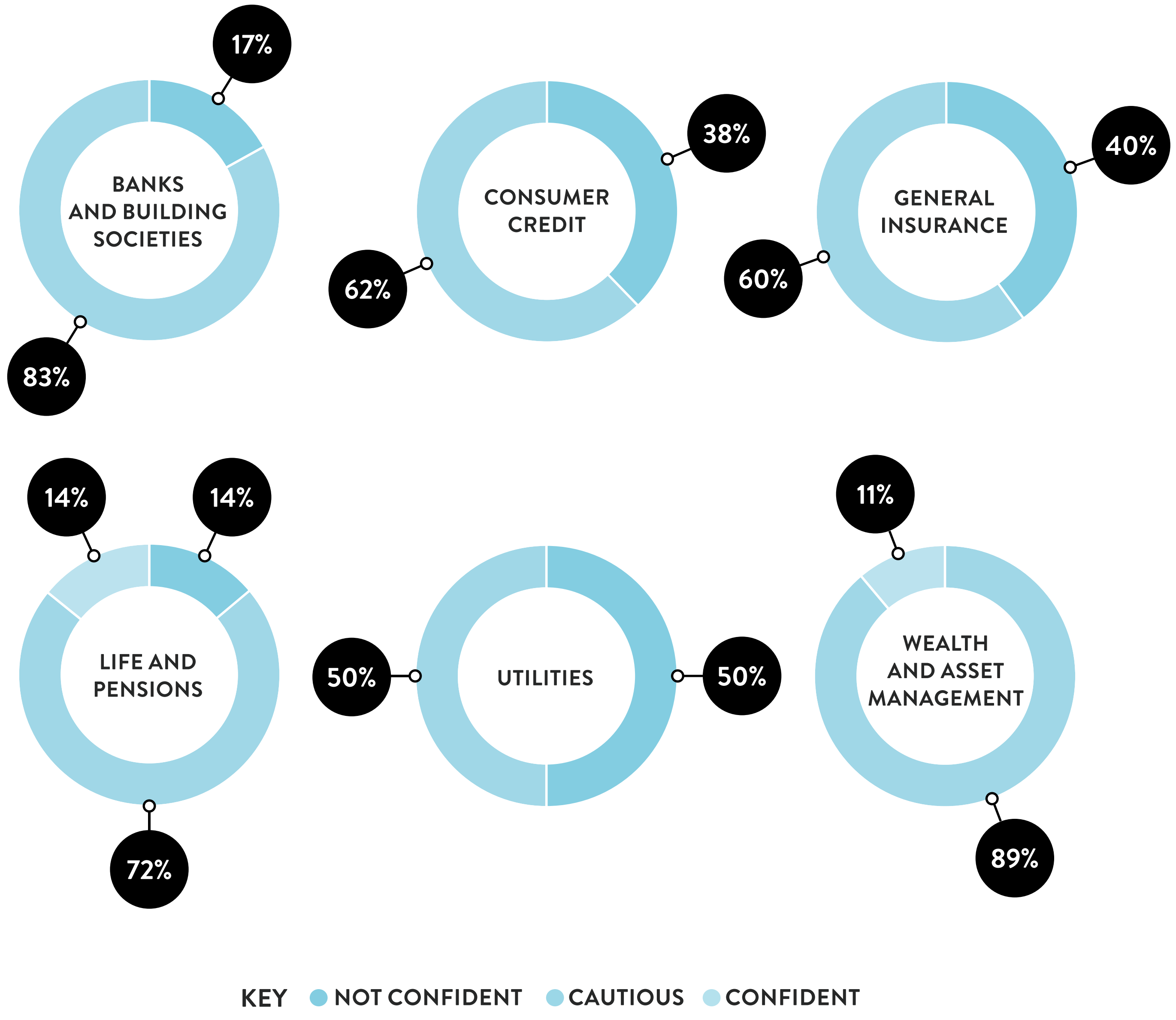
CONTROL FAILURES

Having the right controls in place to not only identify but also mitigate the risk of fraud is therefore essential, although only 5% of our respondents felt confident that they are adequately mitigating fraud risk. Where controls had previously failed, causing firms to suffer fraud losses, the most common of those control failings were:

- Inadequate identification and verification of the customer
- Inadequate customer due diligence procedures
- Inadequate / lack of segregation of duties
- Inadequate / lack of oversight

LINGLIN SONG
PRINCIPAL CONSULTANT
FINANCIAL CRIME AND FRAUD

HOW CONFIDENT ARE YOU THAT YOU ARE ADEQUATELY MITIGATING FRAUD?



The next section of this report goes on to look at how firms can help to adequately protect themselves.

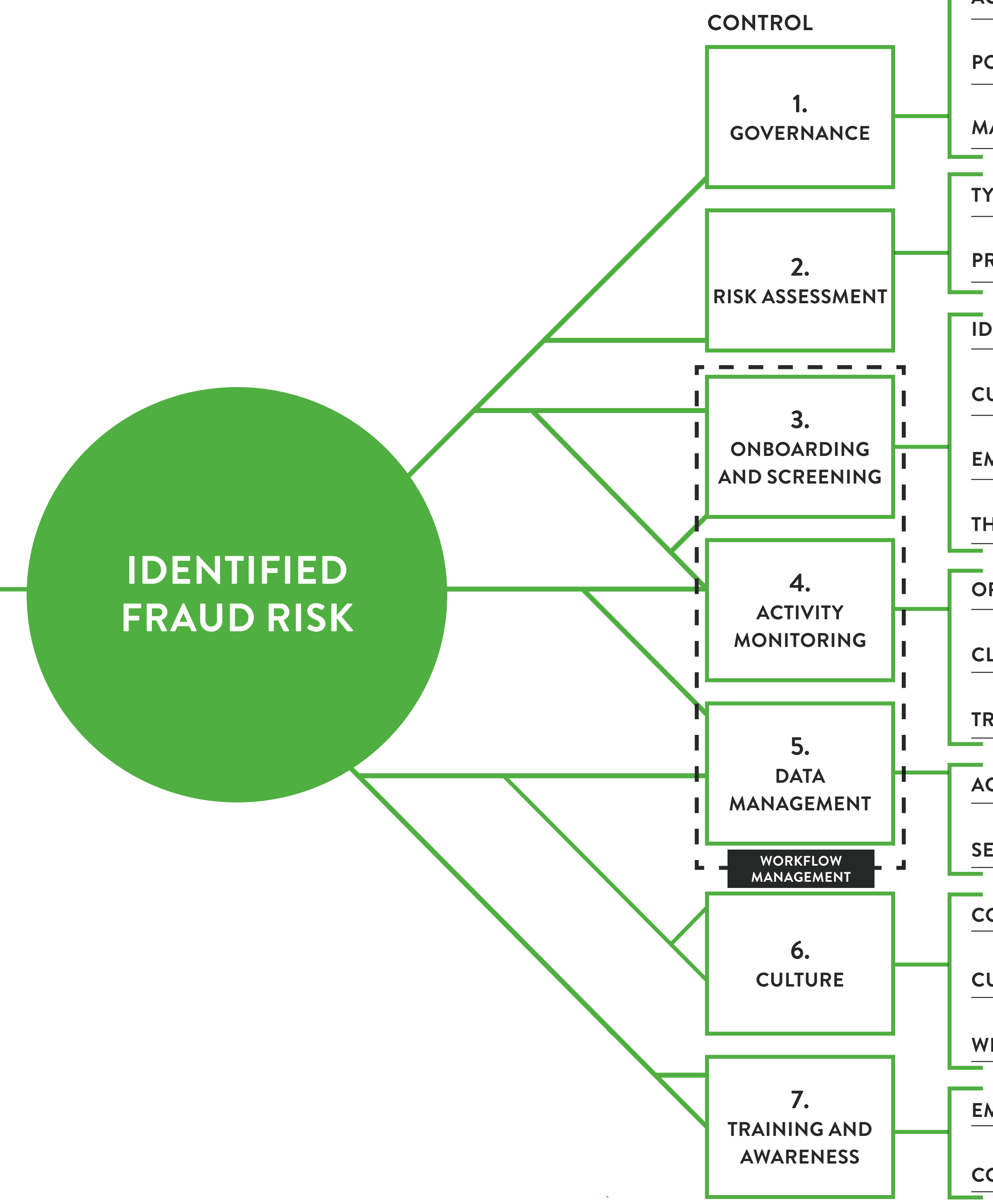
CONTROLLING THE RISK

Whilst there are a wide range of controls that a firm can implement to mitigate its exposure to fraud - ranging from those generic in nature to the more detailed and specific, our analysis has identified seven primary controls, each with its own set of secondary controls, which are essential in ensuring a robust fraud risk management framework:

1. GOVERNANCE
2. RISK ASSESSMENT
3. ONBOARDING AND SCREENING
4. ACTIVITY MONITORING
5. DATA MANAGEMENT
6. CULTURE
7. TRAINING AND AWARENESS

Of these seven controls, three are operational in nature, and so should be integrated within the operational workflow process that they are designed to protect (e.g. onboarding / screening controls, activity monitoring controls and data management). The remainder are more typically part of a broader governance framework and so should support and challenge the delivery of the firm's operational model activity (e.g. governance, risk assessment, culture and training and awareness).

THIS MODEL SHOWS THE RELATIONSHIP BETWEEN THE IDENTIFIED FRAUD RISKS, THE SEVEN PRIMARY CONTROLS AND THE SUBSEQUENT SECONDARY CONTROLS.



	IDENTITY (ID) FRAUD	INSIDE FRAUD	FALSE CLAIMS FRAUD	CYBER - ENABLED FRAUD	ORGANISED SCAMS	PAYMENTS FRAUD	MISUSE OF FACILITY
FRAUD STRATEGY AND BOARD COMMITMENT	●	●	●	●	○	●	●
ACCOUNTABILITY AND OVERSIGHT	●	●	●	●	○	●	●
POLICY AND PROCEDURE FRAMEWORK	●	●	●	●	○	●	●
MANAGEMENT INFORMATION / REPORTING	●	●	●	●	○	●	●
TYPOLOGY BASED RISK ASSESSMENT	●	●	●	●	○	●	●
PROCESS BASED RISK ASSESSMENT	●	●	●	●	○	●	●
IDENTIFICATION AND VERIFICATION	●	●		●	○		
CUSTOMER SCREENING	●		●	●	○	●	
EMPLOYEE SCREENING	●	●		●	○		
THIRD PARTY SCREENING	●	●		●	○	●	
OPEN SOURCE MONITORING	●	●	●	●	○	●	●
CLOSED SOURCE MONITORING	●	●	●	●	○	●	●
TRANSACTION MONITORING				●	○	●	●
ACCURACY AND ACCESSIBILITY	●	●	●	●	○	●	●
SECURITY		●			○		●
CODE OF ETHICS		●					
CULTURAL ASSESSMENT		●					
WHISTLEBLOWING		●			○		
EMPLOYEE EDUCATION AND AWARENESS	●	●	●	●	○	●	●
CONSUMER EDUCATION AND AWARENESS	●	●	●	●	○	●	●

67% of the respondents stated that their approach to fraud controls had changed significantly during the past five years, with most stating the focus had increased as their firms have grown. In terms of expected future developments, respondents identified the following five areas of focus:

ADVANCES IN TECHNOLOGY

A greater use of systems and the introduction of far more advanced systems, particularly at the front end. Fewer manual processes and more advanced algorithms, such as for customer risk-scoring.

CUSTOMER EDUCATION AND PROTECTION

More focus on an improved customer journey and the impact that fraud has on the customer. Greater focus on how the consumer can be protected from fraud, particularly from social engineering. This will include more emphasis on consumer education and employee training - recognising that humans can be the weakest link.

MORE AUTOMATION, ANALYTICS AND ROBOTICS

For both prevention and investigations to augment and streamline manual processing.

IMPROVED DATA SHARING

Within industry sectors and improvement management information within firms.

HIGHER SKILLED RESOURCE

Increased use of technology and fewer manual processes will need to be augmented by suitably skilled resource. More focus on accountability.

THE FOLLOWING SECTIONS LOOK AT EACH OF THE CONTROLS IN FURTHER DETAIL WHILST BRINGING OUT THE FINDINGS FROM OUR RESEARCH

1. GOVERNANCE

Good governance practices drive better-informed decision making at senior management level, improve the anti-fraud control environment and increase investor confidence and consumer trust. These practices can be categorised as follows:

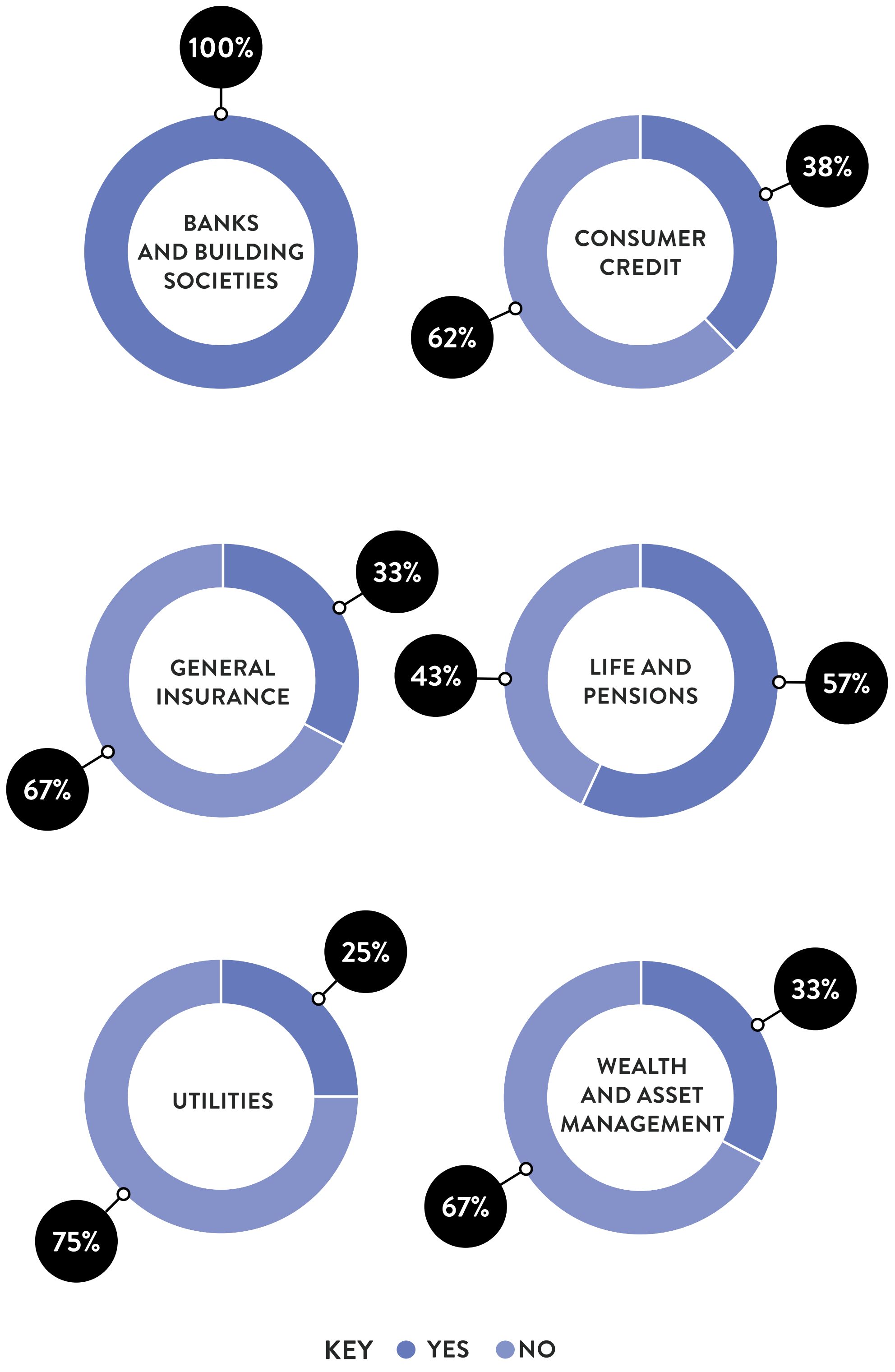
- Fraud strategy and board commitment
- Accountability and oversight
- Policy and procedure framework
- Management information and reporting

FRAUD STRATEGY AND BOARD COMMITMENT

Fraud risk management needs to be seen by firms as a priority, and fraud awareness at board level is vital in building robust and proportionate anti-fraud governance across all layers of the firm; this is where the anti-fraud strategy and message originates. Good practice identified through the survey included, the board maintaining a strong awareness of fraud through board-level training, regular discussions and updates at board meetings. For some firms this was supplemented with an annual 'in-depth' review.

100% OF BANKS AND BUILDING SOCIETIES STATED THAT FRAUD IS AN EXPLICIT AGENDA ITEM AT BOARD MEETINGS

IS FRAUD AN AGENDA ITEM FOR THE BOARD?



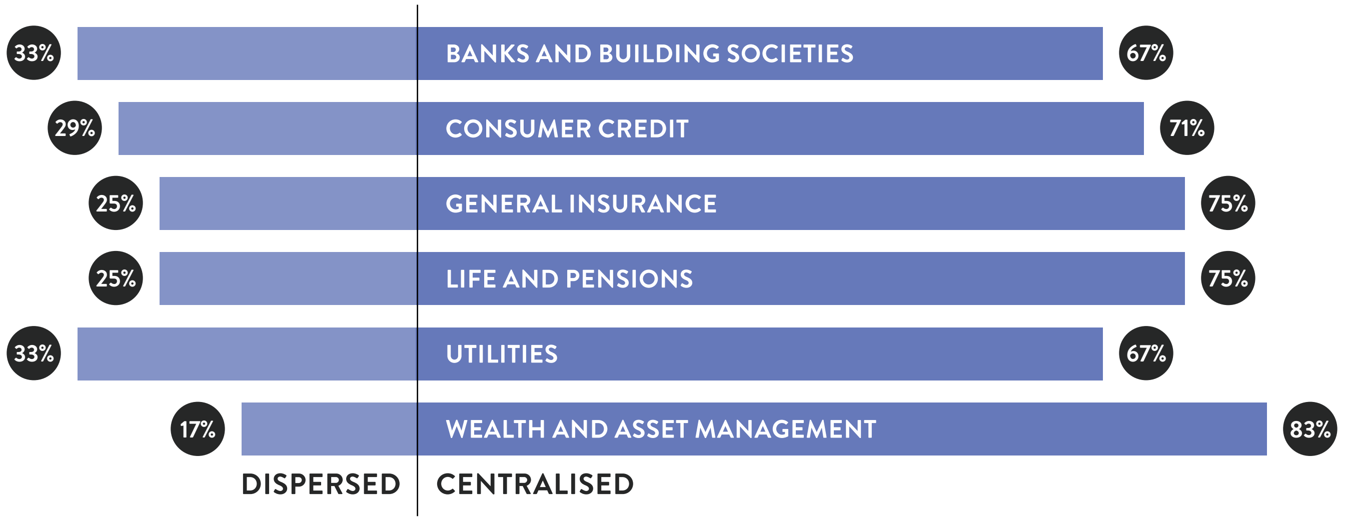
ACCOUNTABILITY AND OVERSIGHT

It is good practice for a named key senior manager to hold overall responsibility for fraud and ensure that the firm's fraud strategy is implemented effectively throughout the firm. Regardless of which senior manager holds responsibility, this should be documented under the roles and responsibilities as part of the Senior Managers and Certification Regime (SM&CR). A number of our participant firms have already mapped accountability, with 28% of respondents identifying the Chief Risk Officer (CRO) as accountable for financial crime risk and 28% stating the Money Laundering Reporting Officer (MLRO) as accountable.

Where oversight activities are then delegated to risk related functions or committees, the board and accountable individuals should assess whether the key risk management, compliance, and internal control roles are well positioned within management, to take the appropriate actions and escalate significant fraud issues for the board's attention.

We asked firms to confirm whether they had consolidated their key fraud resources under the control of centralised leadership or whether they remain distributed across the firm. Most firms in all sectors have a centralised model although, this was usually balanced by having functional reporting lines from the fraud specialists within the operations teams into the centralised model.

ARE YOUR FRAUD RESOURCES CENTRALISED OR DISPERSED?



POLICY AND PROCEDURE FRAMEWORK

A firm's approach to mitigating fraud should be fully documented, regularly reviewed and updated, with any changes cascaded throughout the organisation. All staff should be made aware of the firm's fraud policies and procedures, with regular training provided to not only ensure everyone understands the board's view and objectives in relation to fraud, but also the role they play. Should any policy breaches occur, these must be escalated immediately.

In terms of maintaining policy and risk records, most firms stated that they use Excel spreadsheets, with few firms embedding risk management software solutions that are capable of aligning policies with risks and controls.

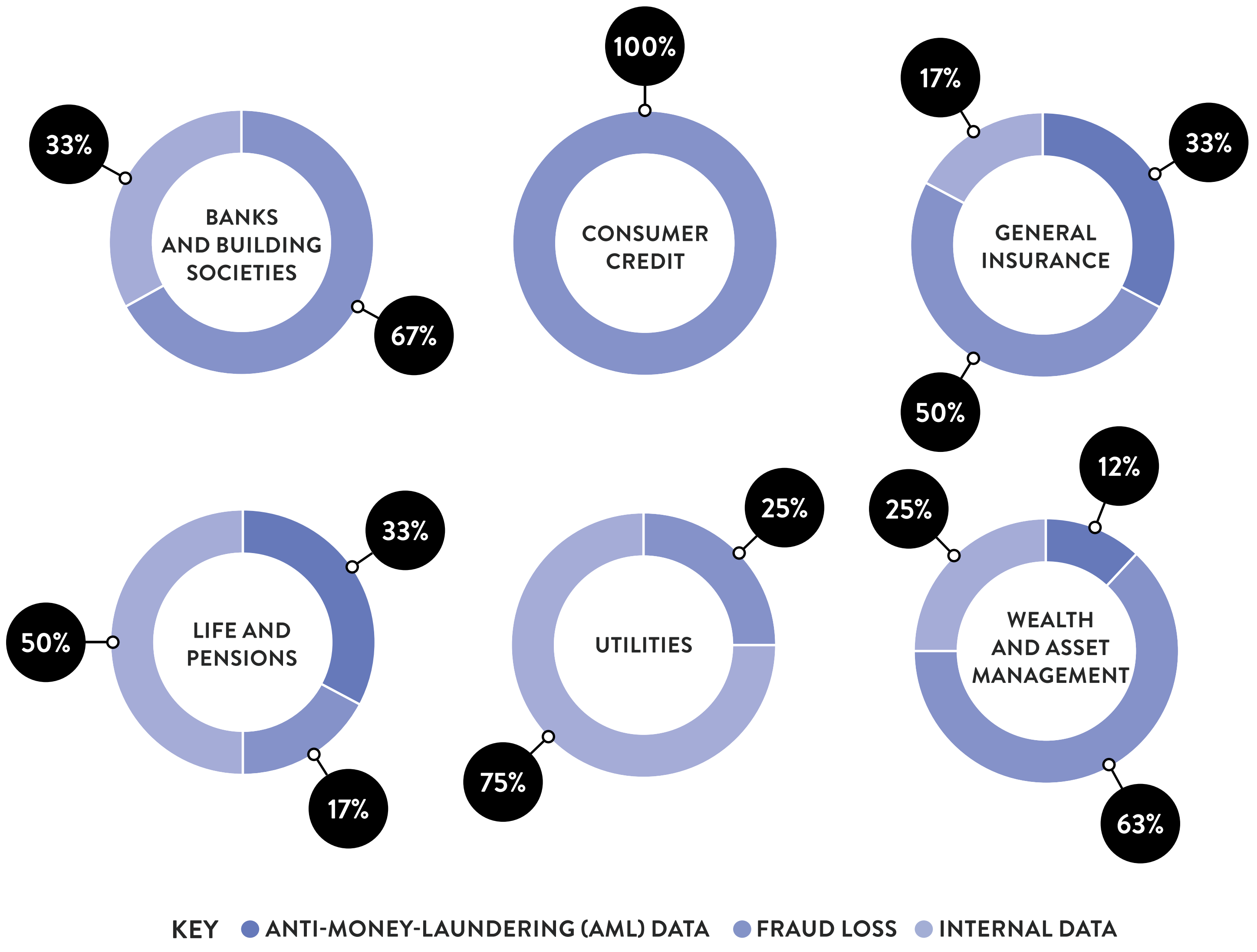
MANAGEMENT INFORMATION AND REPORTING

MI should be obtained from across the business to:

- Provide an accurate and complete view of the fraud threat
- Assist the understanding of risk
- Enable informed decisions to be made to mitigate the risk

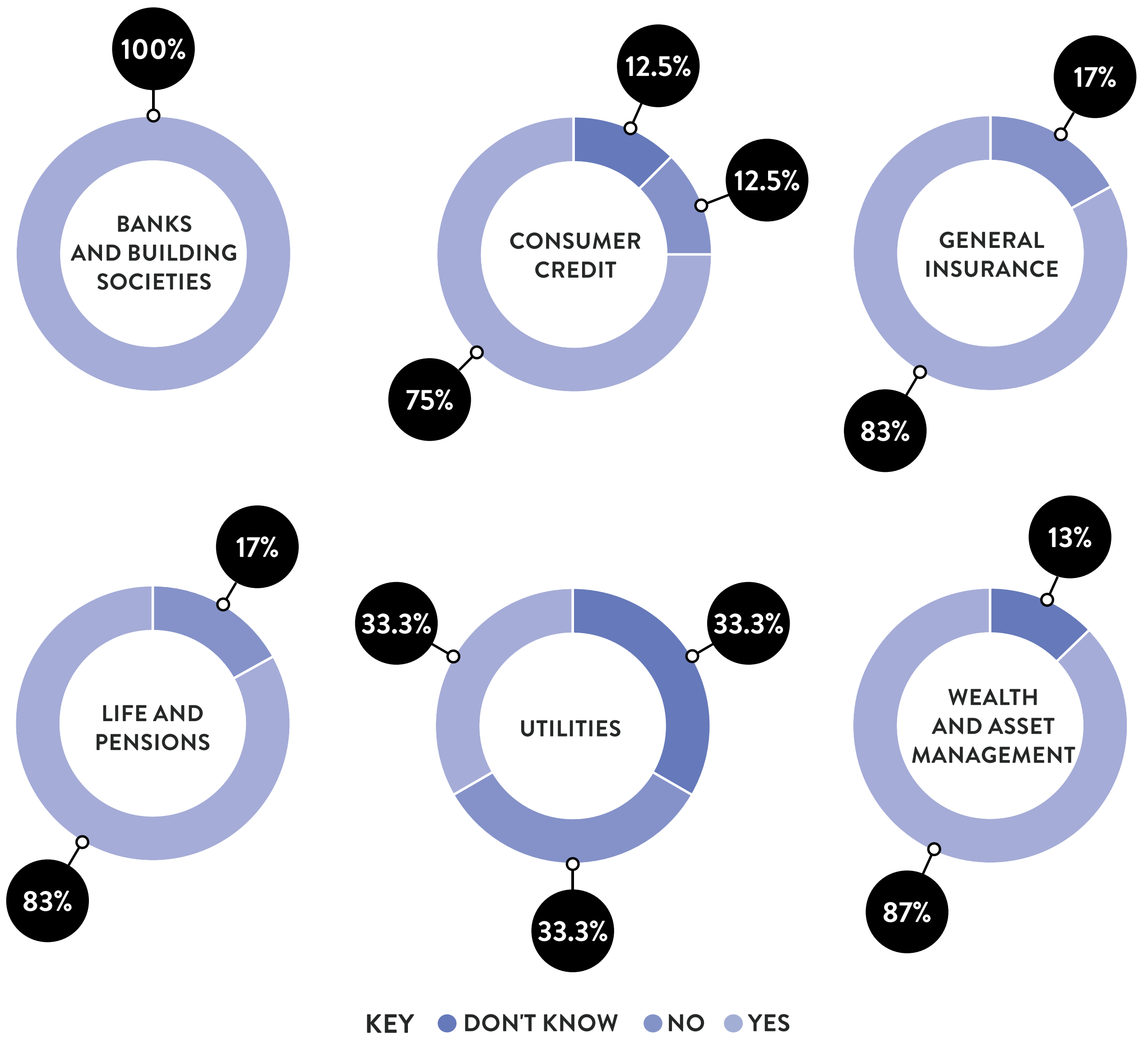
The MI reported by our respondents in terms of the adequacy of fraud controls, varied depending on the sector asked - with consumer credit respondents limiting their MI to the direct cost of fraud losses.

WHAT MI DO YOU REPORT TO SHOW THE ADEQUACY OF YOUR FIRM'S FRAUD CONTROLS?



To ensure a firm's anti-fraud performance is digestible and enables focused discussion at board level, fraud MI should be consolidated into a 'single fraud report' to provide an overarching view of the performance of the firm's fraud risks and controls. Top-down MI requirements should also be set to ensure that the board receives an accurate view of the entire fraud risk and control environment to assess the effectiveness of their fraud strategy. 80% of respondents we interviewed have a 'single fraud report' in their firm.

IS THE MI CONSOLIDATED INTO A 'SINGLE FRAUD REPORT' TO PROVIDE A SINGLE VIEW OF FRAUD RISKS ACROSS YOUR BUSINESS?



> MANAGEMENT INFORMATION OF FRAUD IS RECEIVED BY THE BOARD VIA THE RISK COMMITTEE WITHIN A RISK PACK THAT HAS A SECTION FOR FINANCIAL CRIME. THE STATUS OF EACH FINANCIAL CRIME IS REPORTED ALONGSIDE KPIs. THESE ARE CONTINUALLY REVIEWED AND MADE SURE THEY ARE FIT FOR PURPOSE
>
> NED,
> CONSUMER FINANCE
> PROVIDER

2.
RISK ASSESSMENT

All firms should have arrangements in place to identify and assess both current and emerging fraud threats and should deploy controls that are effective at mitigating them. To assist these efforts, firms should establish standardised definitions for fraud, utilising industry recognised definitions where possible, and implement a risk assessment methodology capable of identifying both:

- Fraud risks that may cause defined operational 'workflow' processes to be disrupted (e.g. 'customer journey')
- The firm’s exposure to thematic and typology-based fraud risks (e.g. 'identify fraud')

Risk management frameworks should be designed to include control testing and control effectiveness monitoring and involve timely refreshes of the risk assessment (e.g. during change activity, when new typologies emerge and during scheduled refreshes). In terms of risk assessment activity, some examples identified by the respondents included:

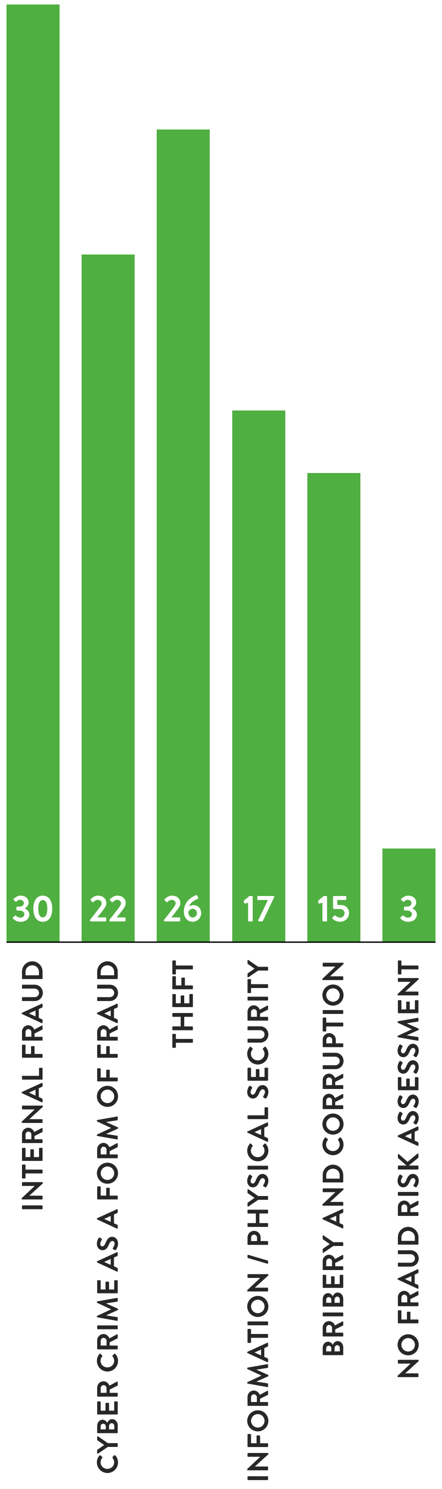
FIRST LINE:

- Attestations from stakeholders that own the risk and controls, such as heads of business units, but also accountable senior executives
- Daily, monthly, quarterly or annual control testing

COMPLIANCE AND / OR AUDIT:

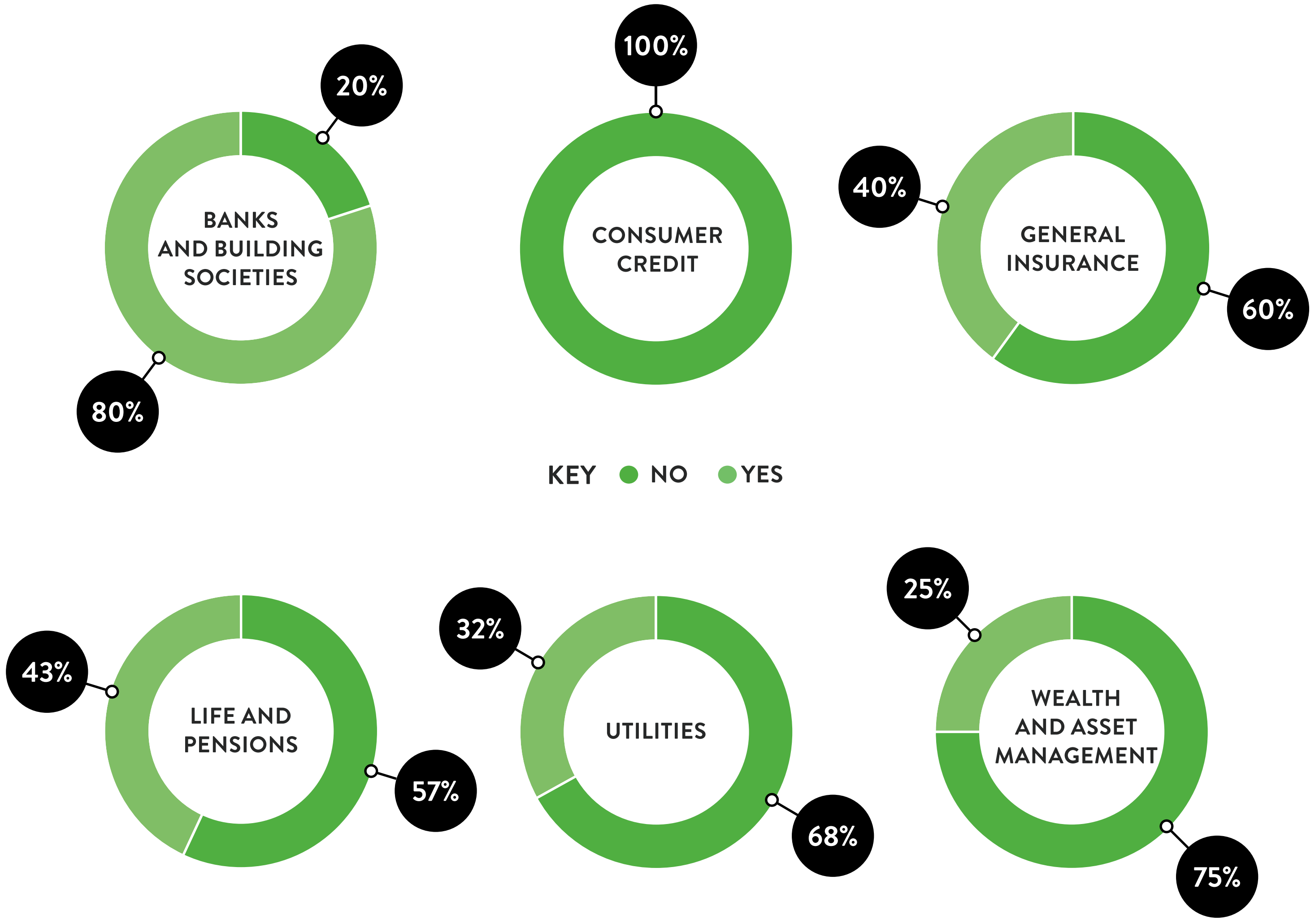
- Daily, monthly, quarterly or annual control testing quality assurance
- Testing of employee and third-party adherence to policies and procedures
- Thematic deep dives into high risk areas
- Independent assurance audits on an annual basis
- Mystery shopping
- Penetration testing

Firms were asked to name the fraud typologies they consider and the frequency of each review, as seen in the diagram here. This revealed that ‘internal fraud’ threats were the subject of most reviews and that a small proportion of firms do not undertake any fraud specific risk assessments.



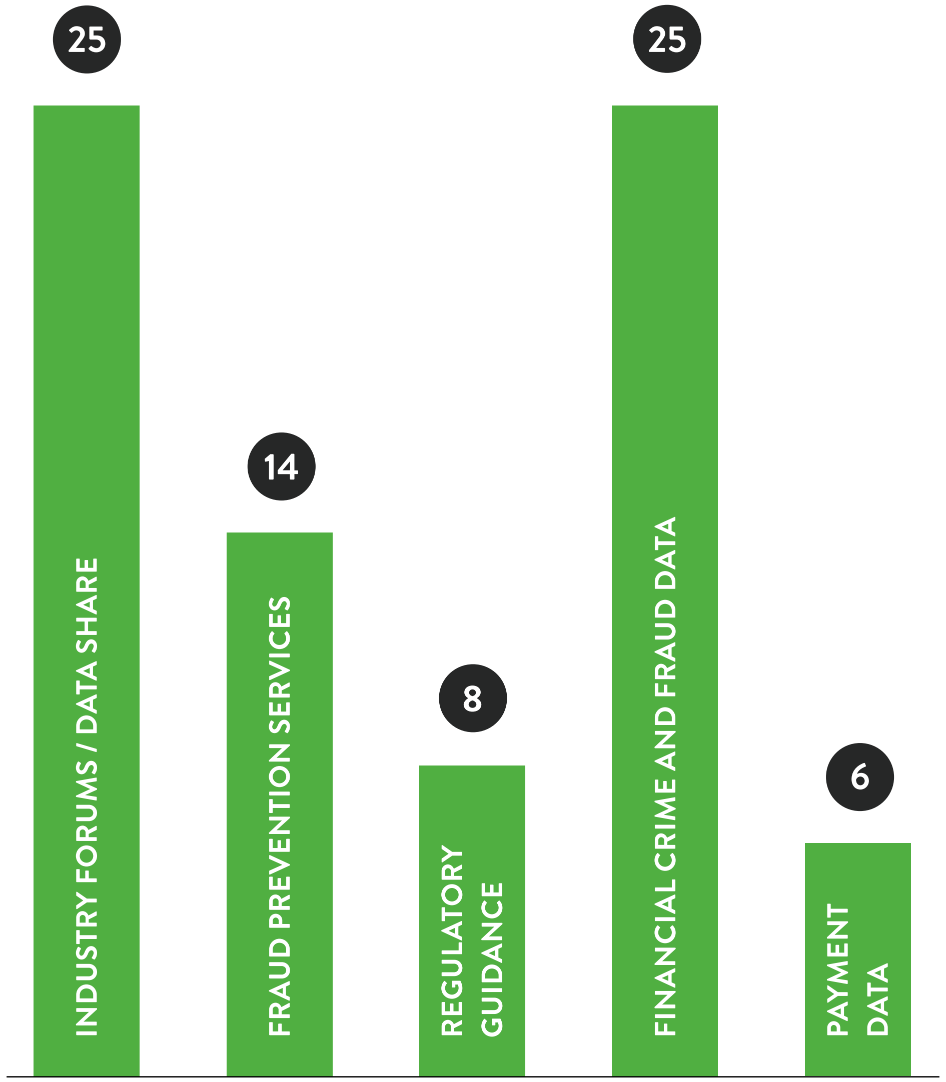
There are a wide range of data sources in the public domain which provide firms with sufficient information to build a forward-looking and proactive approach, to preventing and detecting fraud. However, this external data should be supplemented by industry specific data to provide fraud control leaders with targeted insights into the risk and control environment. Our research highlighted a significant gap in the sharing of industry specific data between firms, with few sharing credible benchmarking information. Benchmarking fraud can often be seen as highlighting a competitive disadvantage against peers, but should instead be viewed as an essential component in any firm's fraud risk management practices.

HAVE YOU BENCHMARKED YOUR FRAUD RISK MANAGEMENT PRACTICE?



Firms identified a broad range of useful information sources which include:

WHAT INTERNAL AND EXTERNAL DATA OR INFORMATION DO YOU UTILISE IN ORDER TO ASSIST YOUR FRAUD RISK ASSESSMENT / HELP YOU UNDERSTAND THE FRAUD RISK YOUR BUSINESS FACES?



The table below provides greater detail about the potential data sources and providers of the data. These were mentioned by interviewees, when asked to identify the data used by them in order to understand and control the risk of fraud. The list is not an exhaustive record of all potential sources or providers however, is a reflection of the responses provided to the interview questions.

INTERNAL DATA

CUSTOMER DATA

- Customer feedback
- Refunds
- Customer behaviours
- Credit reference data
- Authorisation limits
- Charge-backs
- Early arrears
- Early settlements
- Suspicious addresses
- Suspicious email addresses / phone
- Near losses
- Internet Protocol (IP) addresses
- Transaction patterns
- Suspicious activity reports

EMPLOYEE DATA

- Expenses
- Payments
- Turnover
- Fraud near losses
- Data breaches
- Suspicious addresses
- Suspicious email address / phone number

EXTERNAL DATA

GOVERNMENT BODIES

- Financial Conduct Authority Guidance
- UK National Risk Assessment
- Driver and Vehicle Licensing Agency
- Joint Money Laundering Intelligence Taskforce

GLOBAL GUIDANCE

- Financial Action Task Force
- Transparency International

INDUSTRY BODIES

- UK Finance
- CIFAS
- Financial Fraud Action
- National Hunter Data
- Worldpay
- SWIFT
- Financial Leasing Authority
- Association of British Insurers
- Personal Investment Management and Financial Advice Association

MEDIA

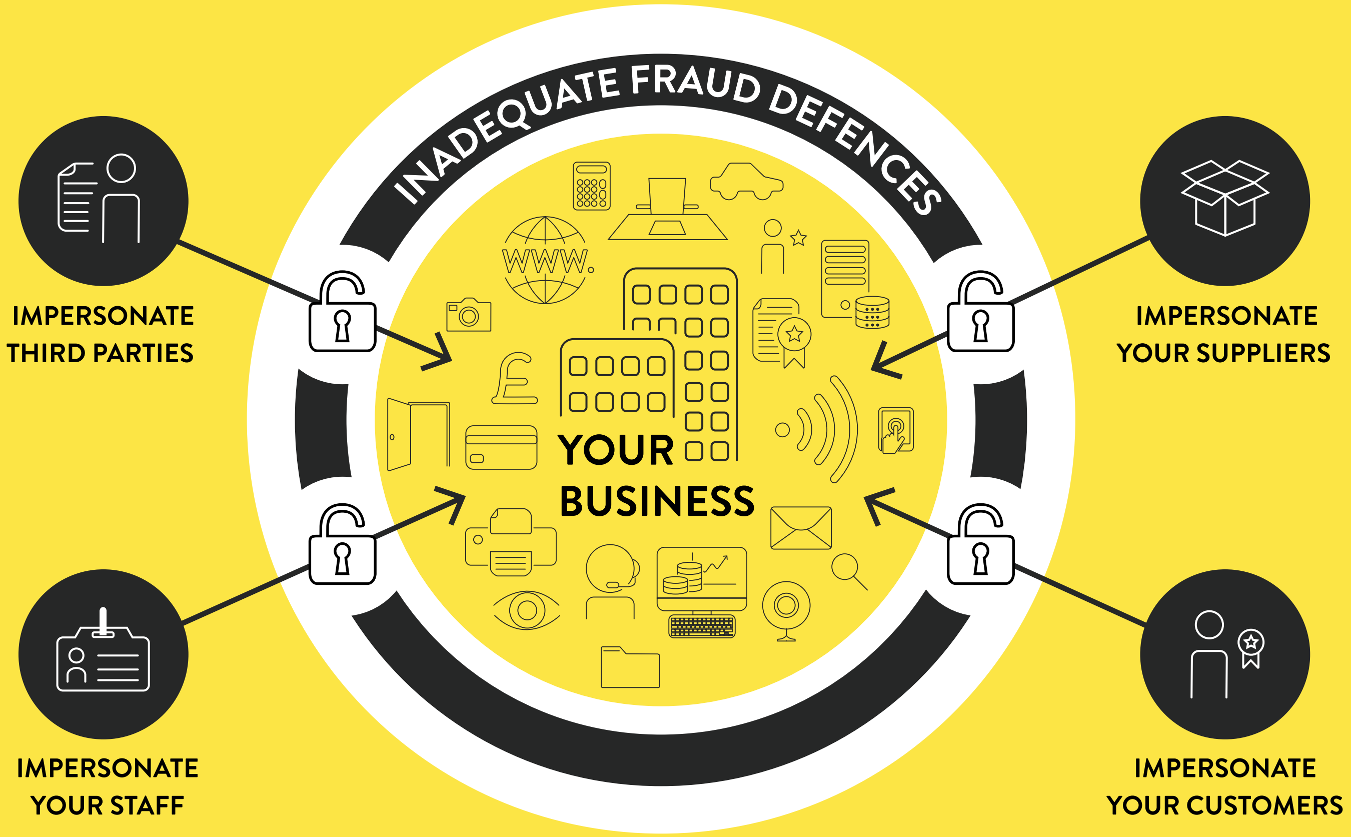
- Financial Times
- Other Online Data

ADDITIONAL DATA ITEMS

- SIRA for fraud prevention & detection
- Solvency information / credit score
- Electoral roll data for ID&V purposes

3. ONBOARDING AND SCREENING

Firms are vulnerable to the risk of onboarding individuals and entities who are not who they claim to be. The threats can come from real individuals who provide true identity records but dishonest information about their circumstances (e.g. qualifications, experience and assets) or by individuals who dishonestly represent themselves to be someone else.


INADEQUATE FRAUD DEFENCES
YOUR BUSINESS
IMPERSONATE THIRD PARTIES
IMPERSONATE YOUR SUPPLIERS
IMPERSONATE YOUR STAFF
IMPERSONATE YOUR CUSTOMERS

IDENTIFICATION AND VERIFICATION (ID&V)

The increasing availability of personal information is being exploited by criminals. Firms should ensure that robust Know Your Customer (KYC) checks are in place to verify customers identities and reduce the risk of fraud such as ID fraud, cyber-enabled fraud, inside fraud and organised scams. These checks can include verifying documents such as passports and driving licences using free, or even paid for systems, and government sourced data.

CUSTOMER SCREENING

Screening provides firms with risk information relating to new and existing customers. It should involve screening for prohibited persons / activity (e.g. trade sanctions), politically exposed persons (PEPs), suspected fraudsters and fraud indicators. These checks can assist firms to screen out individuals who do not meet the firm's risk thresholds or to introduce additional controls for individuals who pose an increased risk.

EMPLOYEE SCREENING

Knowing who you are hiring is just as important as knowing the customers you are onboarding. Several of the firms identified risks created by organised criminal groups targeting their employees or placing their people within firms.

Section 21 of the Money Laundering Regulations 2017 now places a compliance duty on firms to carry out screening on their employees and agents, which includes an assessment of their skills, knowledge, expertise, conduct and integrity. To meet this requirement and ensure an undue burden is not placed on your firm, a risk-based approach should be taken where, for example, stringent due diligence procedures are applied for high-risk roles involving a position of trust prior to appointment.

BESIDES BEING A REGULATORY REQUIREMENT, A CONTINUOUS EMPLOYEE SCREENING PROGRAMME IS AN EFFECTIVE TOOL IN MITIGATING THE RISK OF INTERNAL AND OTHER FRAUDS

THIRD PARTY SCREENING

Due diligence over third parties goes beyond collating routine documentary evidence and requires an inquisitive mind to understand the nature of the business and its relationship to the risk involved. The increased complexity in the way firms distribute their products or rely on third parties for the provision of services, has made managing risk more challenging. Monitoring and oversight of these third party relationships is a key requirement for any organisation to ensure it proactively identifies and minimises risks, and demonstrates that effective controls are in place.

4. ACTIVITY MONITORING

Having onboarded a customer or third party, due diligence should then be viewed as a 'business as usual' activity. This should be with an ongoing process that is triggered if there is a change of circumstances or if MI indicates the risk rating of the third party has changed. Monitoring can be conducted in a variety of ways using open and closed sources and through the review of transactions.

OPEN SOURCE MONITORING

Many firms use a variety of open sources, such as internet investigation including the dark web and social media; regulatory references; and government data sources including Companies House and sanctions lists, for ongoing monitoring, although it has been recognised that these checks are time-consuming and require resources.

CLOSED SOURCE MONITORING

Firms are also utilising paid for services to obtain more in-depth, reliable and personalised data, which is relevant to their specific organisation. This can include access to restricted information such as driving licence numbers, credit references and the CIFAS internal fraud database.

TRANSACTION MONITORING

Firms are wary that greater monitoring may increase alerts and require more investigation resource. Consequently, some firms design their systems to limit the number of alerts that can be processed by a specific team. This means the system is at risk of failure, as it will reduce the ability of the monitoring tool to identify suspicion. Improvements in rule and workflow design can enable firms to become more effective at identifying suspicion or changes in an individual's risk profile, and the responses revealed an emerging trend for firms to move toward design and delivery of robotics and process automation (RPA) solutions within their monitoring.

> PROACTIVE DATA MONITORING AND ANALYSIS ARE AMONG THE MOST EFFECTIVE ANTI-FRAUD CONTROLS. FIRMS WHICH UNDERTAKE PROACTIVE DATA ANALYSIS TECHNIQUES EXPERIENCE FRAUDS THAT ARE 54% LESS COSTLY AND 50% SHORTER THAN ORGANISATIONS THAT DO NOT MONITOR AND ANALYSE DATA FOR SIGNS OF FRAUD
>
> ASSOCIATION OF CERTIFIED FRAUD EXAMINERS (ACFE), REPORT TO THE NATIONS ON OCCUPATIONAL FRAUD AND ABUSE, 2016 GLOBAL FRAUD STUDY

5. DATA MANAGEMENT

ACCURACY AND ACCESSIBILITY

Information obtained from customers is typically stored in different formats and across various systems. This provides a challenge for firms seeking to establish the full extent of their relationship with any one individual and ensuring the data held for that individual is complete and correct. GDPR is however driving firms to improve data quality, which should help to improve the effectiveness of fraud controls that rely on that data.

42% OF FIRMS STATED THEY POSSESS A SINGLE VIEW OF THE CUSTOMER, WITH OTHERS CITING IT AS A 'DESIRED STATE'

Our research found, that an increasing number of firms are seeking to utilise additional data sources in an effort to more fully understand the customer's identity and behaviour, with quoted data sources including:

- Locations analytics
- IP address analytics
- Password analytics
- Social networks
- Application patterns
- Purchasing patterns
- Voice data (e.g. internal database of the voices of suspected fraudsters)

SECURITY

With the increased risk of cyber-enabled fraud, the need for security has expanded far beyond that of just physical controls and firms are feeling the pressure to keep up - particularly when legacy systems and controls are utilised. Firms now need to not only have physical controls in place such as CCTV, employee access passes, classifications (e.g. confidential and employees only) and locked cabinets, but also cyber and information security controls including passwords, encryption and email monitoring.

MARK TOWNSLEY
FINANCIAL CRIME REGULATORY AFFAIRS MANAGER

6. CULTURE

Culture underpins all aspects of organisational performance: commercial, customer, conduct or employee engagement. A strong culture aligned to the strategic vision of a firm will facilitate the effective delivery of short and long-term business objectives. Delivering an effective culture is not about defining whether it is good, bad or compliant in absolute terms; it is about assessing whether the culture is fit for purpose to take the business on its strategic journey and whether it allows people to make the right decisions for customers and business success.

CODE OF CONDUCT

Defining and embedding the desired culture within your firm is crucial for managing fraud risk. When embedding an anti-fraud culture, the 'tone from the top' needs to promote ethical practices and evidence determination in preventing, detecting and managing fraud. It is also important that a fraud and ethics policy is established with strong oversight of adherence in place where integrity is rewarded, and mechanisms are established for identifying, reporting and responding to violations.

WHISTLEBLOWING

A key control outside of systems is your people. Ingraining and actively promoting a culture where employees feel safe to speak up could increase the likelihood of potential frauds, such as organised scams or insider fraud being identified earlier. Best practice is to appoint one senior member as a point of contact but, depending on the size of your organisation, a whole designated team may be in place.

> **A HUGE DETERRENT TO FRAUD IS HAVING THE RIGHT POLICIES AND PROCEDURES IN PLACE, INCLUDING ONES LIKE WHISTLEBLOWING, WHICH NEED TO BE EMBEDDED WITH TRAINING AND AWARENESS, AND THE RIGHT CULTURE**
>
> NED,
> CONSUMER CREDIT FIRM

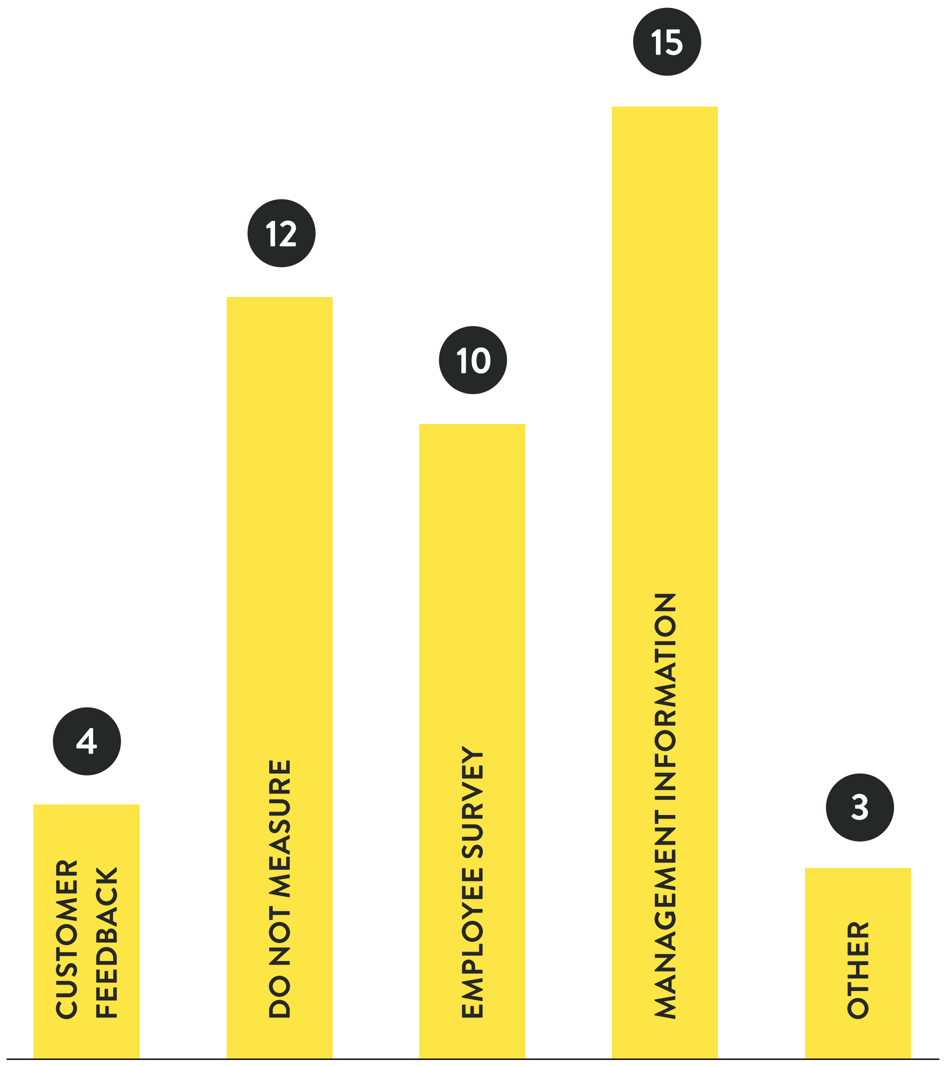
CULTURAL ASSESSMENT

In terms of assessing culture, our respondents use a range of qualitative and quantitative methods, which include employees being encouraged to observe peers' activities and adopting measures for change if required. Although just under a quarter of firms we interviewed use employee surveys and 10% use customer surveys, very few firms considered these results when assessing the effectiveness of their fraud framework. This is particularly surprising considering that failures in corporate culture have been instrumental in enabling highly publicised corporate frauds (e.g. WorldCom and Enron).

Other methods referenced include fraud incidents and senior managements subsequent response, audits and training results.

As with all controls, culture should be managed and reviewed on a regular basis. A failure to do so could result in the firm's culture acting not as an enabler, but as a barrier to effective fraud risk management.

WHAT METHODS DO YOU USE TO MEASURE WHETHER YOU HAVE AN ANTI-FRAUD CULTURE?



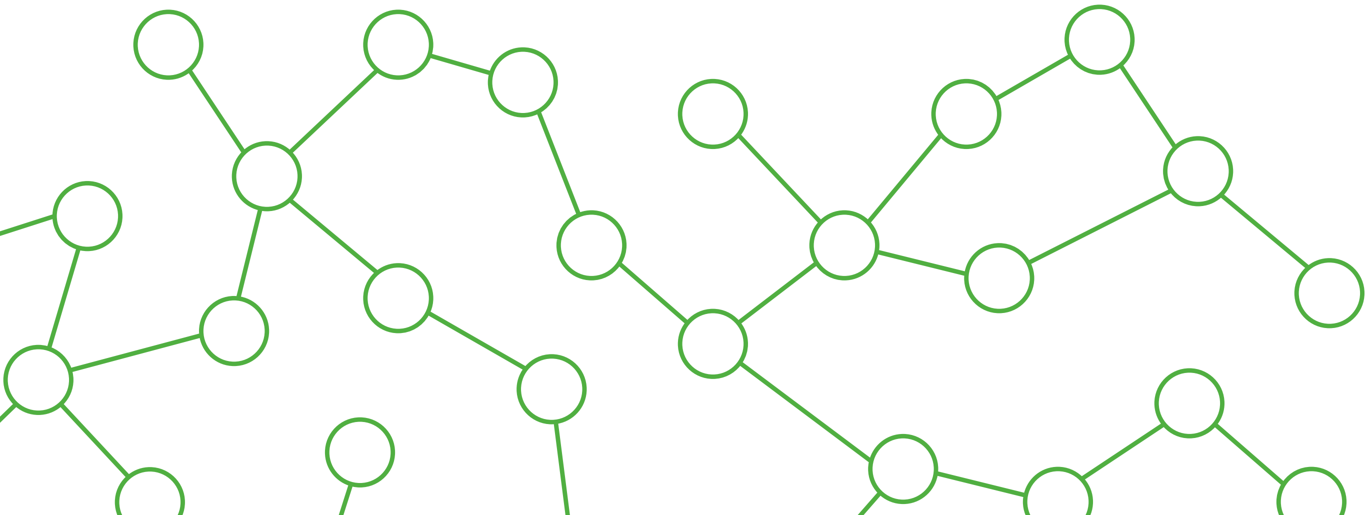
OVER 1/3 OF ORGANISATIONS SURVEYED DO NOT MEASURE WHETHER THEY HAVE AN ANTI-FRAUD CULTURE

7. TRAINING AND AWARENESS

EMPLOYEE EDUCATION AND AWARENESS

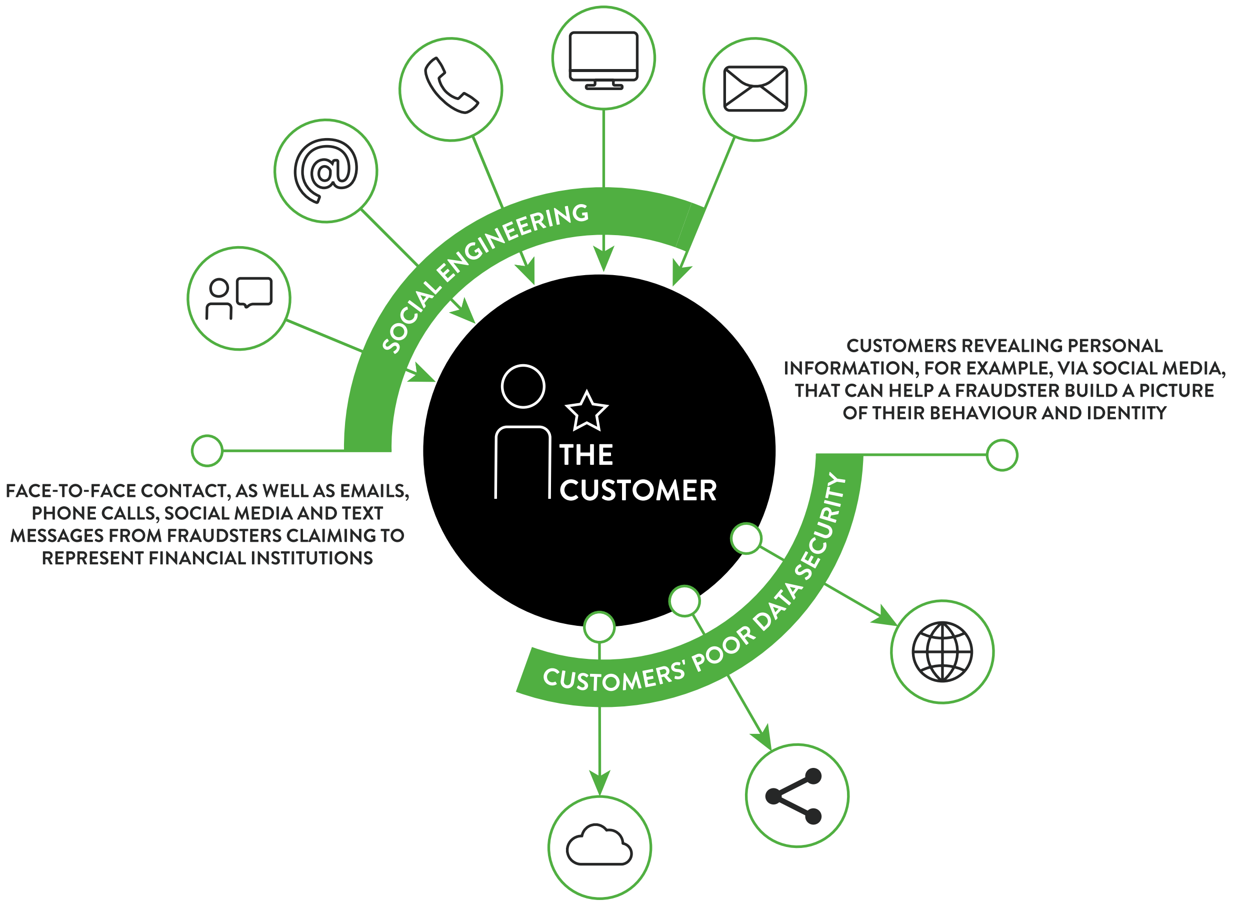
Training and awareness programmes should be undertaken at all levels of the business; from boards to frontline, to ensure both the fraud risk and the firms subsequent culture, policies and procedures are clearly understood. An appropriate blend of different training methods should be adopted, although e-learning is the most popular method used by our respondents, with additional measures factored in for those in higher risk areas or regularly dealing with fraud. These can include centralised repositories of high risk indicators and case studies, e-mail communications detailing where internal and external events have taken place, and attendance at external anti-fraud training, conferences and events.

> FIRMS MUST EMPLOY STAFF WHO POSSESS THE SKILLS, KNOWLEDGE AND EXPERTISE TO CARRY OUT THEIR FUNCTIONS EFFECTIVELY. THEY SHOULD REVIEW EMPLOYEES' COMPETENCE AND TAKE APPROPRIATE ACTION TO ENSURE THEY REMAIN COMPETENT FOR THEIR ROLE. VETTING AND TRAINING SHOULD ALSO BE APPROPRIATE TO EMPLOYEES' ROLES
>
> FCA, FINANCIAL CRIME: A GUIDE FOR FIRMS



CONSUMER EDUCATION AND AWARENESS

The need for training does however span further than just the firm's employees, to include consumers and third parties. Although, only a few of the firms we interviewed roll out training to their third parties, including dealers, brokers, outsourcers and other suppliers. However, many of the firms we interviewed do provide their customers with information about fraud via their website in their terms and conditions and through their mailers. These externally-facing clear anti-fraud messages are key in helping to not only deter potential fraudsters, but to also educate consumers on the risks of social engineering and the importance of data security.



FACE-TO-FACE CONTACT, AS WELL AS EMAILS, PHONE CALLS, SOCIAL MEDIA AND TEXT MESSAGES FROM FRAUDSTERS CLAIMING TO REPRESENT FINANCIAL INSTITUTIONS

CUSTOMERS REVEALING PERSONAL INFORMATION, FOR EXAMPLE, VIA SOCIAL MEDIA, THAT CAN HELP A FRAUDSTER BUILD A PICTURE OF THEIR BEHAVIOUR AND IDENTITY

Implementing a successful training programme does not come without its challenges. Several firms expressed difficulty in engaging their front line in relation to fraud awareness and, taking steps to tackle fraud by spotting and reporting red flags and suspicious activity. Firms also found it difficult to empower lower skilled personnel to speak up or ask probing questions - this was a particular challenge with temporary staff and those who were working in branches, stores, warehouses, remotely or in isolated office locations.

TAKING A HOLISTIC APPROACH

The majority of respondents indirectly highlighted the continued segregated nature of fraud and financial crime controls at their firms; some even segregated the fraud control oversight into different teams for different operational activities (e.g. onboarding, applications, underwriting, surrenders and claims), with little or no communication between these separate teams. The consequence of this segregation meant that some respondents holding fraud control responsibility were only able to identify the risks and controls for their operational activity and had limited knowledge about the fraud controls outside their immediate area.

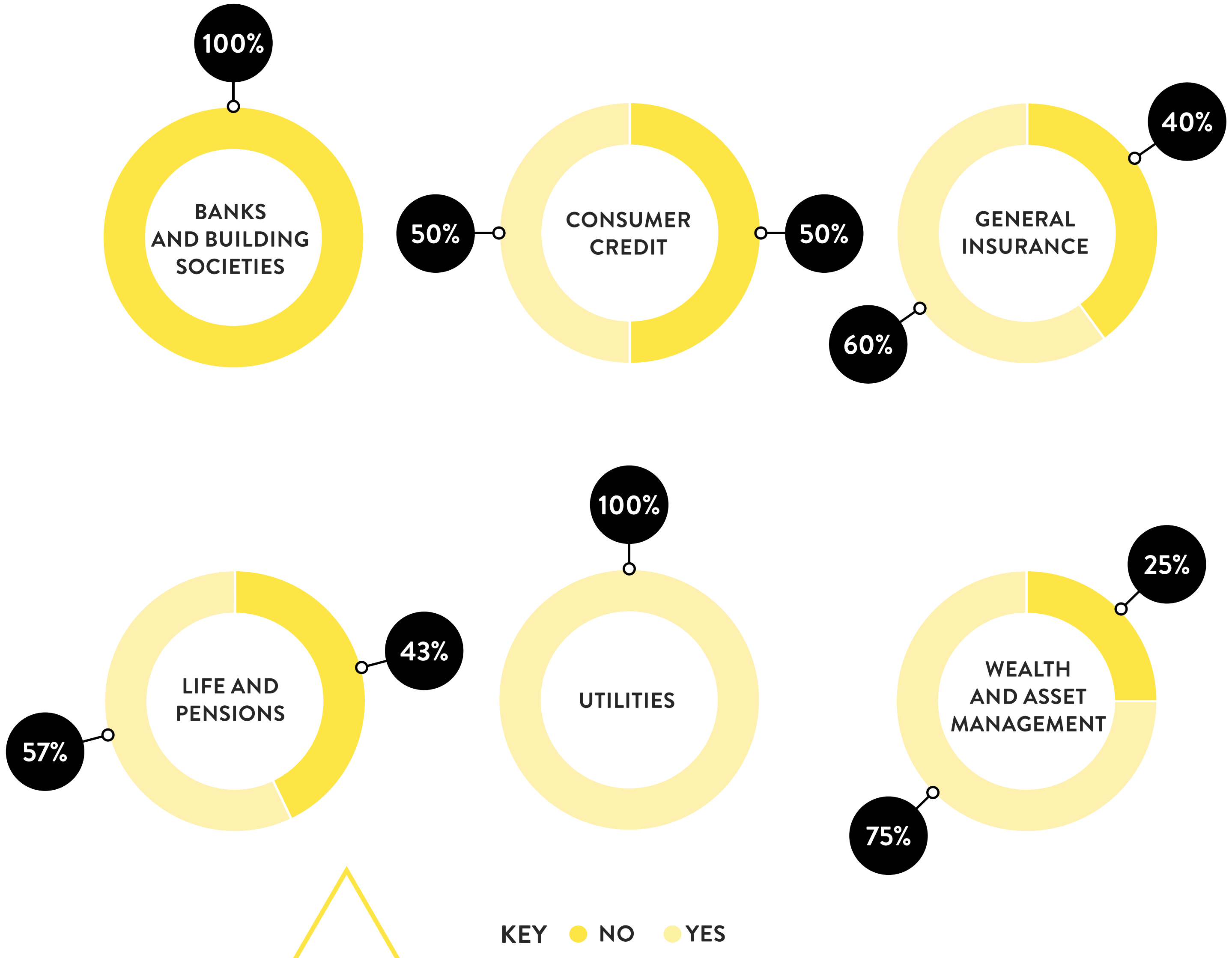
The consequences of running segregated, disconnected control activities are serious and include a reduced customer experience, a less effective control model and a failure to deliver the benefits that could be gained from adopting a more efficient control model.

As a result, firms are increasingly moving towards operating models that provide control efficiencies where controls with multiple risk management benefits (e.g. a control that mitigates fraud, money laundering and improves overall quality) are designed and overseen in a consolidated structure. Whilst this does not mean that individuals are all in the same team, the firm has a shared understanding and responsibility for ensuring that risk and control management is effective, rather than segregated.

This holistic approach should be underpinned by clear, standardised risk assessment methodologies which ensure the assessment activity considers specific typologies, emerging threats and process risks. To ensure it remains effective, the model should reflect dependencies on the risk and control models used elsewhere in the firm.

The absence of a joined-up, holistic approach to managing fraud risks was confirmed by respondents who, when asked whether they held a consolidated register of all controls, responded as follows:

DOES YOUR FIRM HAVE A CONSOLIDATED REGISTER OF ALL FINANCIAL CRIME CONTROL (INCLUDING ALL TYPES OF FRAUD)?



WORKFLOW

Many non-financial services industries organise their operations along end-to-end processes; they receive materials at the start, assemble / organise them in the middle and produce a saleable product at the end. By organising the production efforts along and around defined end-to-end processes, those firms can identify the risks that may cause each process to be disrupted and so can identify where controls could be applied to protect the process in its entirety.

Complex process models are less easy to 'map' but it is the same complexity that means the efficiency and control improvements are likely to be greater than could be possible from a simple process. For example, a complex process might require customer engagement at multiple points, with each requiring a customer 'verification' control. An efficient process would enable the verification to be performed just once during a customer phone call; a less efficient and less connected process might require the verification to be performed several times and in different ways, as the customer is passed around different teams.

Workflow mapping enables firms to identify their key activity (or processes) and the tasks that are involved in delivering it. Examples of possible key processes are;

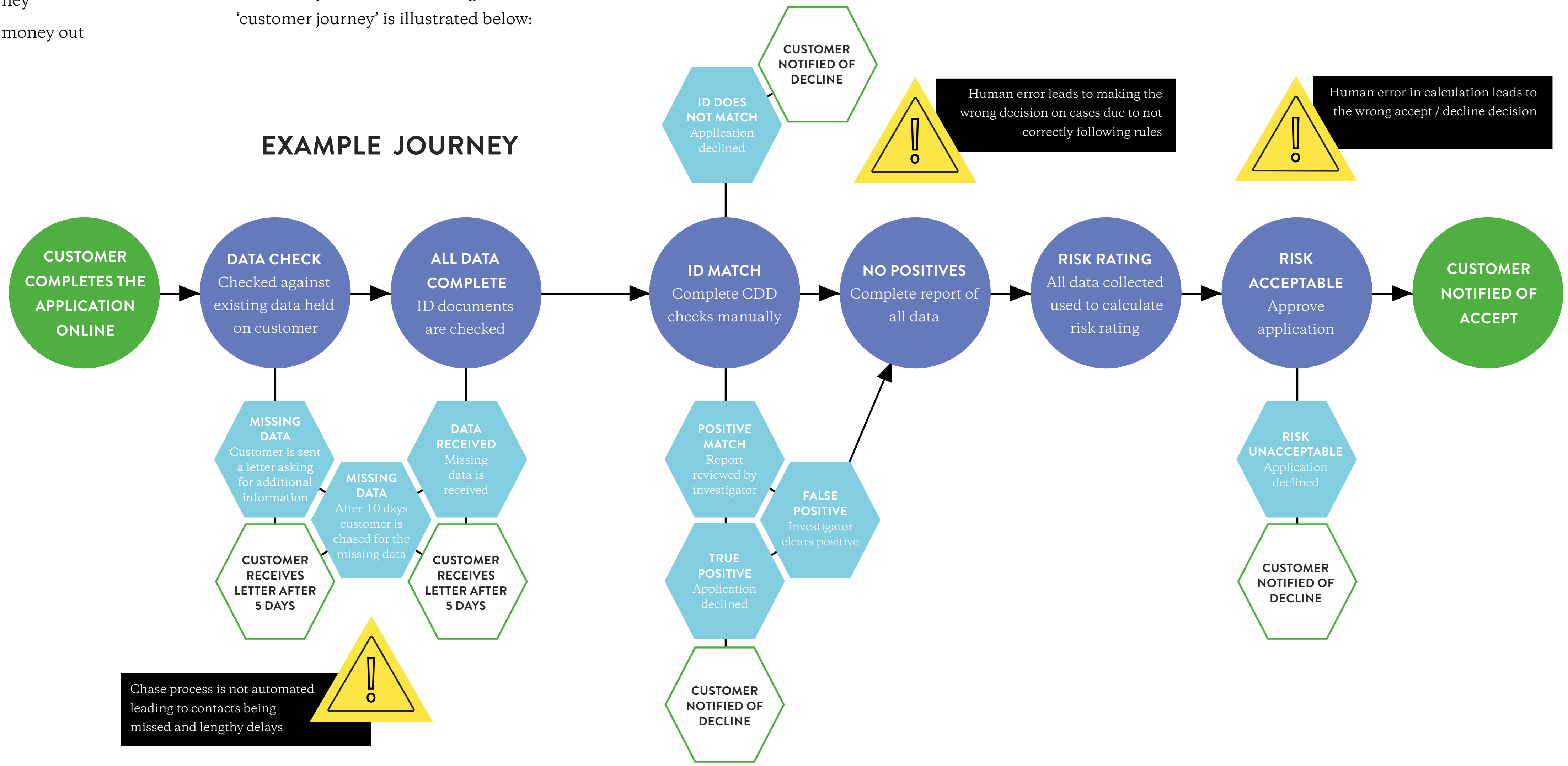
- Customer journey
- Supplier journey
- Employee journey
- Advice journey
- Money in / money out

Respondents who provided the most complete insights into their own firm's risks and controls were those who identified the business processes they protect and were able to describe the points along the process at which the firm applies specific controls to protect the activity.

One example of an onboarding 'customer journey' is illustrated below:

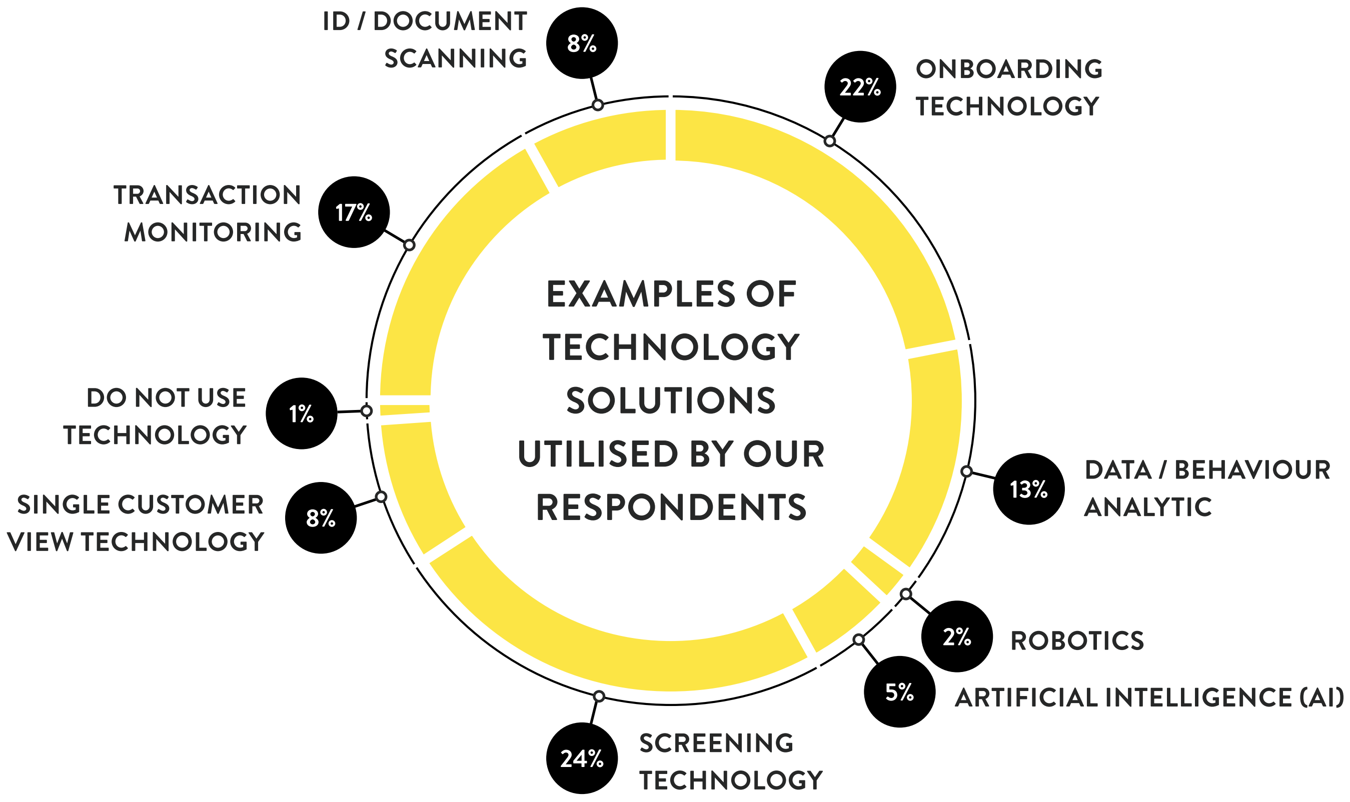
This customer journey shows that a customer will interact with a firm at several different points where, at each, the firm could apply efficient controls to assist the transition through that point. By being aware of the entire customer journey, the fraud leader is equipped to ensure that controls are applied at the most effective point, that their application supports the customer's transition through that point and that people and technology solutions are effectively utilised.

EXAMPLE JOURNEY


CUSTOMER COMPLETES THE APPLICATION ONLINE
DATA CHECK Checked against existing data held on customer
MISSING DATA Customer is sent a letter asking for additional information
MISSING DATA After 10 days customer is chased for the missing data
CUSTOMER RECEIVES LETTER AFTER 5 DAYS
Chase process is not automated leading to contacts being missed and lengthy delays
ALL DATA COMPLETE ID documents are checked
DATA RECEIVED Missing data is received
CUSTOMER RECEIVES LETTER AFTER 5 DAYS
ID MATCH Complete CDD checks manually
ID DOES NOT MATCH Application declined
CUSTOMER NOTIFIED OF DECLINE
Human error leads to making the wrong decision on cases due to not correctly following rules
POSITIVE MATCH Report reviewed by investigator
FALSE POSITIVE Investigator clears positive
TRUE POSITIVE Application declined
CUSTOMER NOTIFIED OF DECLINE
NO POSITIVES Complete report of all data
RISK RATING All data collected used to calculate risk rating
RISK ACCEPTABLE Approve application
Human error in calculation leads to the wrong accept / decline decision
RISK UNACCEPTABLE Application declined
CUSTOMER NOTIFIED OF DECLINE
CUSTOMER NOTIFIED OF ACCEPT

TECHNOLOGY

Technology provides firms with significant challenges as they each strive to protect their firms from the risks associated with increased technology integration, whilst also seeking to exploit the benefits that technology can bring. Whilst some respondent firms feel committed to existing technology, and so are investing in its maintenance, others are more prepared to change suppliers to access improved solutions. Some examples of technology solutions utilised by our respondents include:



Fraud leaders should be challenging their existing technology models to identify more effective solutions. Those who do, will quickly adopt technology gains, deliver improved customer experience and strengthen controls, all at a reduced cost. From the responses we received, several firms are at the early stages of developing RPA solutions to achieve these benefits, although people do continue to feature in those models to perform the more subjective challenging tasks, rather than complete repetitive checks.

Firms that adopted process led control models, as opposed to fraud typology models, were observed to be more effective at identifying technology benefits and improvements, and at embedding them into their process. For example, an insurer that can accurately risk rate a customer at the outset of the customer relationship, ensures that pricing has improved accuracy and claims settlement is managed in accordance with the customer's risk profile (i.e. efficient process).

> TECHNOLOGY IS EMBEDDED IN EVERYTHING WE DO. IN MANY WAYS FINANCIAL SERVICES FIRMS ARE BECOMING TECHNOLOGY COMPANIES. OUR FRAUD STRATEGY IS DEVELOPING IN THE SENSE THAT WE WANT TO DO MORE BY UNDERSTANDING THE TECHNOLOGY AND INFORMATION TECHNOLOGY AVAILABLE ON THE MARKET TO KEEP AHEAD
>
> BOARD MEMBER, GLOBAL INVESTMENT BANK

CONCLUSION

FRAUD IS EVER CHANGING AND THIS RESEARCH HIGHLIGHTS THAT FIRMS ARE FINDING IT CHALLENGING TO EFFECTIVELY MANAGE THE SEVEN CORE RISKS IDENTIFIED. EACH SECTOR PRIORITISED FRAUD RISKS DIFFERENTLY, WITH NO ONE RISK RECOGNISED AS THE CORE CONCERN.

This research also demonstrates, that firms are not confident that they are adequately managing fraud risks. We have outlined the following as key good-practice firms can employ, to reduce their exposure to fraud:

Commitment at board level to an anti-fraud culture with the visibility, investment and senior manager accountability necessary to deliver this

Clear end-to-end processes mapped out with effective controls in place

Robust management information which provides a single-view of fraud risks across the business

Ongoing risk assessments based on the right mix of data sources and benchmarked against peers

Efficient and robust onboarding checks for customers, employees and third parties backed up by risk-based activity monitoring throughout the relationship

Secure data management for both internal and customer data, using a big data approach to analysing customer level information and behaviours. This will help to identify trends and enhance identification and control of fraud

An effective training an education programme for both employees and customers to raise awareness of ways people can protect themselves, and their employer, from fraudulent activity

The benefits of successfully managing fraud risks are significant and varied - from a reduction in financial losses, to increased reputation and customer advocacy. Data sharing within industries is a major challenge which needs to be addressed, however, where industries work together to tackle fraud in a coordinated way, they can deter attacks as it becomes increasingly challenging to prosper from dishonest conduct.

The research has identified that there is still work to be done across financial services and utilities, in more effectively mitigating fraud risks to protect both customers and businesses, however there are clear steps that can be taken to move in the right direction.

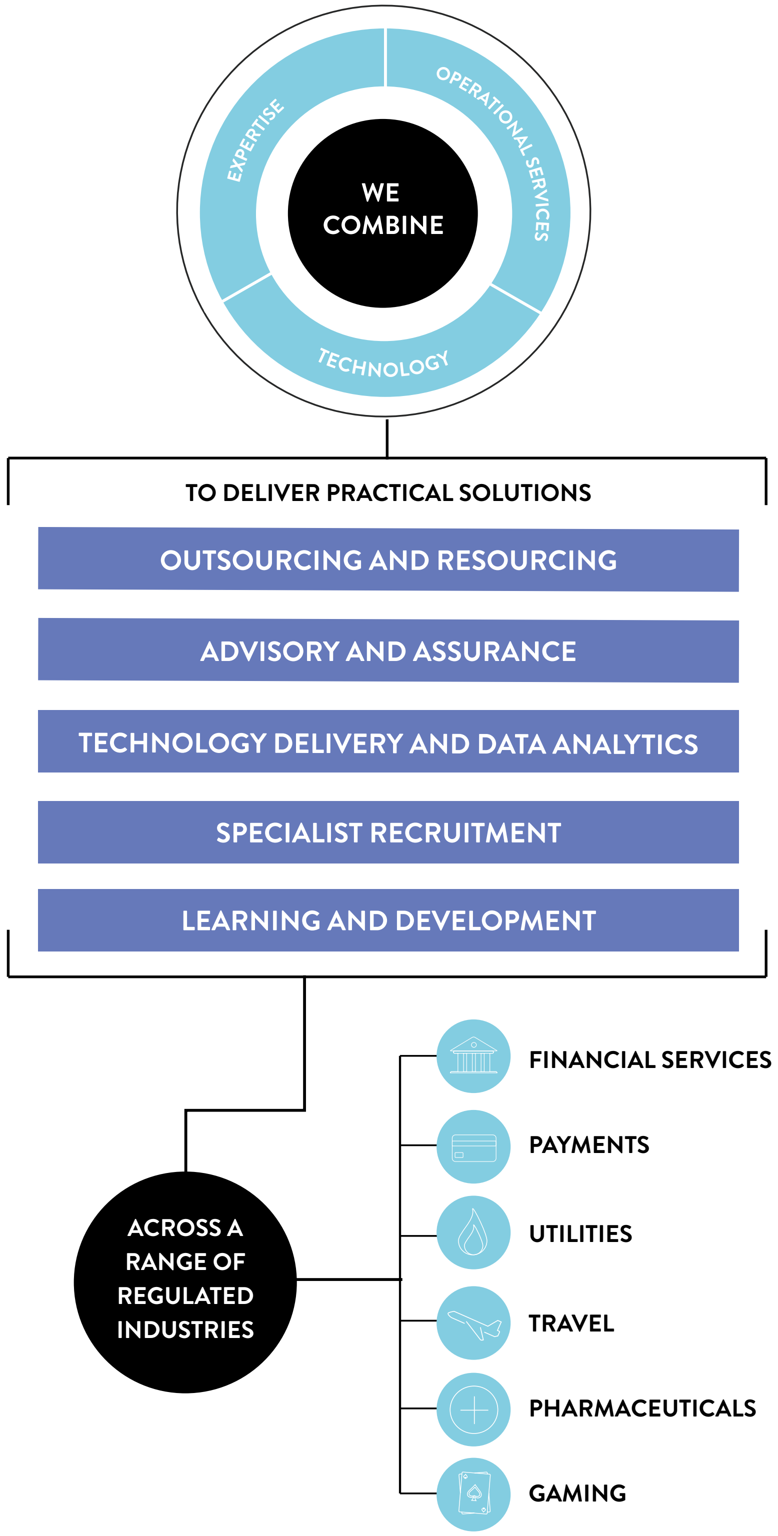
HOW HUNTSWOOD CAN HELP

HUNTSWOOD'S AIM IS TO DRIVE BETTER OUTCOMES - FOR OUR CLIENTS AND THEIR CUSTOMERS.

We achieve this by combining expertise, technology and operational services to deliver practical solutions that help regulated firms deliver high quality services in a cost efficient way, while effectively mitigating business risk:

- Outsourcing and resourcing
- Advisory and assurance
- Technology delivery and data analytics
- Specialist recruitment
- Learning and development

We support clients across a range of regulated industries: financial services, payments, utilities, travel, pharmaceuticals and gaming.



WE COMBINE

EXPERTISE

OPERATIONAL SERVICES

TECHNOLOGY

TO DELIVER PRACTICAL SOLUTIONS

OUTSOURCING AND RESOURCING

ADVISORY AND ASSURANCE

TECHNOLOGY DELIVERY AND DATA ANALYTICS

SPECIALIST RECRUITMENT

LEARNING AND DEVELOPMENT

ACROSS A RANGE OF REGULATED INDUSTRIES

FINANCIAL SERVICES

PAYMENTS

UTILITIES

TRAVEL

PHARMACEUTICALS

GAMING

WE HELP FIRMS TAKE A HOLISTIC APPROACH BY DELIVERING TAILORED SOLUTIONS THAT ENSURE RISKS ARE MANAGED EFFECTIVELY AND EFFICIENTLY.

OUTSOURCING AND RESOURCING

We deliver the experienced resource needed to carry out fraud investigations on either a batch or ongoing process with flexible options around location, management and activity.

ADVISORY AND ASSURANCE

Our experts are skilled in supporting the design, implementation and testing of risk sensitive controls and overlay industry experience of good-practice to propose practical recommendations tailored to the aims of the business.

TECHNOLOGY DELIVERY AND DATA ANALYTICS

Our intelligent work management system accesses multiple data sources using intelligent robotic automation to enable holistic review of customers and transactions. Machine learning enables processes to develop based on data to refine and enhance fraud identification.

SPECIALIST RECRUITMENT

We have a wide network of experienced and qualified financial crime professionals to support clients on a permanent or interim basis. We use our experience and market knowledge to present clients with candidates who offer a real fit for their business.

LEARNING AND DEVELOPMENT

We supporting employees with training on core skills in identifying fraud, understanding regulation and the importance of mitigating fraud risk.

BUSINESS BENEFITS

Increased efficiency and cost savings

Increased customer trust due to using an independent firm

Efficient alert investigations to ensure risk is mitigated whilst protecting customer experience

Evolution of fraud identification through data analytics, mitigating ever changing fraud activities

FINANCIAL CRIME AND PAYMENTS ADVISORY PANEL

Our Panel brings extensive, senior-level experience to support our financial crime and fraud team to deliver market-leading services to clients.

The panel's experience spans terrorist financing, fraud, investigations, bribery and corruption, anti-money laundering, cyber and payments. Their significant track records are drawn from a broad range of backgrounds, including policing (including the Metropolitan Police), the Financial Conduct Authority, the Bank of England, the Fraud Prosecution Service, litigation and technology.

They have been responsible for helping many organisations develop and embed best practice approaches to managing financial crime risk.

PHILIP KENWORTHY
Industry advisor and former Chief Executive and Non-Executive Director at CHAPS Clearing Company Ltd

ANDREW MCDONALD
Ex Head of Specialist Investigations and National Terrorist Financial Investigation Unit, Metropolitan Police

ANDREW CHURCHILL
Consultant & Researcher primarily on Defence & Security Technologies and Innovation

DAN CRISP
Current UK Finance Digital Innovation Director and Former Chief Technology Risk Officer, BNY Mellon

GLEN MARR
Former executive and senior manager in the insurance industry and director of the Insurance Fraud Bureau

GRAHAM HOOPER
Former Director of Financial Crime Risk at Lloyds Banking Group

For full biographies visit www.huntswood.com/fcap
or contact us on 0333 321 7815.

CONTACT US

FINANCIAL CRIME AND FRAUD TEAM

STEVE ELLIOT
MANAGING DIRECTOR
FINANCIAL CRIME, FRAUD,
INFORMATION SECURITY AND PAYMENTS

e selliot@huntswood.com
t 0118 971 8546

LINGLIN SONG
PRINCIPAL CONSULTANT
FINANCIAL CRIME AND FRAUD

e lsong@huntswood.com
t 0118 971 8227

BOCHRA EL MAY
SENIOR CONSULTANT
FINANCIAL CRIME AND FRAUD

e belmay@huntswood.com
t 0333 321 7815

DAVID DAWSON
SENIOR CONSULTANT
FINANCIAL CRIME AND FRAUD

e ddawson@huntswood.com
t 0118 971 8396

MARK TOWNSLEY
FINANCIAL CRIME REGULATORY
AFFAIRS MANAGER

e mtownsley@huntswood.com
t 0118 971 8105

BRIONY RIPPINGTON-BOND
CONSULTANT
FINANCIAL CRIME AND FRAUD

e bcrewe@huntswood.com
t 0118 971 8593

CLIENT PARTNER TEAM

LUKE WOOTTON
HEAD OF BUSINESS DEVELOPMENT
PENSIONS, INVESTMENTS AND WEALTH MANAGEMENT

e lwootton@huntswood.com
t 0118 971 8285

STEVE HIGGS
BANKS AND BUILDING SOCIETIES

e shiggs@huntswood.com
t 0118 971 8141

ALEX PRENTICE
UTILITIES

e aprentice@huntswood.com
t 0118 971 8322

SEAN KULAN
CONSUMER CREDIT

e skulan@huntswood.com
t 0118 971 8284

NIKKI CEKO
GENERAL INSURANCE

e nceko@huntswood.com
t 0118 971 8263

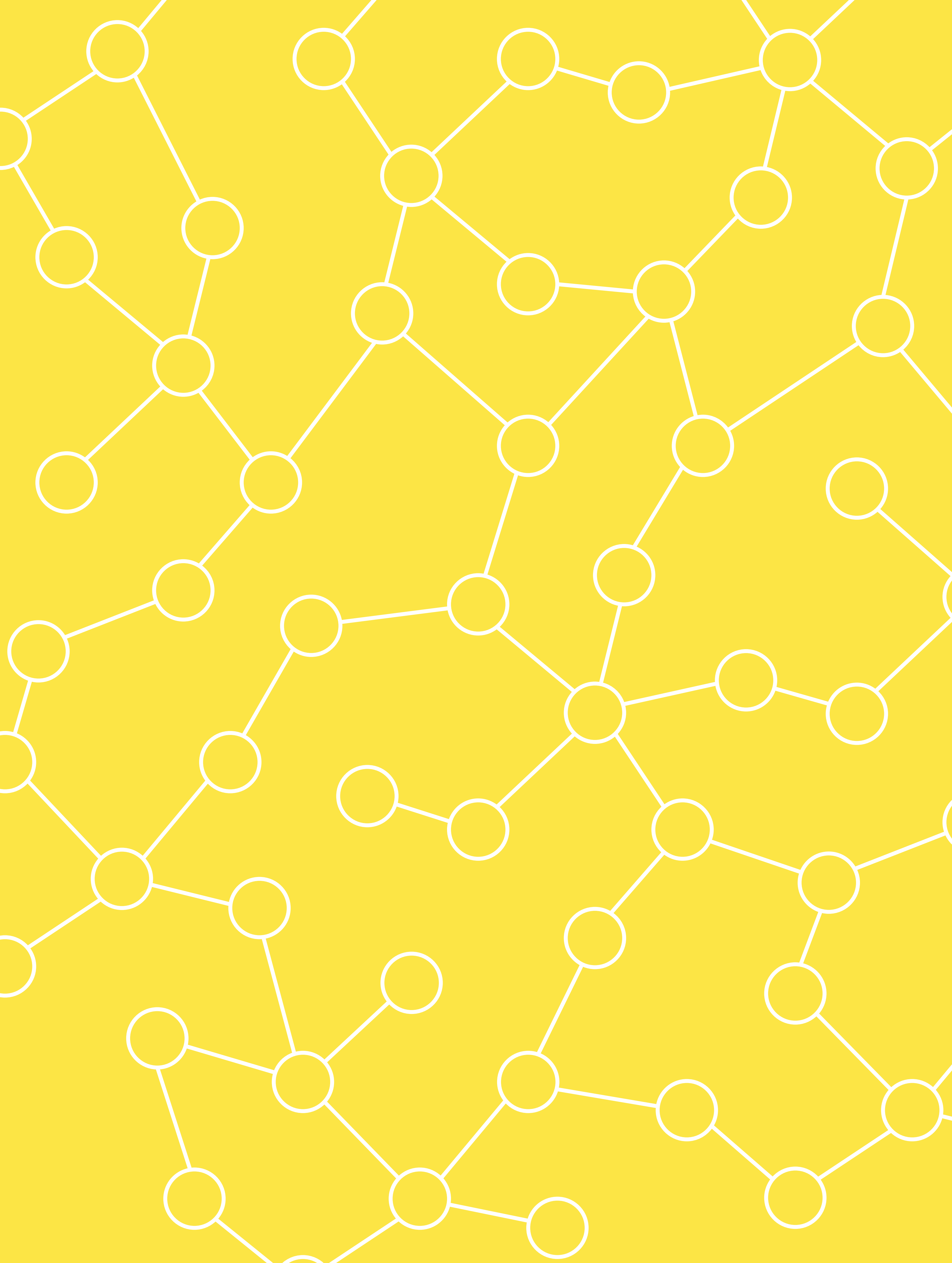
TOM GOODEY
GENERAL INSURANCE

e tgoodey@huntswood.com
t 0118 971 8175

CHARLIE ROBSON
BANKS AND BUILDING SOCIETIES

e crobson@huntswood.com
t 0118 971 8596

WWW.HUNTSWOOD.COM



HUNTSWOOD

Huntswood CTC Limited
Abbey Gardens, Abbey Street,
Reading, Berkshire RG1 3BA
0333 321 7811
enquiries@huntswood.com
huntswood.com

@Huntswood
in Search ‘Huntswood’

NOTES RELATING TO HUNTSWOOD