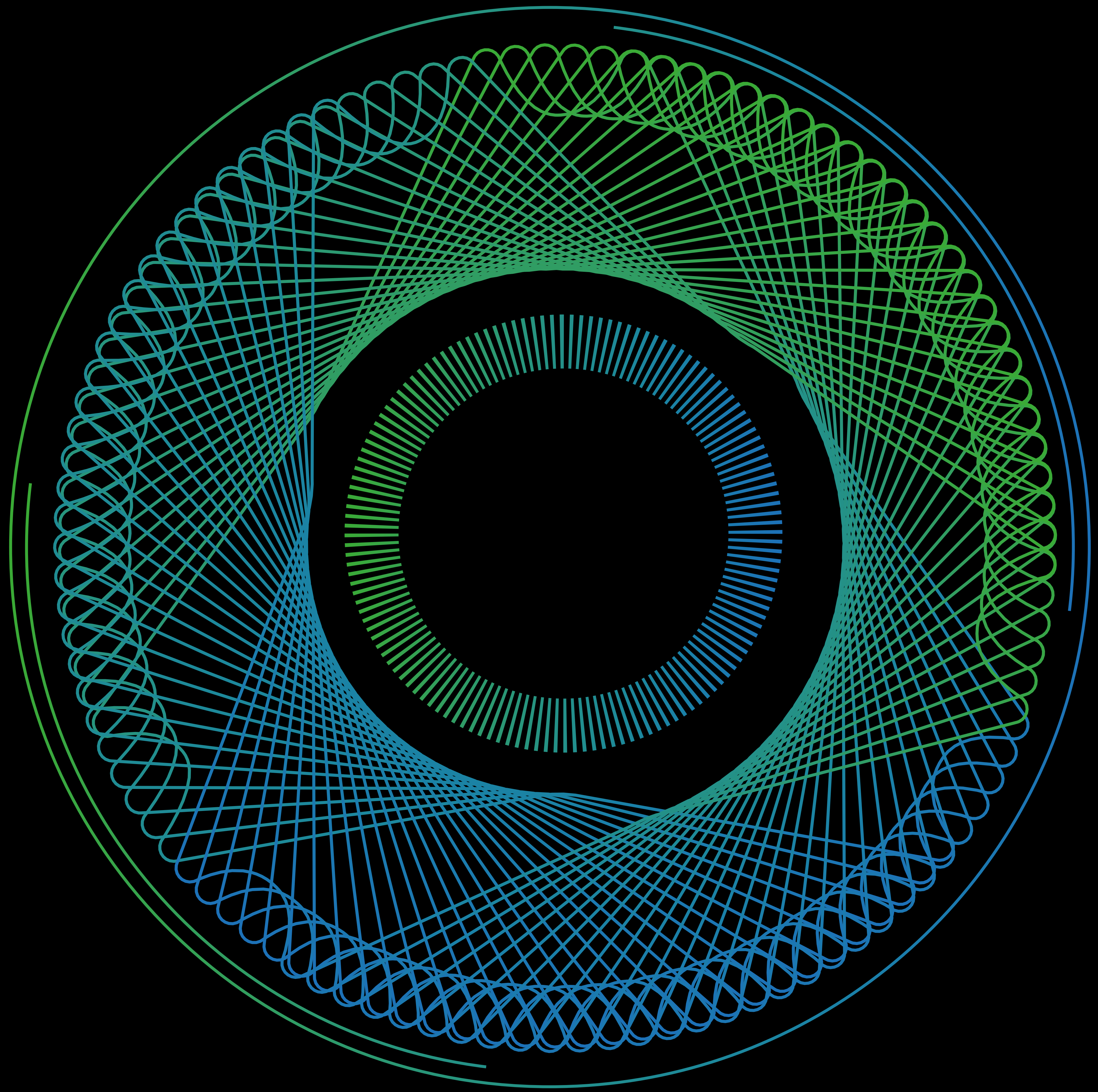
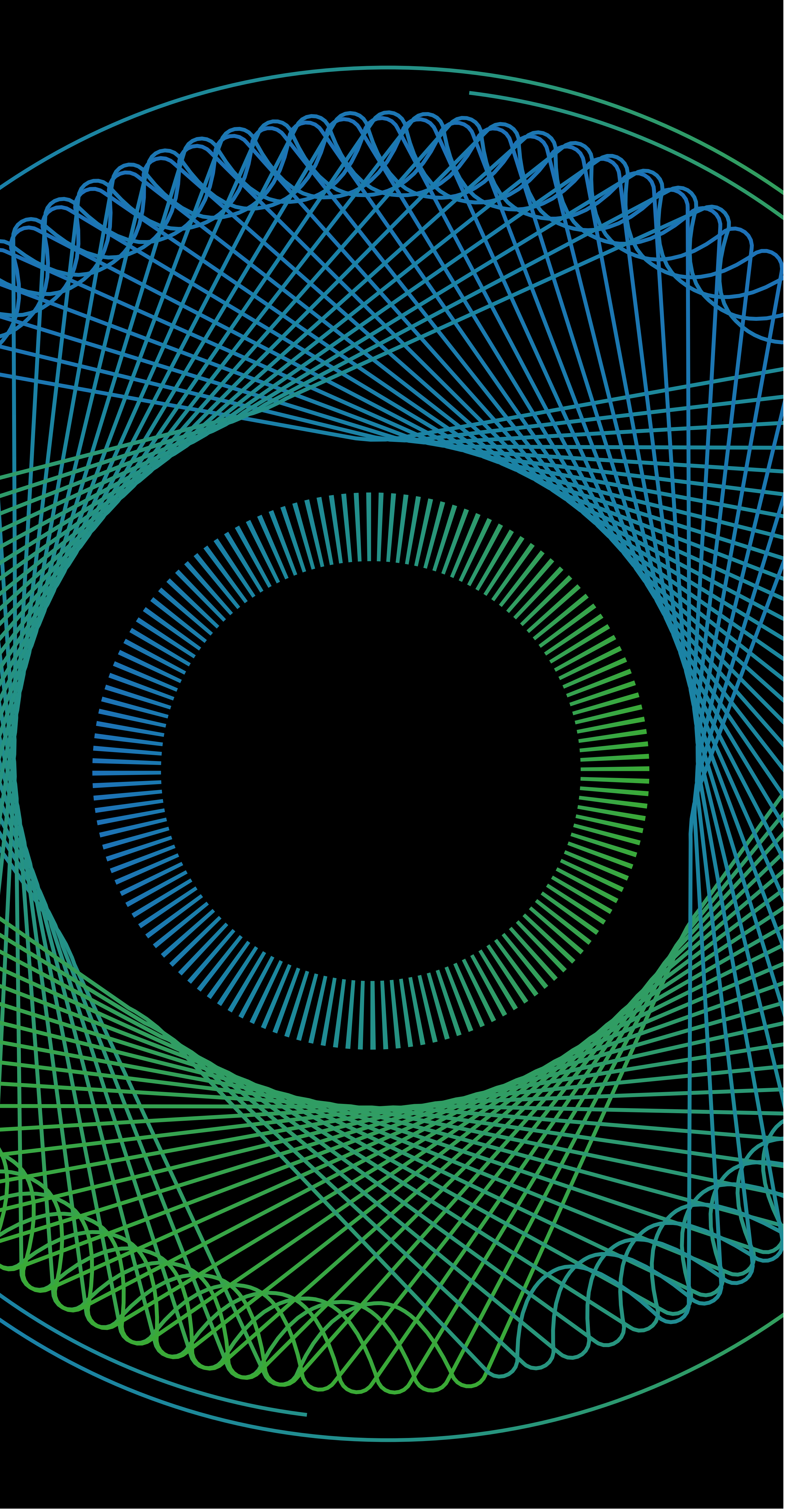
Deloitte.



Resetting the dial

Transforming the fraud reporting and response ecosystem



Contents

1. Introduction

Fraud impacts every corner of society, causing financial and emotional harm to people, communities and businesses. From investment and romance fraud, to identity theft and counterfeit goods, the criminals take whatever shape they need to, constantly morphing and evolving to exploit unwary victims. Fraud now accounts for about 40 per cent of all recorded crime, with an annual estimated cost to the UK economy of £130 billion.[1] However, only 1 per cent[2] of reported cases end in a judicial outcome. And around 85 per cent of incidents go unreported due to embarrassment, failure to recognise that a crime has occurred, and confusion over how and where to report.[3] It is far from being a victimless crime. Victims report experiencing anxiety and stress, sleeping problems and thoughts of self-harm.

In July 2021, the City of London Police announced the development of a new national fraud and cyber-reporting centre. This was a welcome and timely move, for three reasons.

First, it represents an opportunity to transform the way fraud is reported. Second, it should allow the entire ecosystem in the UK and beyond to more effectively prevent, disrupt and detect fraud, at a time when it's increasing in both volume and complexity. Finally, it provides an opportunity to address previous criticisms and take steps to build public trust and confidence.

In this report we will explore the options to transform the existing UK fraud reporting and response ecosystem we now have – to improve Action Fraud as the existing reporting centre and enhance the National Fraud Intelligence Bureau (NFIB).

To support our understanding, we commissioned a survey from Ipsos[4] to reveal the real experiences of fraud among the UK adult population. This survey dispels the notion that fraud is a victimless crime. Seventy-one per cent of those surveyed had been a victim of fraud, with 59 per cent suffering emotional harm.

Some options may well be aspirational and dependent on legislative enablers. Some will require a cultural shift. But to make a difference we must be ambitious and bold. The entire ecosystem must seize this chance to work together and shape a fraud and cyber-reporting and response centre that builds on current foundations, and creates a service that places victims at its heart.

Clearly, it will require an ecosystem that is agile, intuitive and maximises each partner's collective knowledge to prevent and detect fraud and cybercrime.

What follows sets out the context, issues and, where appropriate, offers our perspective, concluding with a proposal for a radical revamp of the ecosystem.

Today's fraud landscape

Fraud has become a high priority for the Home Secretary, with several measures underway to tackle the issue. There is the development of a new Fraud Action Plan; the relaunch of the Ministerial-led Joint Fraud Taskforce; and the publication of sector-based fraud charters.[5]

The legislative landscape is changing too, with the Online Safety Bill, Economic Crime Bill, and consideration being given to future regulation for organisations. The latter follows a consultation by the Department for Business, Education, Innovation and Skills on 'Restoring Trust in Audit and Corporate Governance' and the Law Commission's discussion paper on corporate criminal liability.

The National Fraud Intelligence Bureau (NFIB) is responsible for the assessment of all fraud and cybercrime reports, disseminating them to local police forces for investigation. They regularly produce strategic threat assessments which they share with law enforcement and private industry, alerting them to new methodologies and trends, and empowering them to take preventative action. This information is used to inform the public of the latest threats and appropriate actions they can take to protect themselves.

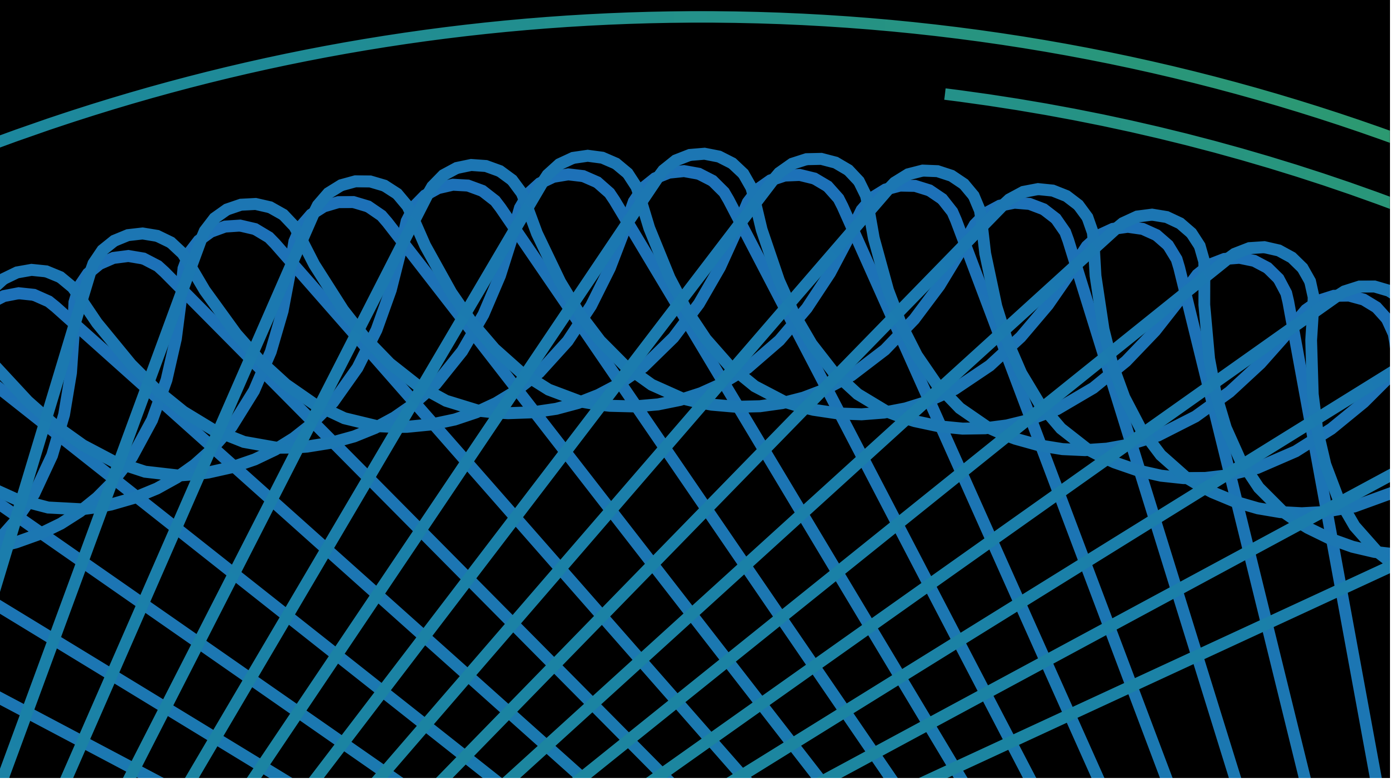
Although there is considerable room for improvement in the UK's counter-fraud landscape, there are things to be proud of too.

> ***"The UK is one of the only countries in the world to have a central fraud and cyber-reporting centre."***

And in 2020/21, Action Fraud recorded over 400,000[6] fraud and cybercrime reports (via phone, web chat and online), providing a platform to issue prevention advice and send out regular alerts to help keep the public safe from fraud.

1. ONS stats 2020/21 – Overview of fraud statistics – Office for National Statistics (ons.gov.uk) **2.** Graeme Biggar, Director-General of the UK's National Economic Crime Centre: "There is not a sufficient deterrent for fraudsters and there is insufficient recourse for victims" | REDD-Monitor
3. Nature of fraud and computer misuse in England and Wales – Office for National Statistics (ons.gov.uk) **4.** Ipsos interviewed a representative sample of UK adults aged 16-75. **5.** Home Office announcement 21/10/21 – www.gov.uk/government/news/joint-taskforce-relaunched-to-protect-against-rise-in-fraud-crime.
6. Action Fraud fraud assessment – 2020-21-Annual-Assessment-Fraud-Crime-Trends.pdf (actionfraud.police.uk)

> *Fraud accounts for about 40 per cent of all recorded crime, with an annual estimated cost to the UK economy of £130 billion."*



2. The Challenge

The scale of the problem is daunting. Fraud and cybercrimes continue to rise year on year. Fraud accounts for about 40 per cent of all recorded crime, with an annual estimated cost to the UK economy of £130 billion. The Office of National Statistics (ONS) reports that in the year 2020/21 there were 837,104 recorded offences of fraud and cybercrime — an increase of around 62,000.[7] These figures are powerful, but we also know fraud and cybercrimes are significantly under-reported – possibly by as much as 85 per cent.[8]

The stark reality is that our research found 71 per cent of respondents reporting that they had been a victim of fraud in the last 10 years, with over four in ten (44 per cent) reporting they had received an email, text message or telephone call that turned out to be a scam or fraud.

Estimated total annual fraud
5,800,000[i]

Recorded annual fraud
835,000[ii]

Referred fraud
38,000[iii]

Judicial outcomes
6,300[iv]

i Based on an estimated 85% of fraud being unreported.
ii Per 2020/21 'Fraud Crime Trends', Action Fraud.
iii https://www.actionfraud.police.uk/data
iv https://www.actionfraud.police.uk/data

Only 58,000[9] of fraud crimes are classified as 'cyber-dependent'. This is when a digital system is both the target and means of attack. It includes attacks on computer systems to disrupt IT infrastructure and stealing data over a network using malware. These crimes can range from a sophisticated criminal hack or coordinated Denial of Service (DNS), to social engineering that leads to the disclosure of passwords or bank details.

In addition, approximately 80 per cent of all fraud is now committed online. Unlike cyber-dependent crimes, a cyber-enabled crime may be any one where a computer is used to commit the offence.[10]

Fraud crimes range in complexity and harm. A targeted investment fraud can lead to complete devastation for the victim, with life savings and their sense of security irrevocably lost. In a romance fraud, the perpetrator seeks to bleed the victim dry, an act that inevitably impacts on the victim's emotional well-being. For the purposes of this report, we use the term 'fraud' to cover all forms fraud.

In the National Crime Agency's recent National Strategic Threat Assessment of Serious and Organised Crime[11], it was recognised that fraud and cybercrime is under-represented in terms of threat, scale and knowledge of the number of offenders. It is strongly suspected that Serious and Organised Crime (SOC) groups have diversified into the fraud and cybercrime arena for a simple reason: low risk, high reward.

The Royal United Services Institute, a leading defence and security think-tank, recently made clear that SOC groups are active in the fraud and cybercrime space. In their paper *The Silent Threat – The Impact of Fraud on UK National Security*,[12] they suggest that fraud has reached epidemic levels and, as the volume-crime of our time, should be treated as a threat to National Security.

7. ONS reports 2020/21 Overview of fraud statistics – Office for National Statistics (ons.gov.uk) **8.** Nature of fraud and computer misuse in England and Wales – Office for National Statistics (ons.gov.uk) **9.** Action Fraud fraud assessment – 2020-21-Annual-Assessment-Fraud-Crime-Trends.pdf (actionfraud.police.uk) **10.** Action Fraud fraud assessment – 2020-21-Annual-Assessment-Fraud-Crime-Trends.pdf (actionfraud.police.uk) **11.** NCA National Strategic Assessment 2021 – https://www.nationalcrimeagency.gov.uk/who-we-are/publications/533-national-strategic-assessment-of-serious-and-organised-crime-2021/file **12.** The Silent Threat – The Impact of Fraud on UK National Security 26/01/21 – rusi.org/exploreour-research/publications/occasional-papers/silent-threat-impact-fraud-uk-national-security/

2.1 The policing response

Despite the exponential growth of fraud and cyber offences, policing resources to address the threat have not increased. It has been estimated that just one per cent[13] of police budgets are dedicated to fraud. This does not tell the whole story though, with front line officers and staff nationwide responding daily to calls from people reporting fraud — often referred to as a 'call for service'.

Each policing region has a dedicated Regional Economic Crime Unit (RECU) that forms part of the wider Regional Organised Crime Unit, yet it is clear fraud is not seen as a policing priority. With finite resources, the police must prioritise based on the threat, risk, and harm to the public. On many occasions, officers and staff dedicated to investigating fraud are redeployed to support other priorities.

In 2019, Her Majesty's Inspectorate of Constabulary and Fire and Rescue Service (HMICFRS) conducted a review into how policing dealt with fraud. The report, *Fraud, time to choose,*[14] recognised the challenge of competing policing priorities and quotes one officer who pertinently points out that "*fraud does not bang, bleed, or shout*". Yet it quietly does so much harm. The report went on to say, "*Leaders in government and police forces can either continue to respond to fraud in an inconsistent manner, often leaving victims confused and disillusioned, or they can act to ensure that there is a clearer strategy, less variation in service between forces and better communication with the public*".

The decision on whether a fraud is investigated is made by local police forces with increasingly stretched resources and budgets leading to an inconsistent approach and low prosecution rates. Through the NFIB, the City of London Police assesses the reports from Action Fraud and prepares investigation packages for police forces across the UK.

On receipt of an investigation package, the relevant police force undertakes its own screening process before allocating it to an investigator. On occasion, it is unclear who should take primacy for an investigation, and this is often due to interpretation of the Home Office Counting Rules (HOCR).[15]

These are a guide for the allocation of crimes, with an emphasis on where the suspect resides or has been residing. This is not always clear and a link may be as tenuous as a money movement through a local bank. It is understandable, therefore, that a police force may be reluctant to allocate resources to an investigation that does not directly impact on its local community.

In 2020/21 there were only 6,300 fraud judicial outcomes, equating to less than one per cent of reported fraud.[16] That said, these figures do not take into account where a fraud investigation has led to a non-fraud related judicial outcome, such as money laundering, theft or offences under the Identity Cards Act. Cases where police have decided to target and disrupt an offender through other methods rather than undertaking a fraud investigation are not accounted for in these figures.

Perspective

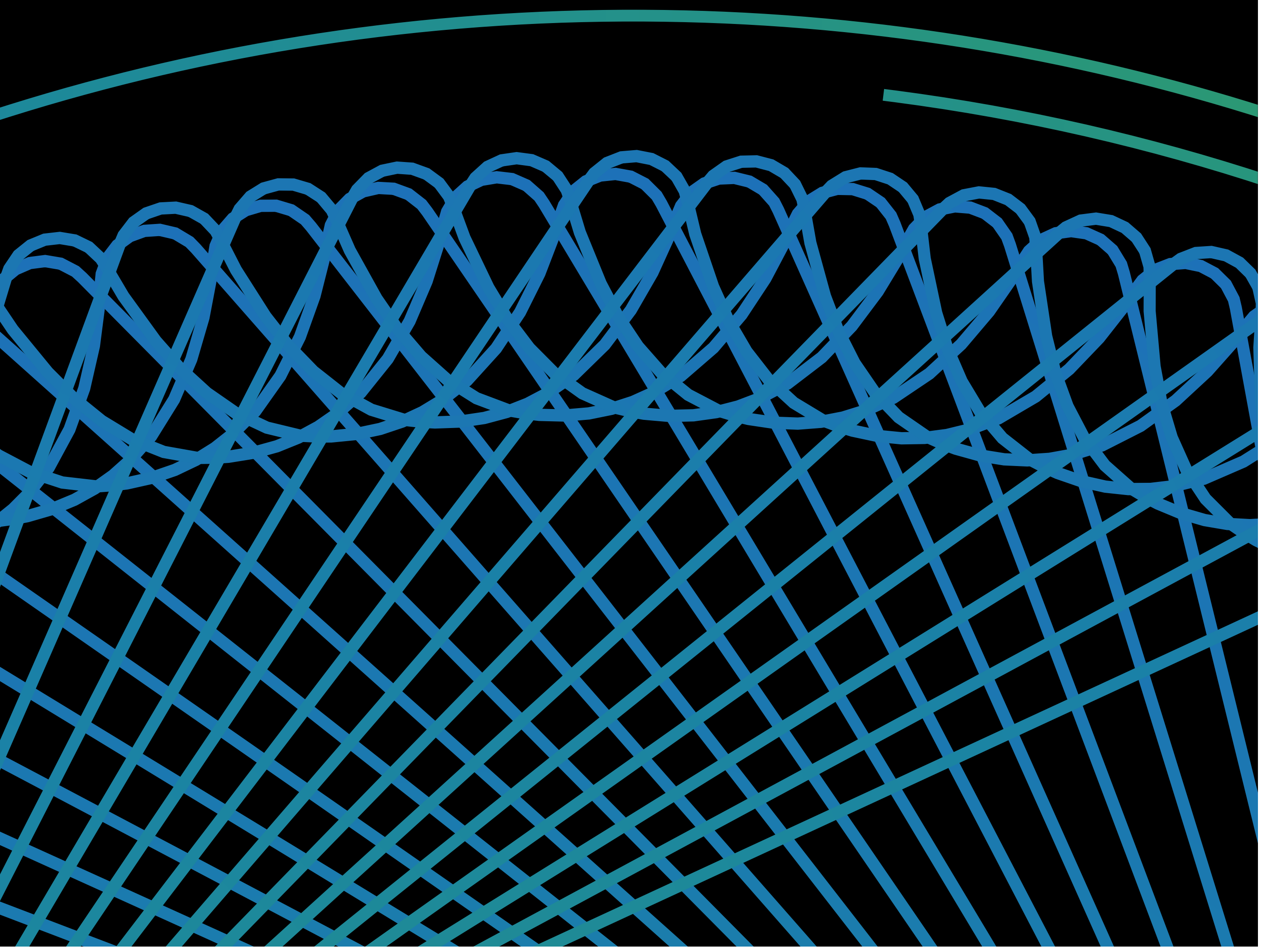
> **"*It's time to consider combining all available fraud and cybercrime resources under one agency."***

An agency is needed that will prioritise investigation and disruption against those causing the greatest threat to individuals, businesses, and government. So far, there has not been sufficient appetite for such a transformational change — but now is the moment to think and act differently.

If there is not an appetite for a single agency, there needs to be a discussion about the development of a centrally coordinated and funded local delivery model for fraud and cyber. One that uses current counter terrorism policing as a model of good practice. This would ensure that the highest harm threats are addressed as a priority and staffing is accordingly ring-fenced.

[13] Graeme Biggar, Director-General of the UK's National Economic Crime Centre: "There is not a sufficient deterrent for fraudsters and there is insufficient recourse for victims" | REDD-Monitor [14] Her Majesty's Inspectorate of Constabulary and Fire and Rescue Service (HMICFRS), 2019, Fraud: Time to Choose: An inspection of the police response to fraud (justiceinspectorates.gov.uk) [15] Home Office Counting Rules fraud – Counting rules for fraud (publishing.service.gov.uk) [16] Fraud and cybercrime national statistics – https://www.actionfraud.police.uk/data

> *“The longer we delay, the easier it becomes for the criminals to operate.”*



2.2 Information sharing

The proactive sharing of information and intelligence is critical but currently it lacks a consistent approach. There is an appetite across many private sector organisations to share but often this is one way, with reluctance from law enforcement to provide feedback or to proactively share.

Currently organisations can utilise the ‘legitimate interest’ provision under the Data Protection Act to share information and intelligence. This is used to great effect by Cifas, a not-for-profit service that works to prevent fraud, enabling their members to share fraud data and prevent further crimes.

Cifas is one of six specified, anti-fraud organisations enacted by section 68 of the Serious Crime Act 2007. This enables public authorities, for purposes of fraud prevention, to disclose information to a member of a specified anti-fraud organisation.

There are limited exchanges of actionable intelligence between public and private sectors. However, a good example of this working effectively is the Joint Money Laundering and Intelligence Taskforce (JMLIT) part of the National Economic Crime Centre . The taskforce consists of over 40 financial institutions, the Financial Conduct Authority, Cifas and five law-enforcement agencies: the NCA, HMRC, the SFO, the City of London Police, and the Metropolitan Police Service. It is considered internationally to be an example of best practice.

Perspective

We need to build and broaden the scope of the good practice in place with JMLIT, by including key sectors such as telecommunications, social media, and energy companies in this, whilst increasing inputs from the public sector, particularly HMRC and Companies House. One idea is to develop several industry hubs to share real-time fraud and cyber intelligence, whilst having a two-way flow of information to the NFIB.

We do not underestimate the challenge this presents. Under existing legislation, legal teams are often reluctant to share data outside specific scenarios. This current impasse cannot continue. The longer we delay, the easier it becomes for the criminals to operate. We must enable two-way intelligence sharing, either by providing up-to-date guidance that empowers organisations to share under existing legislation, or by expediting new legislation to encourage proactive information sharing.

To achieve this vision, a corresponding technology solution that enables the security, storing and analysis of high volumes of data, and the identification and prioritising of the service to vulnerable victims is needed. This would deliver a real-time, two-way flow of intelligence that enables disruption and prevention opportunities to multiple partners. It would also recognise new methodologies and trends not visible to the naked eye, and the identification and prioritisation of high-harm offenders for allocation to law enforcement for investigation.

Above all, by taking every opportunity to share information and intelligence, we will help individuals, businesses, and law enforcement to do their job more effectively.

2.3 Culture

The last and potentially biggest challenge is the cultural change required. If we are not able as individuals, organisations, or sectors, to unite and address this critical threat to our economic well-being, then we are giving the fraud and cyber criminals free rein to exploit our future prosperity. There is insufficient understanding of the impact of fraud on victims, their families and sometimes communities. Too often, stating that you are a victim of fraud is met with negativity thus creating a stigma. It can often be assessed as being a victimless crime. Our research shows that this is absolutely not the case.

Perspective

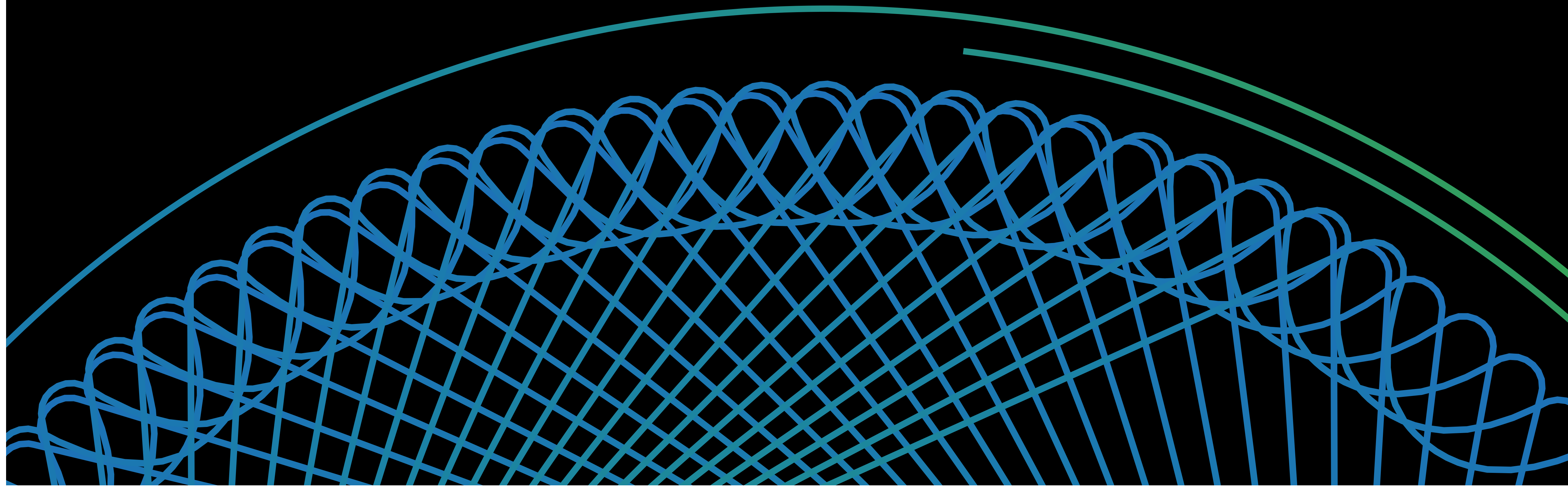
Police and crime agencies need to take a step back to realign risk appetites to address the current threat, and bring together their collective knowledge, expertise, information, and intelligence, to make the UK a truly hostile environment for these criminals.

Consideration should be given to rebranding Action Fraud. As our survey informs us, Action Fraud is not an established brand with victims remaining confused on where to report fraud and cyber-crimes. Furthermore, those who are aware of it, often perceive it negatively.

This rebranding should be completed when the new enhanced system is developed and delivering its core purpose.

As one fraud ecosystem, we must collaborate and deliver a hard-hitting public education drive, centred around simple, consistent messaging that truly resonates. It should help dispel the stigma of being a victim of fraud and promote awareness, so that together we can protect the many. It is recognised that such a campaign would naturally lead to increased reporting and consideration of this would be needed at the outset to prevent backlogs.

> “*Consideration should be given to rebranding Action Fraud once a new system is developed and delivering its core purpose.”*



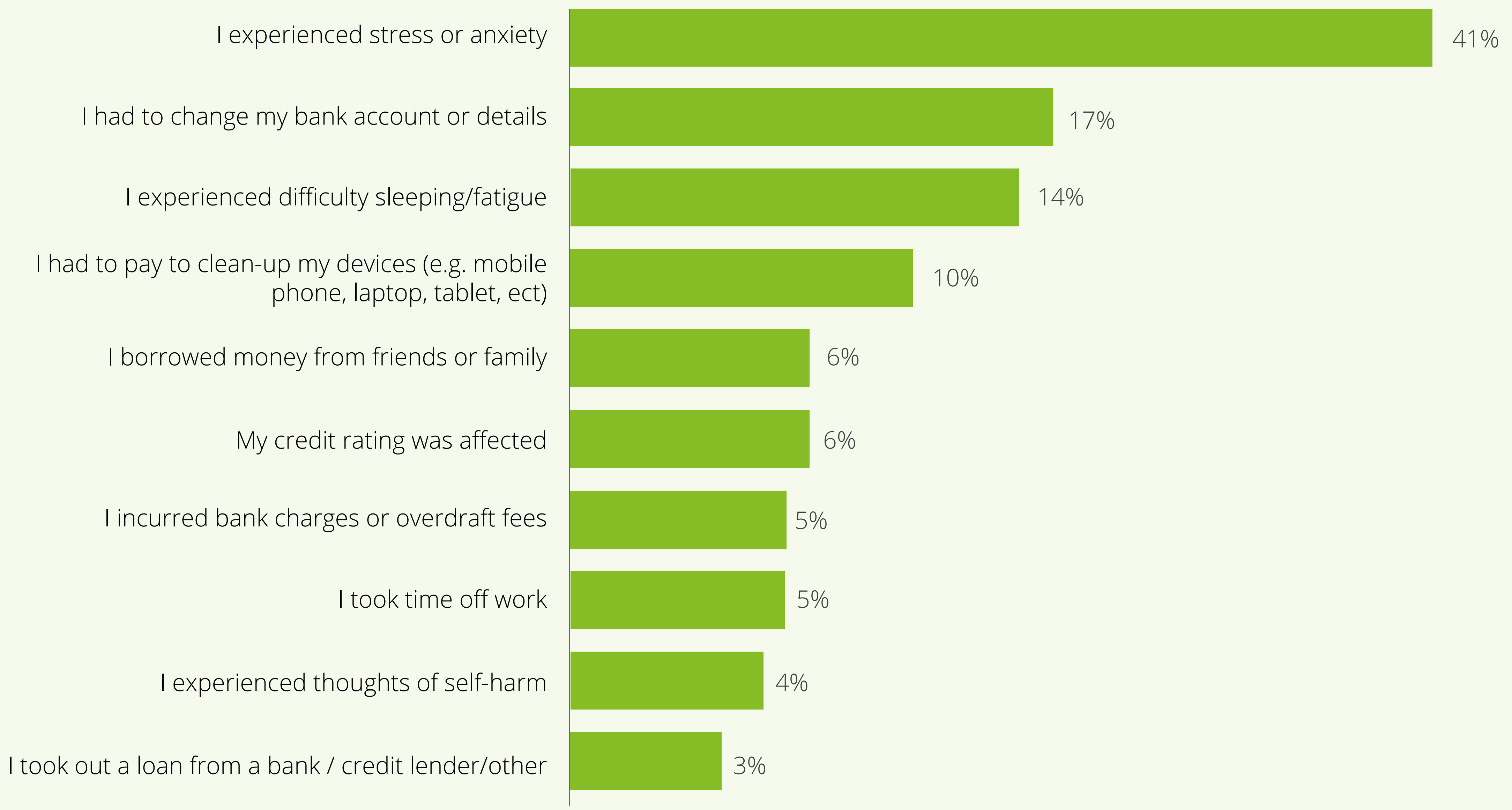
3. The victim experience

3.1 Impact of fraud

Fraud causes significant harm to individuals, their families, communities, and businesses, both financially and psychologically.

As part of our survey, we sought the views of victims on the impact of fraud. Forty-six per cent surveyed said they suffered emotional harm as a direct impact of fraud. Forty-one per cent said they had experienced stress or anxiety, 14 per cent suffered with sleep deprivation, and 4 per cent had thoughts of self-harm. Understandable when you consider the scale of financial loss experienced by some. Between August 2019 and August 2020, Action Fraud received more than 400 reports a month of romance fraud in the UK, with victims scammed out of an average of £10,000 each.[17]

Which, if any, of the following happened to you as a result of the fraud you experienced? (*top 10*)



Perspective

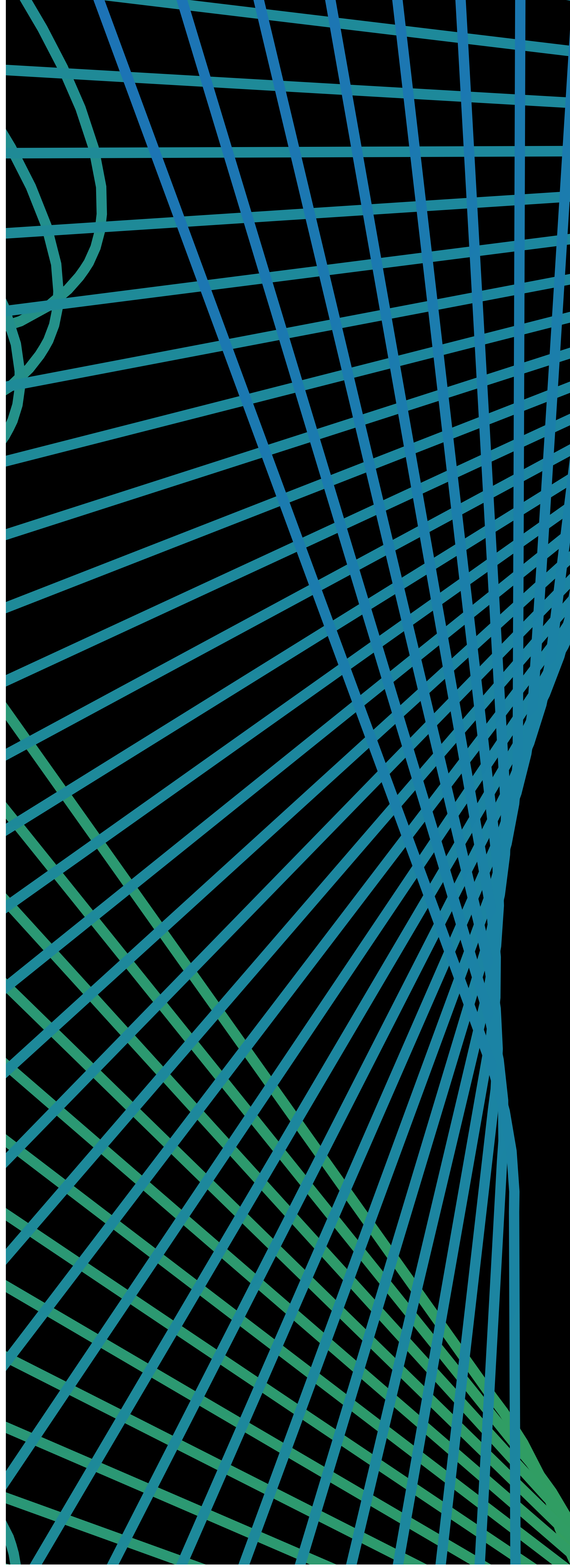
Victim well-being must be a priority and action is needed to improve confidence and satisfaction with the system. To do this we must first establish why up to 85 per cent[18] of fraud goes unreported and improve the service to victims. Crucially, it will encourage more to come forward.

We also need to enlist support from elsewhere in the ecosystem to make this happen. Support from third-sector partners in providing wraparound care for complex, vulnerable victims is a must. But how can financial institutions, social media organisations, technology and telecommunications companies contribute to creating a holistic response to victim care?

One priority should be to improve communication with the victim, whether an individual or a business. Providing them with feedback and regular updates sounds simple but is rarely achieved.

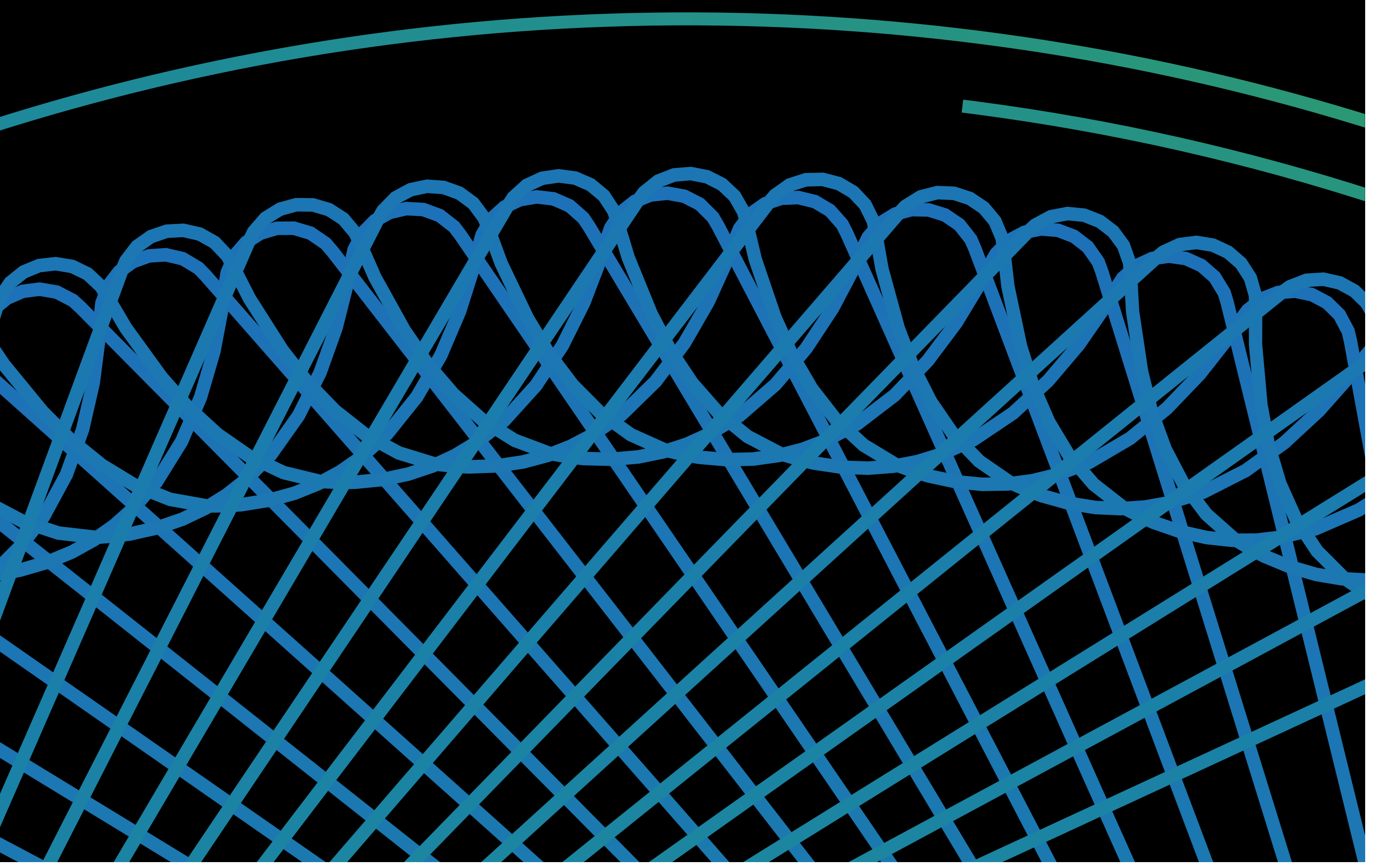
Similarly, organisations that share intelligence with the NFIB often receive no acknowledgement of receipt or its value to law enforcement. Inevitably, this disenfranchises and limits their willingness to share in the future.

There are some areas of good practice, with the City of London Police taking significant steps to improve the care given to vulnerable victims by introducing the National Economic Crime Victim Care Unit (NECVCU). Several police forces have also adopted the Operation Signature model that identifies and supports vulnerable victims of fraud. These good practices need to be replicated.



17. BBC news article – https://www.bbc.co.uk/news/uk-wales-54855321 **18.** Nature of fraud and computer misuse in England and Wales – Office for National Statistics (ons.gov.uk)

> *46 per cent of those surveyed did not know where or how to report a fraud or cybercrime."*



3.2 Reporting fraud

Every fraud report helps to better understand and address the threat in the long term. So how do we encourage more of them?

Key themes have emerged from our research. We specifically wanted to explore the following areas in more detail:

i. Knowing where to report

ii. Incentive to report

iii. Recognising you are a victim

iv. Embarrassment and reputational impact

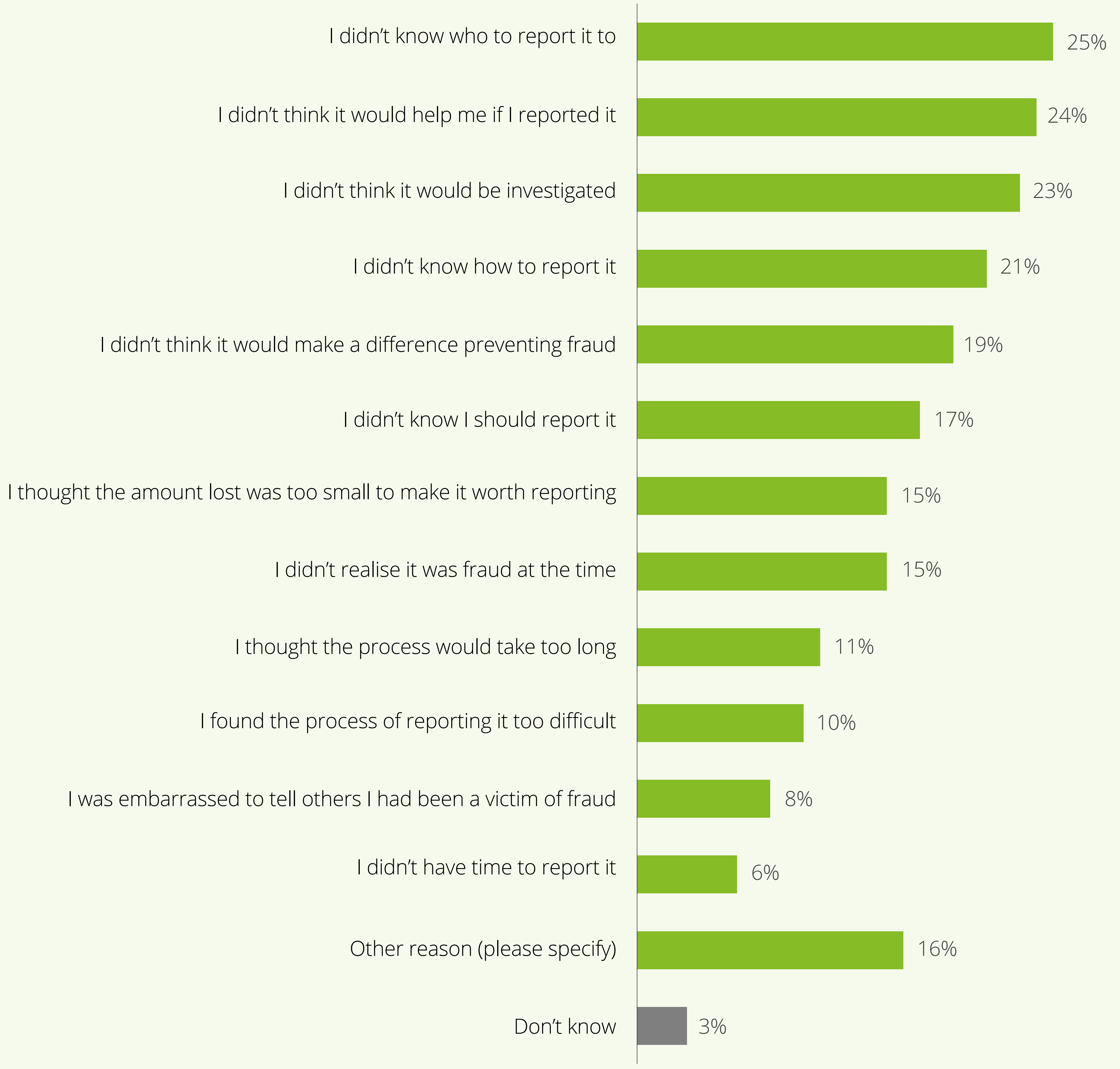
v. Lack of confidence

vi. Victim's reporting priorities

3.2.i Knowing where to report

Our survey informs us that at least thirty-four per cent of those surveyed who had experienced a fraud but did not report it did so because they did not know where or how to report. For those participants who had reported, the majority did so to their bank. Action Fraud, although mentioned, was only seen as the primary place to report when they had experienced a virus on their computer or received a scam text/email.

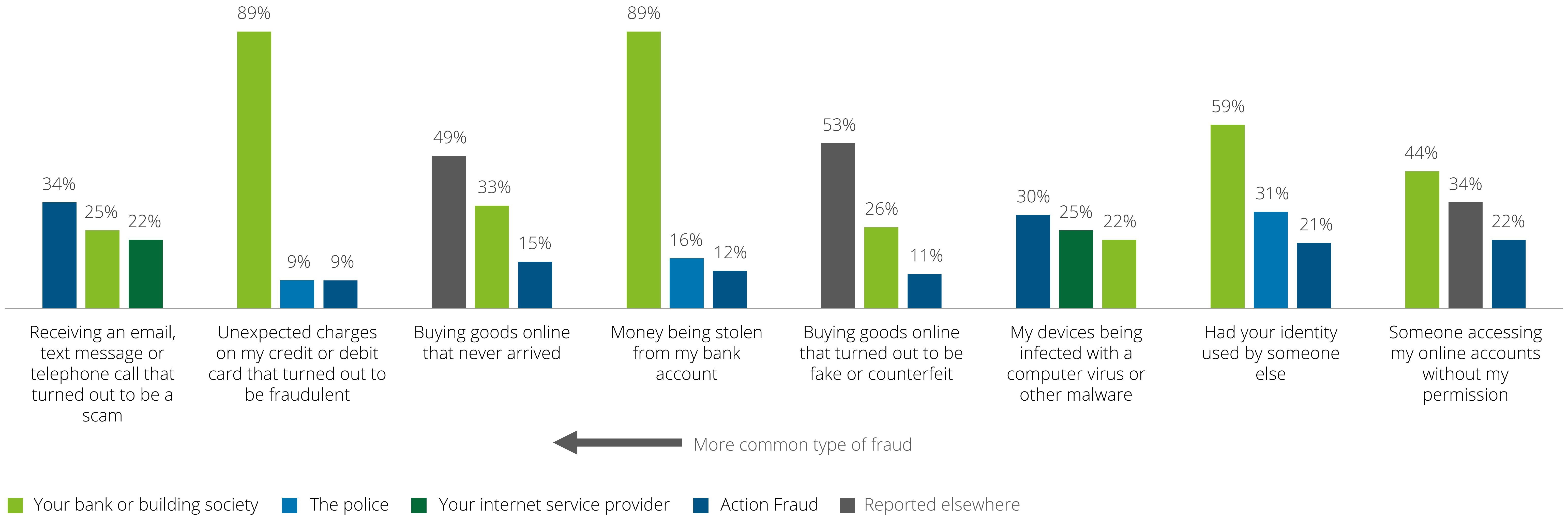
You mentioned that you chose not to report the fraud that you had experienced. Why was that?

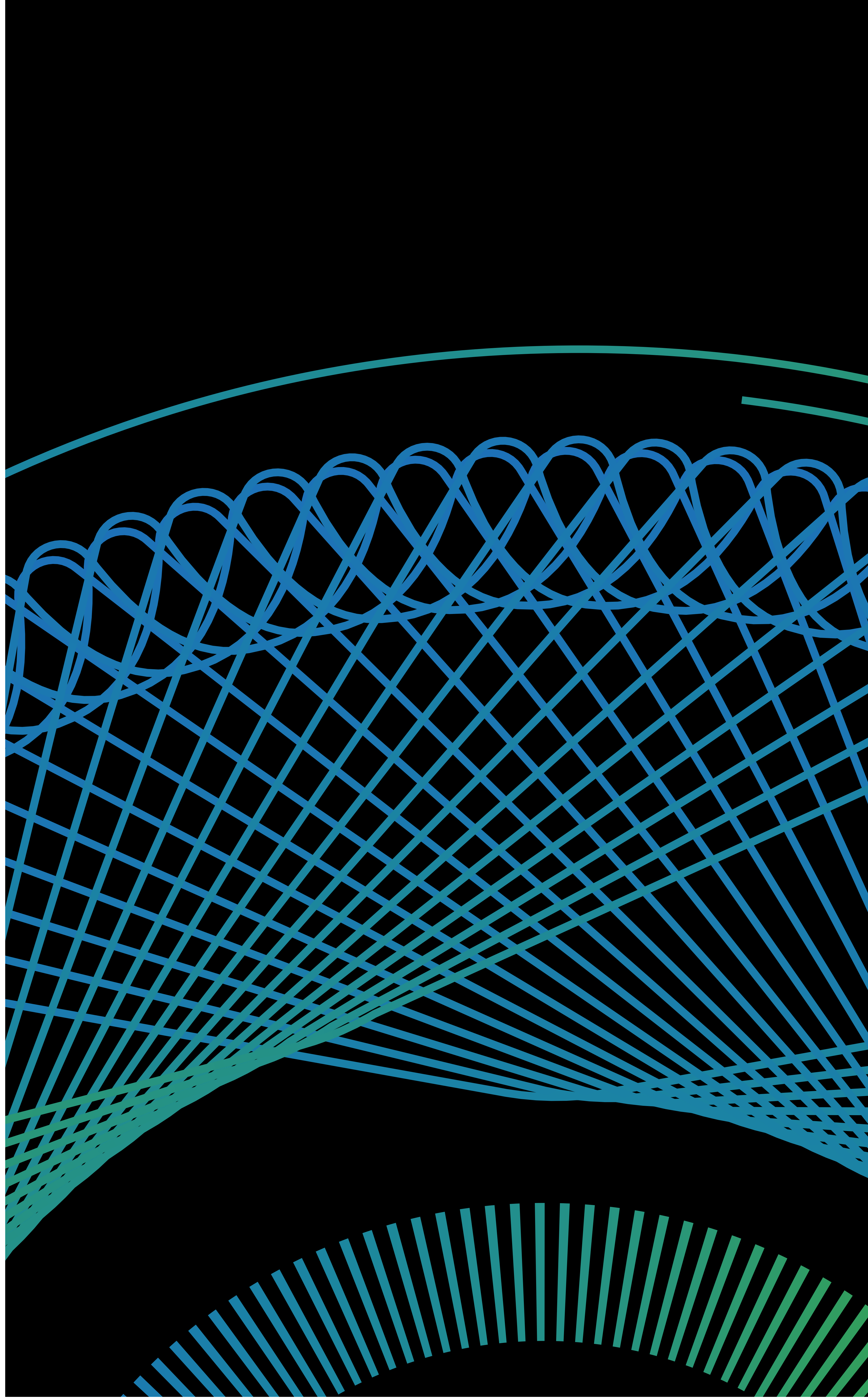


Where the public report fraud depends on the type of fraud. A majority of participants reported fraud related to their bank account, credit/debit cards or identity to their bank or building society, but there is greater variation for other types of fraud. Action Fraud was the most common for scam messages/calls and viruses/malware, and other organisations the most common for buying goods online that never arrived or were fake (possibly online retailers who sold the goods).

This is not surprising. The current messages about where to report fraud and cybercrime are confusing. You can see evidence of this on the diagram on the next page which sets out the fraud-reporting landscape. The variety of reporting channels also means it is virtually impossible to build a reliable picture of volumes, trends, patterns, links, and issues that would help drive effective prevention and communication back to victims and stakeholders.

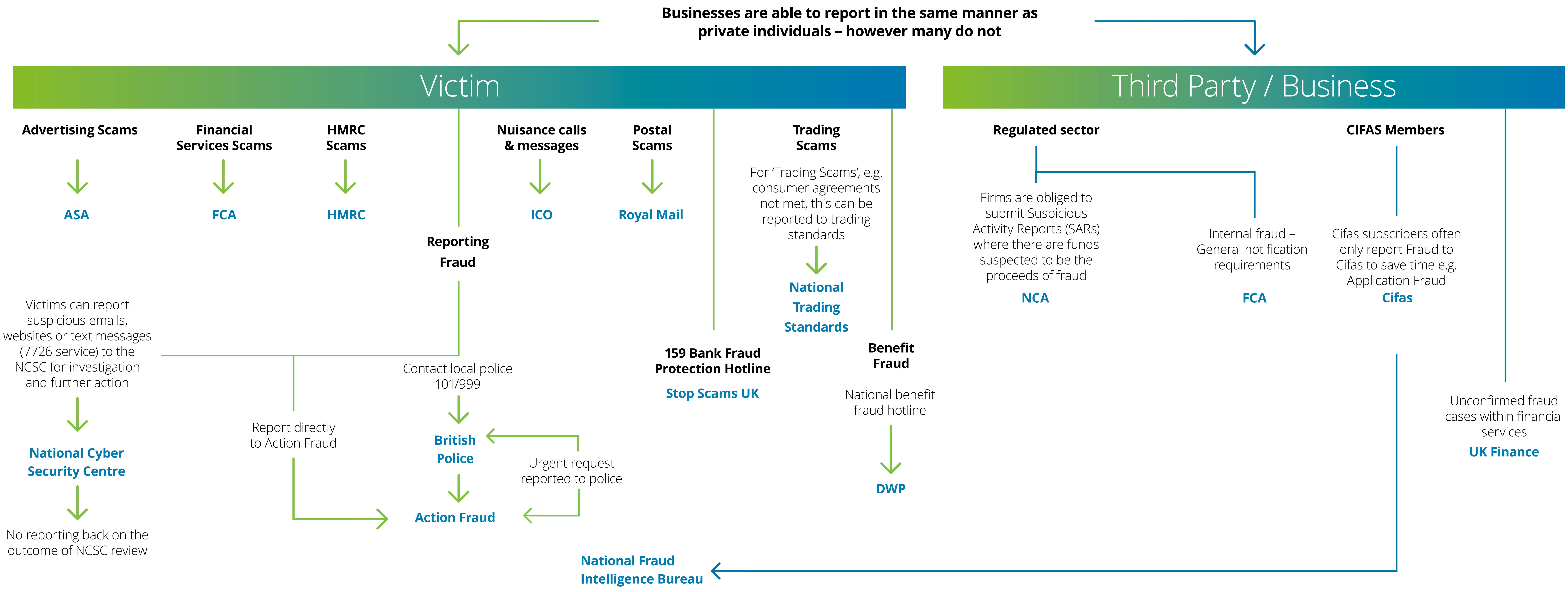
Who did you report this [fraud] to? Top three organisations selected
(Only types of fraud experienced by more than 100 respondents are displayed)





Current reporting landscape

For victims of fraud there is no single streamlined route for reporting fraud



Businesses are able to report in the same manner as private individuals – however many do not

Victim

Advertising Scams

ASA

Financial Services Scams

FCA

HMRC Scams

HMRC

Reporting Fraud

Victims can report suspicious emails, websites or text messages (7726 service) to the NCSC for investigation and further action

National Cyber Security Centre

No reporting back on the outcome of NCSC review

Report directly to Action Fraud

Contact local police 101/999

British Police

Urgent request reported to police

Action Fraud

Nuisance calls & messages

ICO

Postal Scams

Royal Mail

159 Bank Fraud Protection Hotline

Stop Scams UK

Trading Scams

For 'Trading Scams', e.g. consumer agreements not met, this can be reported to trading standards

National Trading Standards

Benefit Fraud

National benefit fraud hotline

DWP

Third Party / Business

Regulated sector

Firms are obliged to submit Suspicious Activity Reports (SARs) where there are funds suspected to be the proceeds of fraud

NCA

Internal fraud – General notification requirements

FCA

CIFAS Members

Cifas subscribers often only report Fraud to Cifas to save time e.g. Application Fraud

Cifas

National Fraud Intelligence Bureau

Unconfirmed fraud cases within financial services

UK Finance

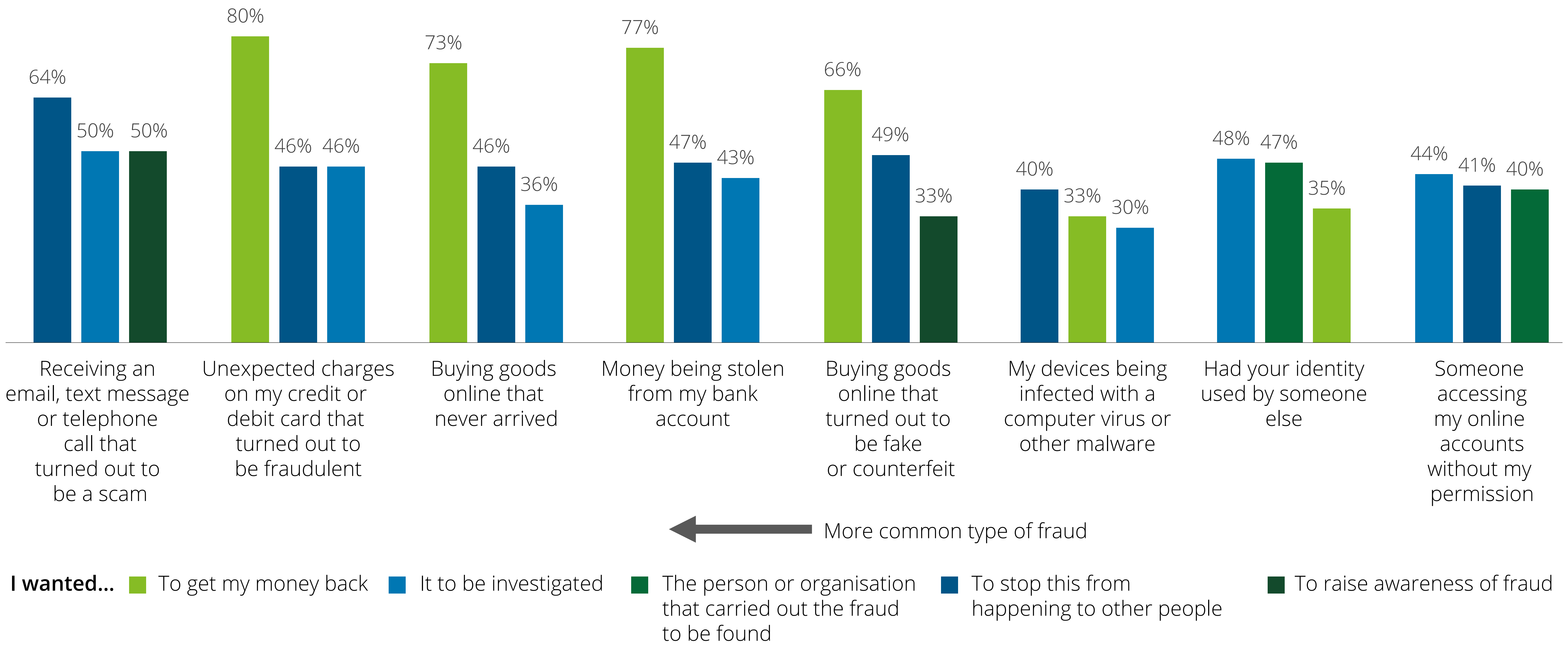
3.2.ii Incentive to report

To better understand someone's motivation or reluctance to report, we asked victims of fraud for the main reason why they chose to report it. Whilst recovering their money was primary, pleasingly, stopping others becoming a victim was also important, typically mentioned by half of those that had experienced a fraud (varies by fraud experienced). Other popular reasons were to have their case investigated, or to raise awareness of fraud.

Take the example of a victim identifying activity on their bank account that has defrauded them of £150. They report this to their bank, which reviews and confirms the details and subsequently reimburses the funds. The bank may or may not advise the victim to report the case to Action Fraud - there is no incentive for the victim to do so in the current system and therefore the likelihood is they will not.

If, however, the future solution provided a single-entry point with a joined-up response as demonstrated in the romance fraud SRS, then we would likely see a significant increase in reports to the new fraud and cyber reporting and response centre.

What made you decide to report the fraud you had experienced? Top three reasons
(Only types of fraud experienced by more than 100 respondents are displayed)



Perspective

There is little incentive for businesses to report fraud and cybercrime offences. The risk to consumer confidence, reputational damage and cost, outweigh any perceived reward. So how do we encourage businesses to do this?

Having access to feedback, case updates and intelligence from the SRS would enable organisations to identify and mitigate threats, thereby enhancing their own fraud disruption and prevention efforts. If they fully understand the role they can play in tackling fraud by reporting and sharing data, it would go a long way to improving understanding of the threat. With such knowledge we can strengthen defences, enhance disruption opportunities and increase public confidence.

The Joint Committee on the draft Online Safety Bill was appointed on 22 July 2021 to recommend improvements to the government. We are pleased to note that one aspect of their recommendations is to include paid-for scam/fraud advertising. This will place a duty of care on online service providers to protect its customers from the harm relating to paid advertising, including fraud. When this becomes law, it will likely lead to a significant uplift in fraud reporting from many organisations. Positively, the Lending Standards Board have also updated the Contingent Reimbursement Model (CRM) Code to strengthen protections against APP scams, while enabling more firms to sign up to its protections.

In addition, the Department for Business, Education, Innovation and Skills consultation on 'Restoring Trust in Audit and Corporate Governance', seeks to place greater focus on directors' and auditors' responsibilities in mitigating fraud risks.

Similarly, the Law Commission's discussion paper on corporate criminal liability considers broadening corporate liability to fraud and other economic crime. These potential changes are likely to trigger a wave of investment and focus on fraud risk management – consequently increasing corporate knowledge, intelligence, and the reporting of fraud.

It's important that organisations take steps to review their preparedness for any such legislative changes. Ultimately, if they occur and we can collectively remove the stigma of fraud reporting as well as enhance communication with victims, we will create a step-change in the volume of reports. It follows that those developing the next generation of fraud and cyber reporting and response centre will need to build a system capable of managing an exponential increase in reports.

3.2.iii Recognising you are a victim

The very nature of fraud offences mean they can go undetected. As such, victims may not recognise they have been defrauded for a considerable period. Equally, they often feel embarrassed about being 'duped'.

This is particularly prevalent in cases of romance fraud and mass marketing fraud. Often, despite clear evidence, the victim does not wish to recognise they have been a victim of fraud.

Similarly, the length of time it takes a victim of fraud to recognise they have been duped provides time and space for the fraudster to escape and conceal the proceeds of their crimes.

In other cases, the victim may not even know it is a crime, or that they can and should report it. This is evidenced by our survey, with 17 per cent of respondents stating they did not report because they did not know they should, and 15 per cent failing to do so because they did not realise it was fraud.

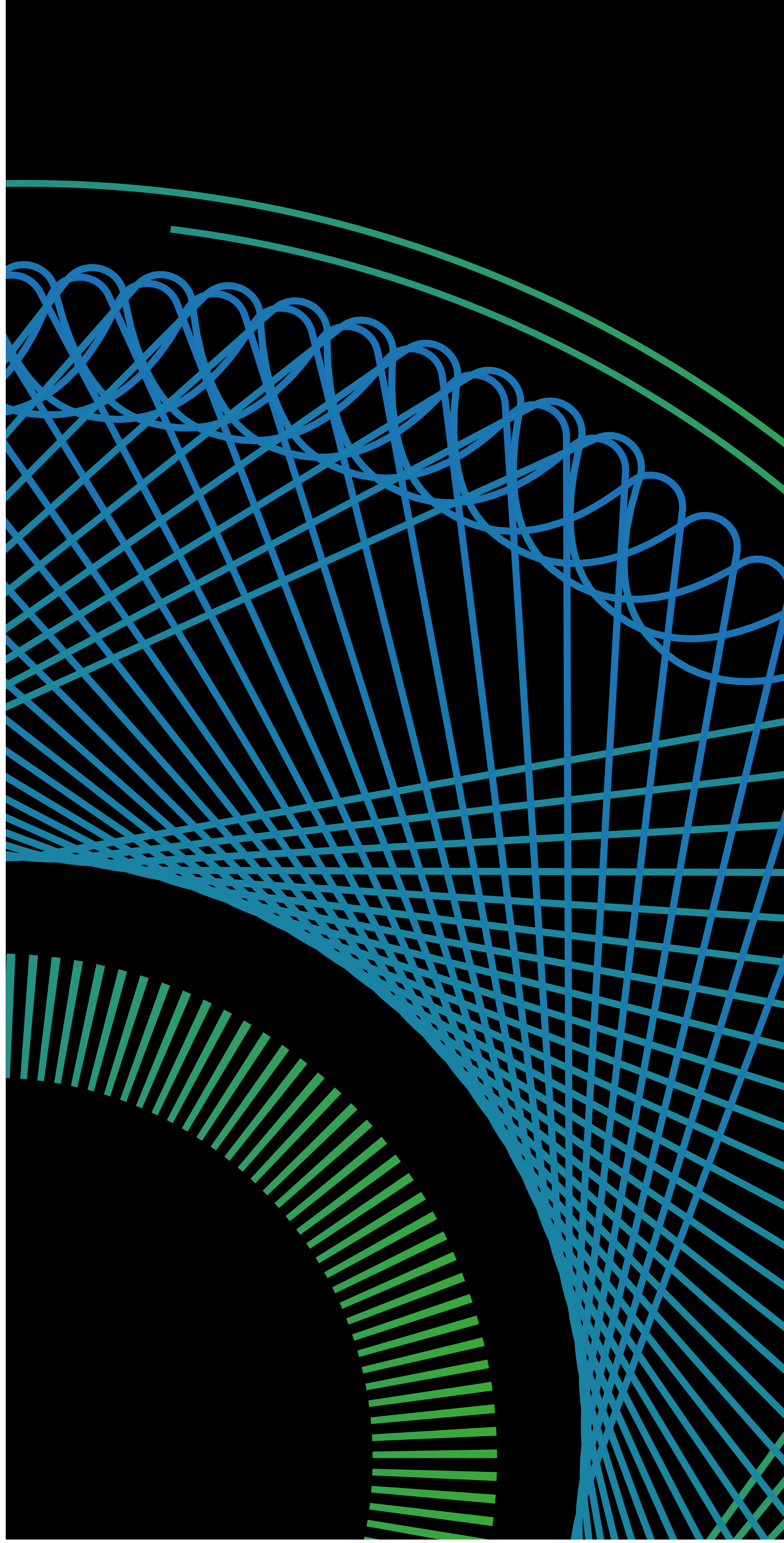
> *17 per cent of respondents stated they did not report because they did not know they should, and 15 per cent because they did not realise it was fraud."*

Perspective

The language we use to describe fraud plays a vital role. It is not uncommon for organisations to use the word 'scam' to describe a fraud that has occurred. For some, the interpretation of a scam is that it is not a crime, merely an activity carried out by a harmless trickster. This is explored in more detail by Betts & Kassem, in *Is the Language of Fraud Failing its Victims?*[19]

The same applies to the term 'cyber': what does this mean to the public? Does the average person understand the difference between cyber-dependent and cyber-enabled? Is the word 'cyber' even helpful when looking at a fraud? Would the term 'online fraud' adequately describe what has happened? And, in these technologically enabled times, is it necessary to distinguish between cyber and non-cyber crime at all?

Moving forward, communication is key; and as a collective, it is crucial to ensure the language and terminology we use is consistent and clear to everyone.



[19] Betts & Kassem, 'Is the language of 'Fraud' failing its victims, November 2019, www.researchgate.net/publication/337089740_Is_the_language_of_fraud_failing_its_victims

3.2.iv Embarrassment and reputational impact

For some people, admitting they have been a victim of fraud is deeply embarrassing, and sharing it with friends and family can be even worse than reporting it to the authorities. This desire to keep it quiet plays into the fraudster's hands, allowing them to continue their criminal activity without fear. Many offenders actively attempt to isolate their victims, turning them against family members who might point out the folly of continuing the contact or investment.

Perspective

We need to remove the stigma and stop 'victim blaming'. There needs to be a hard-hitting public information campaign, with impactful stories that highlight the issues; and as a collective, we must dispel comments such as "How could they be so stupid?" or "I'd never fall for that", when in reality, many of us have been a victim or know someone who has.

This applies across the fraud landscape, both for individuals and for businesses, where much fraud also goes unreported. Depending on the nature and scale of it, reluctance to report may be based on a combination of embarrassment and concerns about the reputational impact that could potentially lose them the confidence of their shareholders or customers.

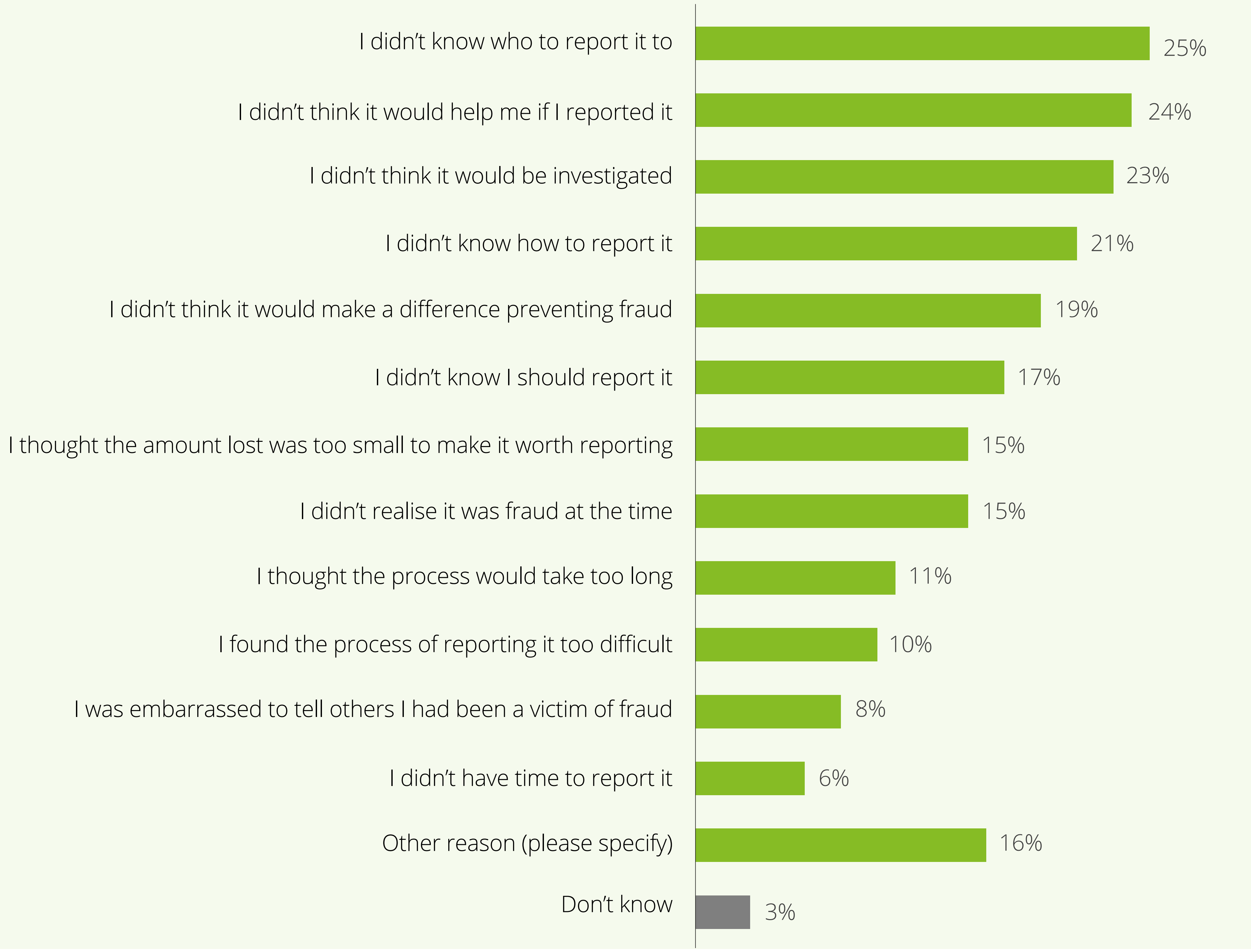
Ultimately, if we really are to move the dial on fraud reporting, change is needed from individuals and businesses alike.

3.2.v Lack of confidence

It is unsurprising that individuals and businesses falling victim to fraud are apathetic to the idea of reporting. The small number of frauds investigated makes a criminal justice outcome unlikely.

As part of our survey, we asked participants to explain why they did not report their fraud. Twenty-four per cent stated they did not think it would help if they did, and 25 per cent said that they did not know who to report it to, nineteen per cent thought it would make no difference in preventing fraud.

You mentioned that you chose not to report the fraud that you had experienced. Why was that?



Perspective

We must respond to the needs of victims. There are some simple actions that can be taken, starting with management of their expectations. It is crucial to be honest and open, and to explain that the chance of an investigation being opened is small but recognise the importance of the report in preventing and disrupting further criminal activity.

Ensure feedback is given to the victim at a later stage regarding how their report has contributed to safeguarding others, disrupting a criminal money flow, or identifying a criminal network. This quality feedback will enthuse them and help to spread the message that reporting is vital.

3.2.vi. Victims' reporting priorities

When we asked the public what they would prioritise within a fraud reporting service, the top attributes were:

1. Outcome
2. Ease and speed of submitting a report
3. Having a single point of contact.

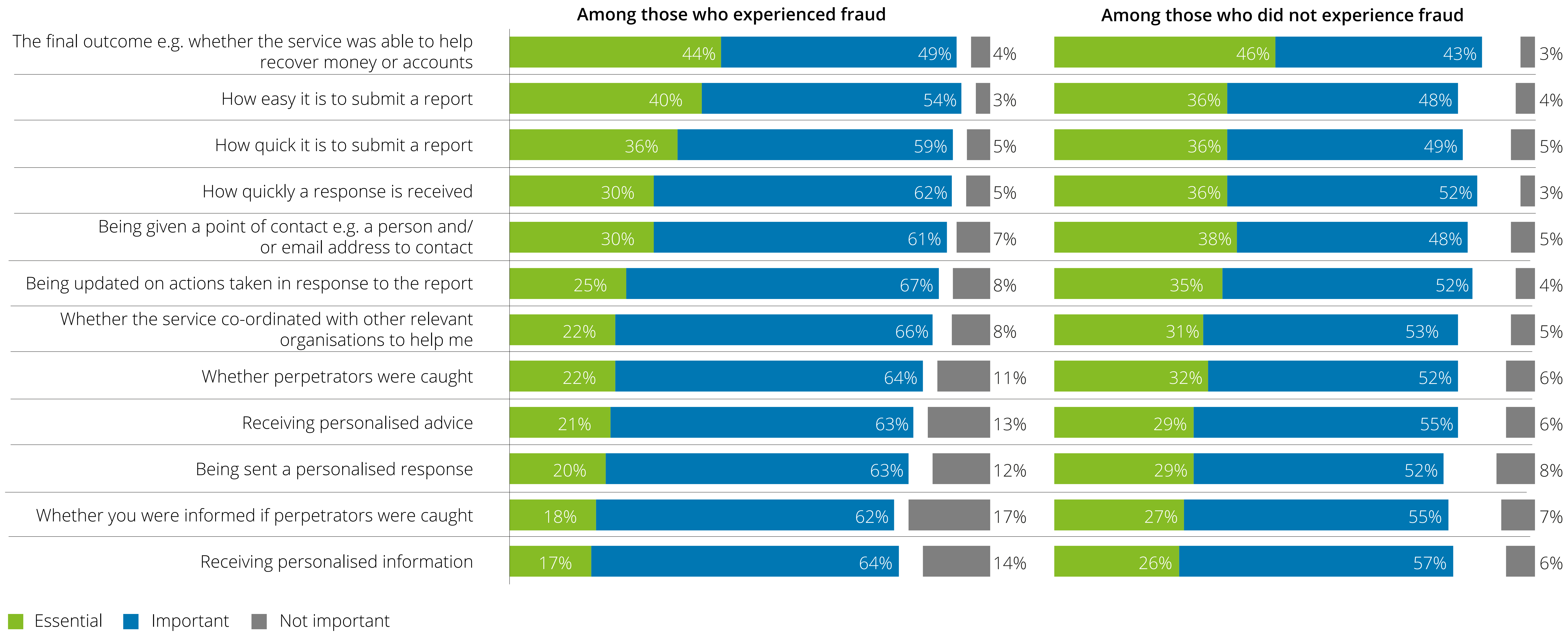
Ninety-four per cent of those that had experienced a fraud wanted a service that could help them recover their money, while over nine in ten wanted a service that allowed for quick and easy reporting (both ninety-four per cent).

Consequently, the key considerations should be how to:

- Bring all existing sources of reporting together to develop a single body with the ability to capture all reports of fraud by phone, app or online.
- Clearly signpost the way to support agencies (e.g., Victim Support, Citizens Advice), their financial institutions or another appropriate agency.

Ideally, one online report or call should take you to all the support you need. Indeed, 88 per cent of those victims surveyed stated that the co-ordination of services was either essential or important to them.

[If you were to experience something similar again and wanted to report it to someone], to what extent, if at all, would you consider the following to be important?



Single fraud reporting mechanism – example in action with romance fraud.

Using a case of romance fraud, the diagram illustrates how communication flows could work via the proposed single reporting solution (SRS). The victim of a fraud is first directed to report the incident to the SRS, which can be through a web-based reporting form, telephone, or mobile app. The SRS is then able to triage the data provided and relay it to all relevant bodies/agencies on behalf of the victim and pass key case data points through to the NFIB for intelligence sharing.

In the example provided, these additional bodies/agencies may include victim support agencies, the victim's bank, the National Economic Victim Care Unit (NEVCU) and a debt management organisation. This enables proactive action to identify and protect vulnerable fraud victims. Steps could also be taken to add additional account protections or provide bespoke support to the victim. The SRS can also act as a single relay point for the victim in providing prevention advice and ongoing access to case updates and outcomes.

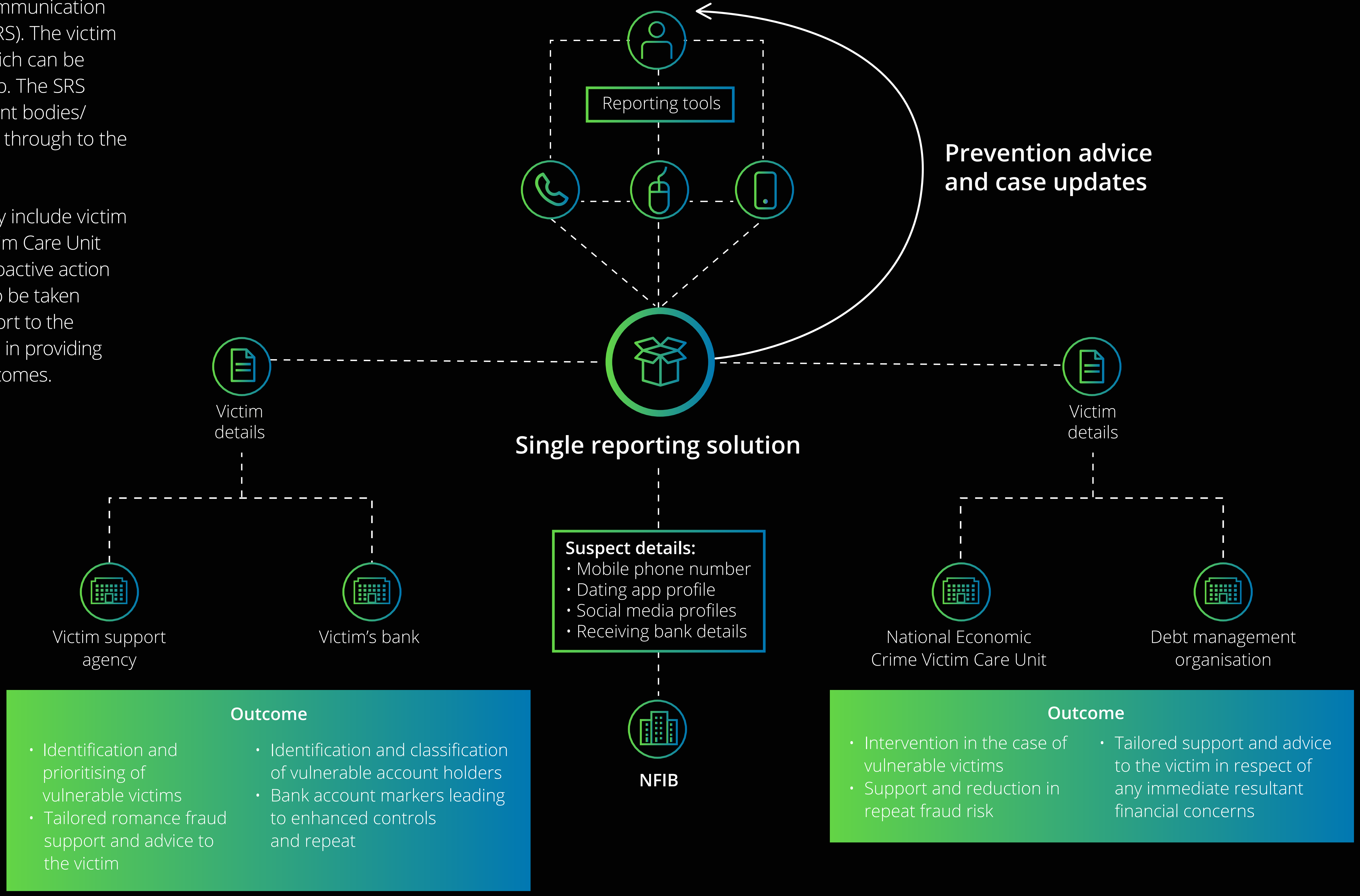
A victim of fraud has sent the entire balance of their personal savings (£10,000) to a third party after initially connecting through a dating app.

The victim has the following information of the suspected fraudster:

Mobile phone number

Dating app profile

Receiving bank details



Reporting tools

Prevention advice and case updates

Single reporting solution

Victim details

Victim support agency

Victim's bank

Outcome

- Identification and prioritising of vulnerable victims
- Tailored romance fraud support and advice to the victim
- Identification and classification of vulnerable account holders
- Bank account markers leading to enhanced controls and repeat

Suspect details:
- Mobile phone number
- Dating app profile
- Social media profiles
- Receiving bank details

NFIB

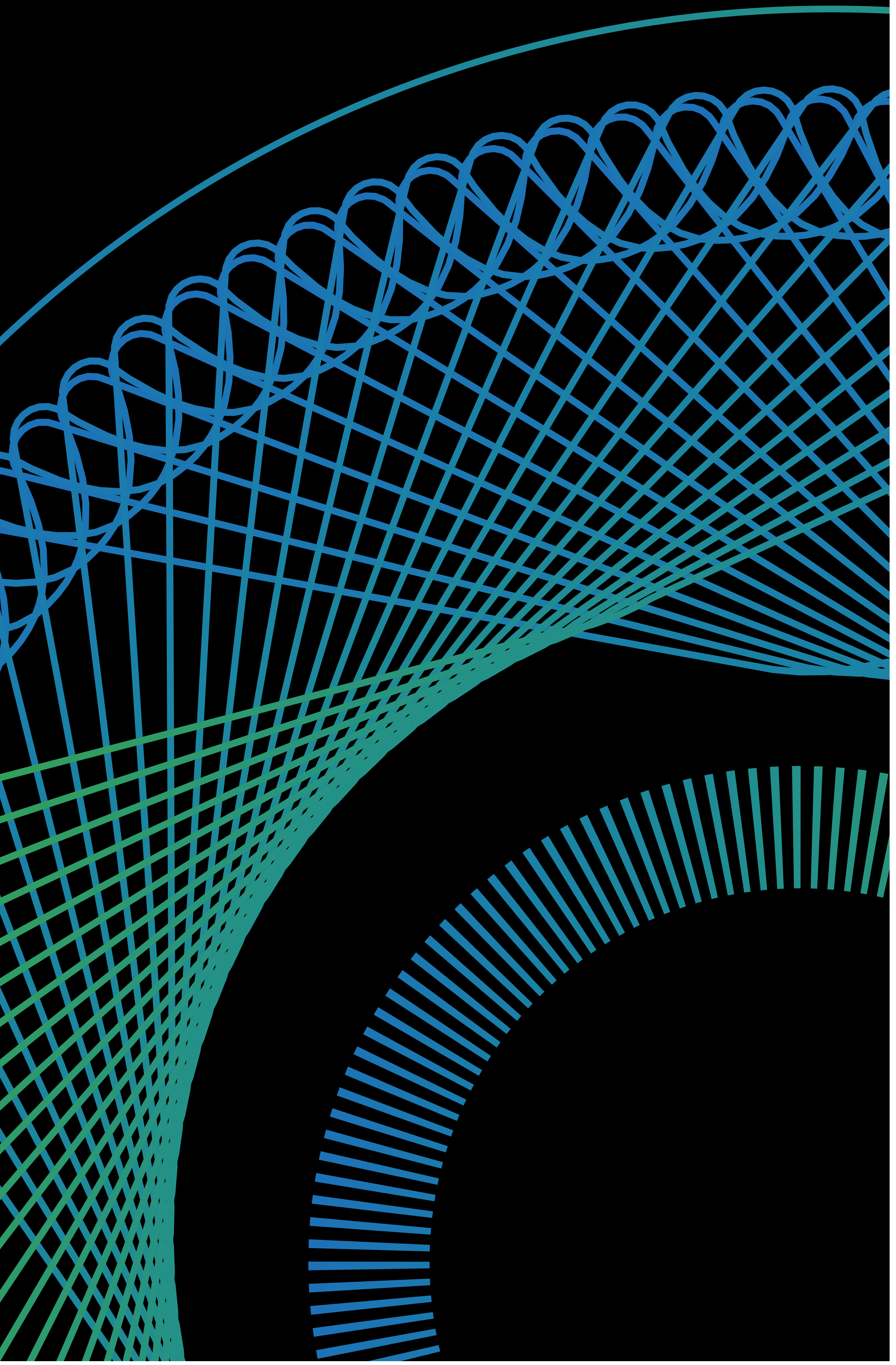
Victim details

National Economic Crime Victim Care Unit

Debt management organisation

Outcome

- Intervention in the case of vulnerable victims
- Support and reduction in repeat fraud risk
- Tailored support and advice to the victim in respect of any immediate resultant financial concerns



4. Towards a new fraud ecosystem

A different approach is required. One with far greater focus on proactive prevention and disruption that will allow our limited investigative capacity to target those causing most harm to our communities and the UK economy.

Bringing all parts of the ecosystem together across public and private sector – policy makers, law enforcement, financial institutions and the wider corporate sector, particularly social media, technology, and telecommunications providers – is vital. As is placing the victim at the centre of this new ecosystem. The next iteration of the Economic Crime plan presents an opportunity to do this; to reset and outline a new strategy.

A strong starting point will be the development of a single reporting solution, to transform Action Fraud into a world class victim-centric fraud and cybercrime reporting and response centre. This should place the victims needs first, managing their expectations, providing a seamless link to support services, offering meaningful prevention advice and keeping them informed every step of the way.

The second step is to transform the NFIB into a world leading intelligence and data analytics centre, delivering fast to real time prevention, disruption and detection opportunities across the public and private sector.

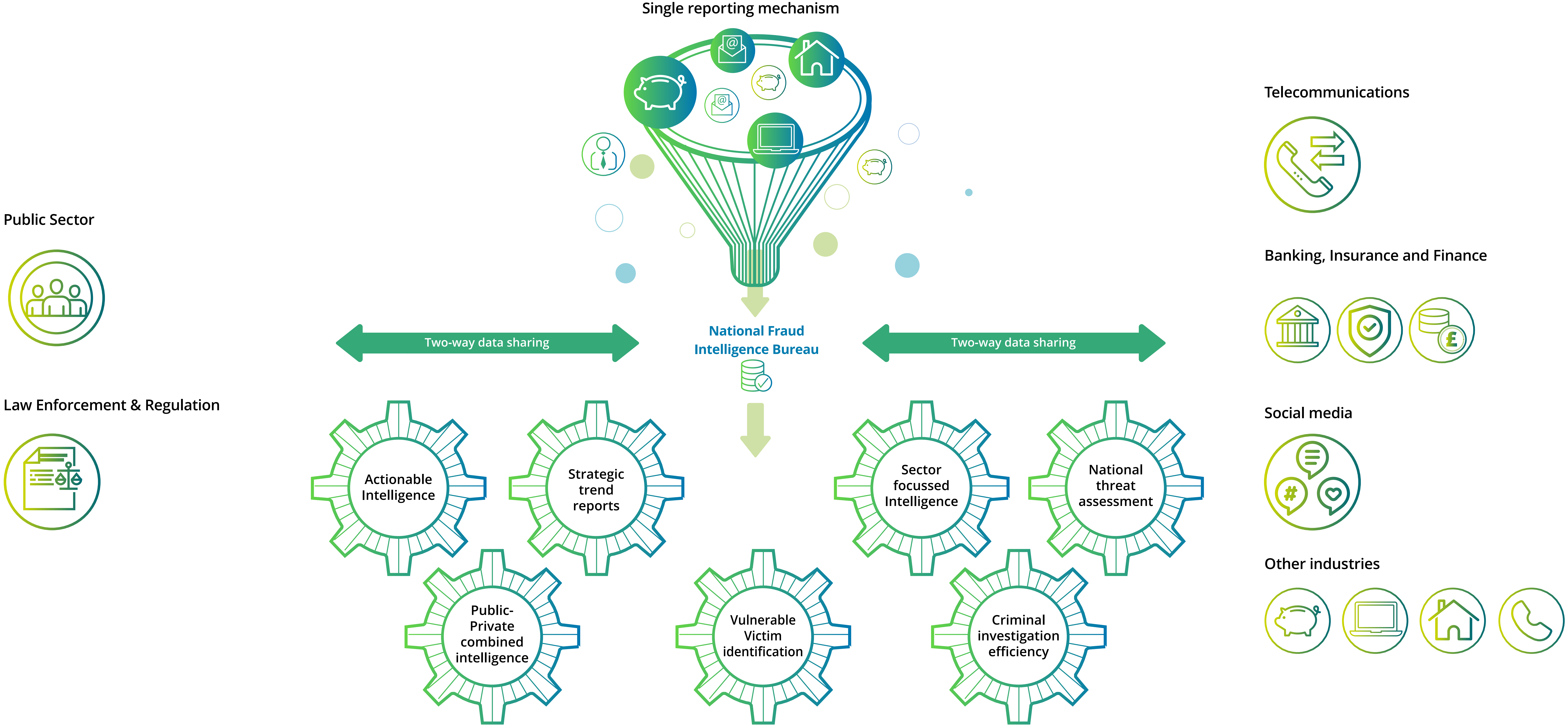
In other words, the redesign of Action Fraud and the NFIB presents an opportunity to develop a two-way flow of information and intelligence from across the economic crime ecosystem, into and out of the NFIB. One that also provides the public and business with a simpler, more focused, and more responsive reporting channel.

There's also the opportunity to build and incorporate wider ecosystem changes, such as Companies House reform, the reform of the suspicious activity report regime, and the Home Office-led information sharing pilots, that will to help enrich any new fraud reporting landscape.

Where it is appropriate to do so, and without compromising investigations, a proactive data feed would empower partner organisations to take justified and proportionate disruptive action during the investigative process. Such as suspending a bank account or removing a fraudulent post from social media. The diagram on the following page shows how the system could work.

> ***"A strong starting point will be the development of a single reporting solution, to transform Action Fraud into a world class victim-centric fraud and cybercrime reporting and response centre."***

4.1 Vision of the NFIB ecosystem



Single reporting mechanism

National Fraud Intelligence Bureau

Two-way data sharing

Two-way data sharing

Public Sector

Law Enforcement & Regulation

Telecommunications

Banking, Insurance and Finance

Social media

Other industries

Actionable Intelligence

Strategic trend reports

Public-Private combined intelligence

Vulnerable Victim identification

Sector focussed Intelligence

National threat assessment

Criminal investigation efficiency

4.2 The importance of public-private data sharing

If we are going to truly transform the way fraud is reported and responded to, the sharing of data between the public and private sectors will be critical. The scenario set out in the diagram shows why. We see in this scenario a vulnerable victim of fraud has sent £20,000 from their personal current account following a cold call from an investment company. The victim has reported the fraud to the Single Reporting Solution and provides the mobile number that was used by the criminal.

The mobile phone number has no subscriber details to name the suspect. However, the interconnectivity of private sector data allows the operator to link the suspect to various products and services across the private sector. In this case, the phone number used in the fraud is linked to a car insurance policy. This connects the reported fraud to the named policy owner, who is subsequently linked to a suspicious activity report. The connected data then produces a picture showing a boiler room fraud with four suspects.

A Single Reporting Solution offers prevention and disruption opportunities by blocking and suspending the suspect's products and services within the private sector. On the other hand, it also allows operators to produce an effective arrest package for law enforcement officers to pursue a criminal investigation and obtain a detection.

4.3 Assisting vulnerable victims

The connected data across the private sector provides opportunities to provide early detection of vulnerable victims. For example, financial services identify vulnerable customers to comply with conduct regulations to ensure fair treatment. Home energy services assess vulnerable customers to ensure fair treatment and provide extra support to comply with their social obligations.

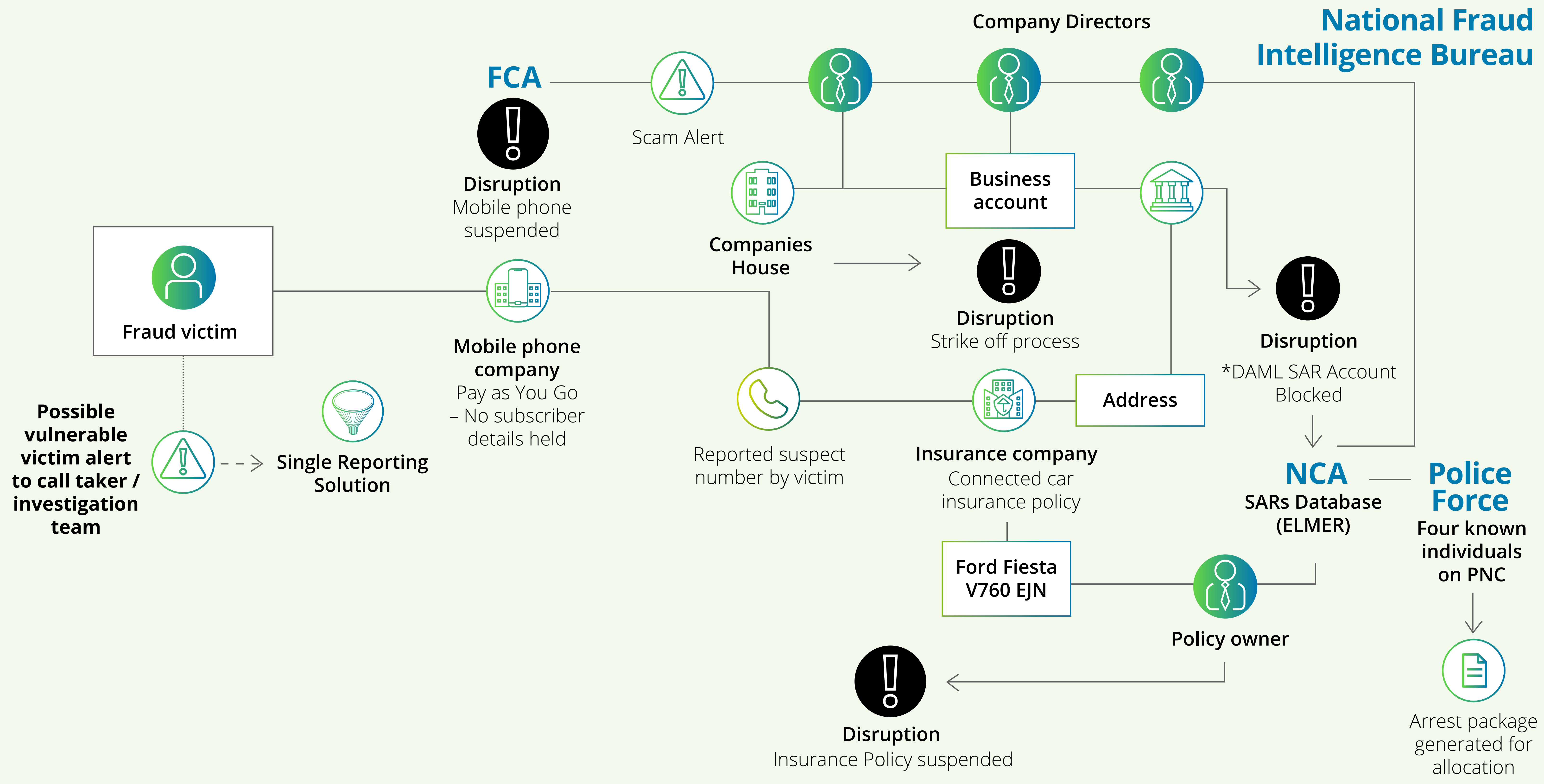
This enriched, holistic intelligence picture, facilitated by a single reporting channel and the sharing of information across sectors, will generate significant benefits – most importantly in the disruption, prevention, and investigation of fraud.

It will also inform the national picture by identifying new risks, trends, methodologies, locations, and offenders, and enable this vital data to be shared in a timely manner for assessment and action by the appropriate law enforcement partner.

Finally, and by no means least, it will support a robust feedback loop and communication channel with the victim. Such a model will create a far greater deterrent against the most harmful offenders and those lower down the fraud food-chain.

Undoubtedly, there will be challenges with this approach to proactively share information and intelligence to prevent crime. None more so than the legislative framework and perceptions about how that should be used.

Example in action – a demonstration of how intelligence can be identified and shared throughout the ecosystem to disrupt criminals


Company Directors
National Fraud Intelligence Bureau
FCA
Scam Alert
Disruption
Mobile phone suspended
Business account
Companies House
Disruption
Strike off process
Fraud victim
Mobile phone company
Pay as You Go – No subscriber details held
Disruption
*DAML SAR Account Blocked
Address
Possible vulnerable victim alert to call taker / investigation team
Single Reporting Solution
Reported suspect number by victim
Insurance company
Connected car insurance policy
NCA
SARs Database (ELMER)
Police Force
Four known individuals on PNC
Ford Fiesta V760 EJN
Policy owner
Disruption
Insurance Policy suspended
Arrest package generated for allocation

5. Conclusion

Fraud and cybercrime offences continue to increase, causing harm to our communities and impacting the economic well-being of the UK.

Across the ecosystem are multiple organisations with brilliant, passionate people trying to make a real difference. But despite their best endeavours, they have not stemmed the rising tide of fraud and cybercrime. Without a change in approach, that tide will continue to grow in force, impacting more victims, communities, businesses, and our economic prosperity. It is sobering to think that potentially 71 per cent of the population have been victim of one or more frauds or cybercrimes.

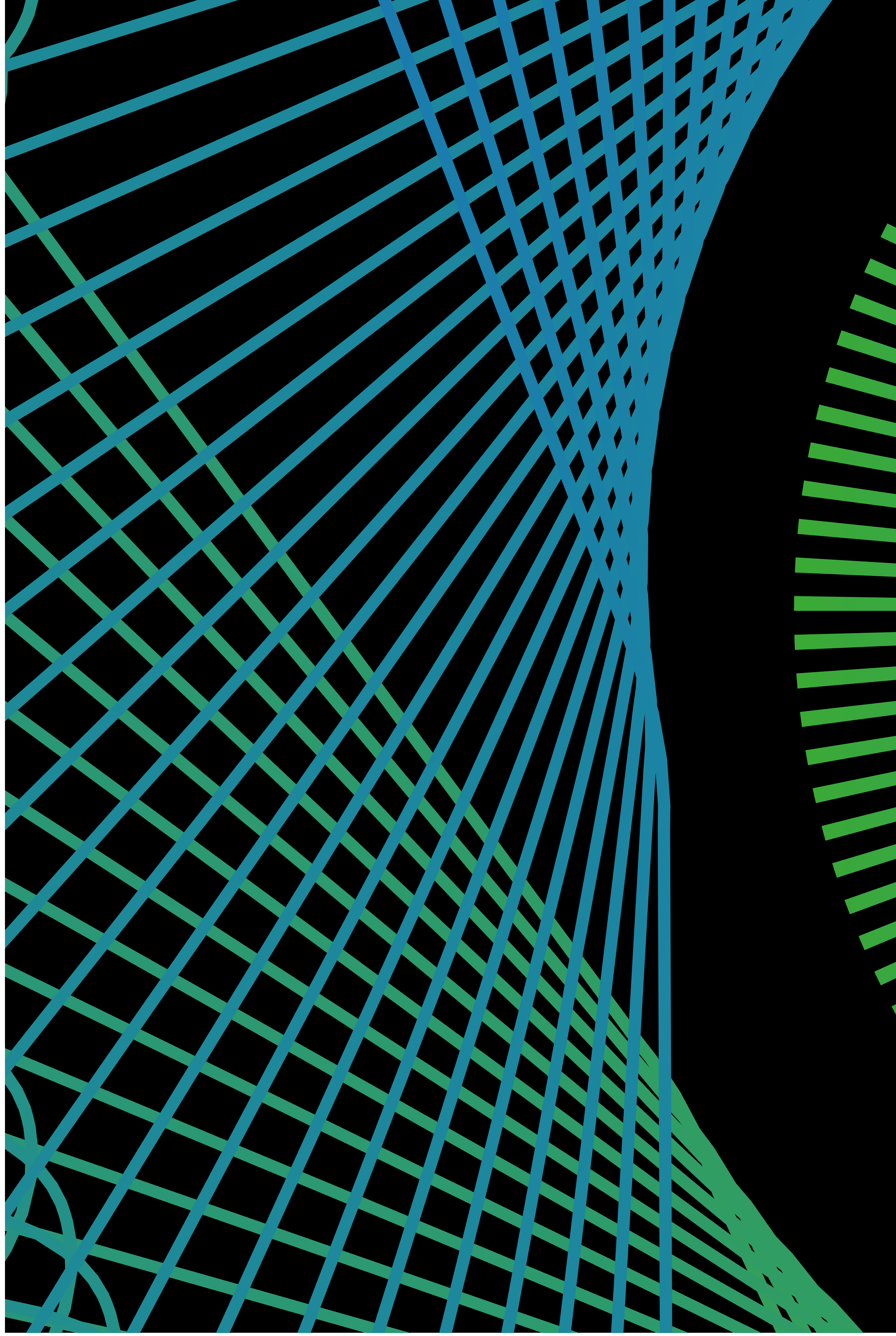
> ***"There is an opportunity to build on the foundations of Action Fraud, and develop a world class, victim-centric fraud and cybercrime reporting and response centre. One that will succeed in disruption, prevention, investigation, and victim support."***

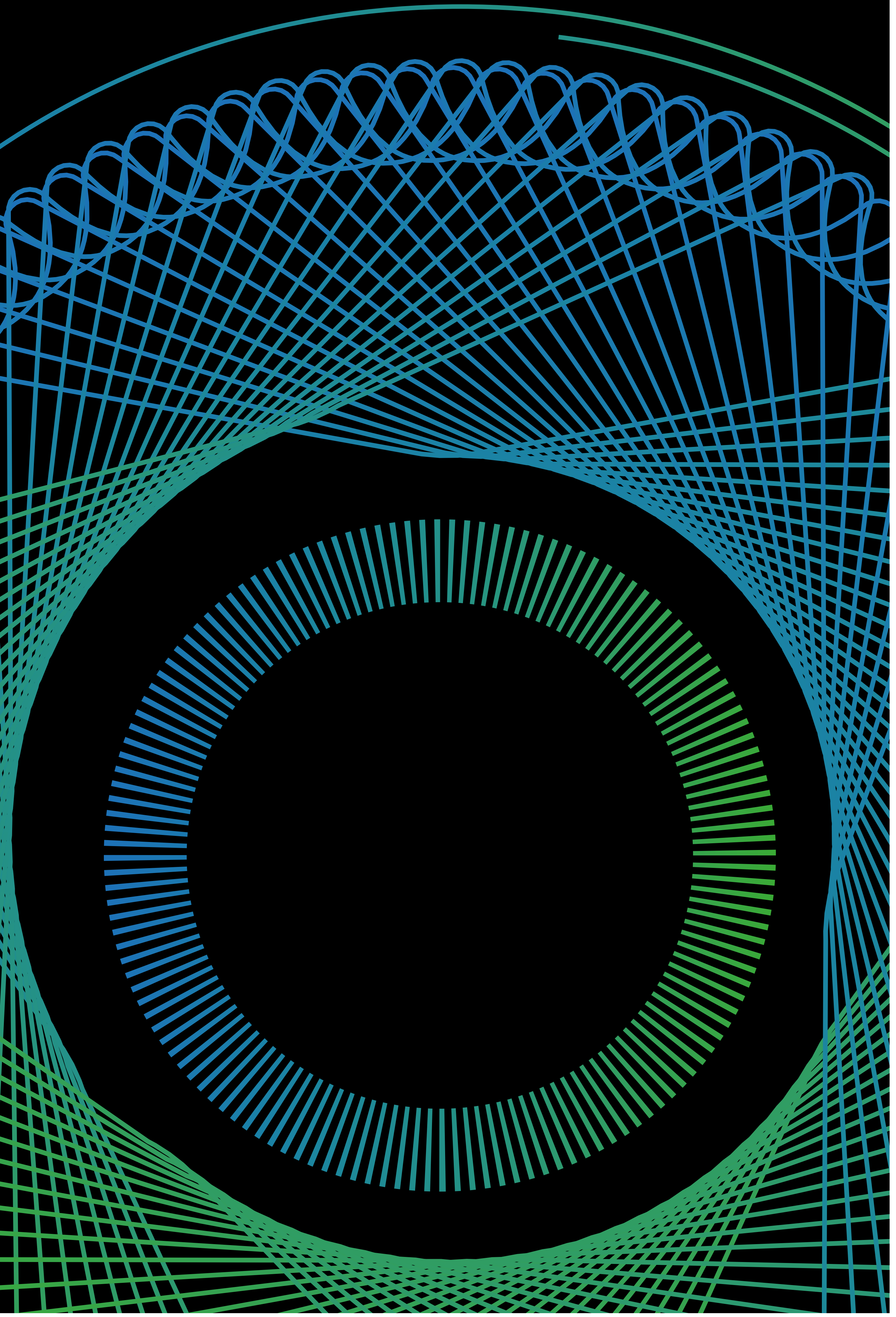
The ecosystem must place the victims' needs first, manage their expectations, provide a seamless link to support services, offer meaningful prevention advice and keep them informed every step of the way. All this underpinned by one consistent, coordinated public education and behavioural campaign.

An improved service will encourage more and better reporting from individuals and businesses. It will increase victim satisfaction and confidence, reduce repeat victimisation, and have the potential to build an active fraud and cybercrime prevention community.

Through collaboration and enhanced intelligence and data sharing, the UK can build a world-leading intelligence and data analytics centre. This capability will be alerted to new risks, trends, and methodologies. It will deliver fast prevention, disruption, and detection opportunities across public and private sectors, making it a more hostile environment for organised crime groups to operate.

Now is the time to be transformational, ambitious, and courageous; to have a single vision and objective in mind. This requires both public and private sectors to collaborate fully — demonstrating the bold leadership necessary to drive the paradigm shift required.





Nick Downing
Economic Crime Specialist, Director
nickdowning@deloitte.co.uk
+44 (0) 20 8071 0802

Jules Colborne-Baber
Head of Fraud and Investigations, Partner
jcolbornebaber@deloitte.co.uk
+44 (0) 7803 207 417

Richard Hobbs
Lead Partner for Security and Justice UK
rhobbs@deloitte.co.uk
+44 (0) 7779 573 856

James Meadowcroft
Fraud Specialist, Director
jmeadowcroft@deloitte.co.uk
+44 (0) 7946 650 551

Deloitte.

Important notice

This document has been prepared by Deloitte LLP for the sole purpose of enabling the parties to whom it is addressed to evaluate the capabilities of Deloitte LLP to supply the proposed services.

Other than as stated below, this document and its contents are confidential and prepared solely for your information, and may not be reproduced, redistributed or passed on to any other person in whole or in part. If this document contains details of an arrangement that could result in a tax or National Insurance saving, no such conditions of confidentiality apply to the details of that arrangement (for example, for the purpose of discussion with tax authorities). No other party is entitled to rely on this document for any purpose whatsoever and we accept no liability to any other party who is shown or obtains access to this document.

This document is not an offer and is not intended to be contractually binding. Should this proposal be acceptable to you, and following the conclusion of our internal acceptance procedures, we would be pleased to discuss terms and conditions with you prior to our appointment.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 1 New Street Square, London EC4A 3HQ, United Kingdom.

Deloitte LLP is the United Kingdom affiliate of Deloitte NSE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NSE LLP do not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

Designed and produced by 368 at Deloitte. J21714

BACK <