



# A 'VICTIMLESS CRIME'?

WHY FRAUD POLICING NEEDS A RE-DESIGN

MICHAEL SKIDMORE

MAY 2025

THE  
POLICE  
FOUNDATION  
The UK's policing think tank



# A 'VICTIMLESS CRIME'?

## WHY FRAUD POLICING NEEDS A RE-DESIGN

**MICHAEL SKIDMORE**

### **About Virgin Media O2**

Virgin Media O2 launched on 1 June 2021, combining the UK's largest and most reliable mobile network with a fully gigabit broadband network.



The company has more than 45 million UK connections across its award-winning broadband, mobile, TV and home phone services. Its fixed network covers more than half of the country (18.4 million premises serviceable) alongside a mobile network that covers 99 per cent of the nation's population. The company is on track to bring 5G to all populated areas by end 2030 and already offers 5G outdoor coverage to more 77 per cent of the UK population.

### **About the Police Foundation**

The Police Foundation is the only independent think tank focused exclusively on improving policing and developing knowledge and understanding of policing and crime reduction. Our mission is to generate evidence and develop ideas which deliver better policing and a safer society. We do this by producing trusted, impartial research and by working with the police and their partners to create change.

# CONTENTS

<b>Foreword</b>	<b>3</b>
<b>Executive Summary</b>	<b>5</b>
<b>1. Introduction</b>	<b>7</b>
1.1 Methodology	7
<b>2. Context</b>	<b>9</b>
2.1 The volume and cost of fraud	9
2.2 The harm caused by fraud	9
2.3 The key characteristics of fraud	10
<b>3. The police response to fraud</b>	<b>13</b>
3.1 A lack of resources	13
3.2 A predominantly local response to a cross-border crime	13
3.3 A lack of an ability to identify harm and seriousness	14
3.4 A lack of skills	14
3.5 The response remains too focused on arrests and prosecutions	15
3.6 There is a lot of data on fraud but insufficient insight is being generated from it	15
<b>4. Re-designing our police institutions to tackle fraud</b>	<b>17</b>
4.1 The importance of prevention	17
4.2 Organisational reform	18
4.3 Collaboration with the private sector	20
4.4 Skills	21
4.5 Resources	22
<b>5. Conclusion</b>	<b>23</b>
<b>References</b>	<b>24</b>





# FOREWORD

**Lutz Schüler, Chief Executive Officer of Virgin Media O2**

The UK is in the midst of a fraud epidemic. Accounting for two in every five crimes, scams have become ubiquitous. A quarter of Brits are targeted every single week.

Consumers are under near constant attack from fraudsters posing as representatives of banks, mobile providers, parcel delivery companies, online retailers and even HMRC, all attempting to steal personal data and money. In a single year, Virgin Media O2 blocked suspected fraudulent transactions worth £250 million. Despite the proactive action taken by the telecoms sector, often in collaboration with the financial services industry, fraud is costing the economy £6.8 billion a year and shattering people's lives.

Despite this, more and more fraudsters are getting away with it. While the fraud risk has grown exponentially and there are an estimated 4.1 million frauds committed in the UK every year, the latest Home Office crime outcomes data shows only 3,641 fraud cases resulted in a charge, down 10 per cent year on year.

With consumers and businesses facing this perfect storm, we commissioned the Police Foundation to undertake in-depth research on the problem. They've spoken to experts working across fraud from local police forces up to the Home Office and National Crime Agency, providing a comprehensive picture of the challenges and complexities faced by those working in law enforcement today, as well as compelling recommendations on how to ensure better outcomes for fraud victims.

This report reveals the police do not lack the willingness or ambition to tackle fraud. Rather, they are constrained by a system created in a different era to fight a crime that has evolved beyond recognition.

Put simply, too heavy a burden is falling on local officers who lack the skills or resources needed to tackle this complex, organised and cross-border crime.

The report's recommendations offer a practical way forward for the government to deliver its manifesto commitment of doing more to fight fraud, and come ahead of the new, expanded fraud strategy expected later this year.

*A victimless crime?* is a deliberately provocative question posed in the title of this report. Of course, it couldn't be further from the truth for those who experience it, but it's hard to imagine any other crime reaching this scale without becoming a national priority to tackle.

As is made clear throughout, tackling fraud does not fall entirely to the police. Businesses, like ours, have a vital role to play in preventing fraud. Over the last two years, our investments have helped block more than 168 million scam text messages from ever reaching customers' phones, and we flag more than 50 million scam and spam calls every month.

But the data shows that we simply can't build our walls high enough - prevention is only part of the solution. It's clear that urgent action is needed to end this fraud epidemic and prevent it from becoming a crime without consequence.





# EXECUTIVE SUMMARY

Fraud has become the single biggest form of crime affecting people in the UK and yet our policing institutions have not caught up with the scale of that change. We have a 1960s local policing structure trying to fight a 21st century cyber-enabled cross border crime. As a result, the police are achieving limited success and victims are receiving too little by way of service.

In 2024 4.1 million people were victims of fraud which alone constituted 43 per cent of all crime affecting those aged over 16 in England and Wales (ONS, 2025). The UK government's National Fraud Strategy<sup>1</sup> estimates that fraud costs UK society £6.8 billion a year (UK Government, 2023).

Fraud is not a 'victimless crime'. According to a recent Police Foundation survey 58 per cent of fraud victims in two police force areas felt worried, 56 per cent experienced stress, 46 per cent felt vulnerable and unsafe and 18 per cent experienced depression.

Taking the above statistics into account, the police response to fraud does not match the level of threat to the public. In England and Wales less than a third of frauds are reported to the police. Of those that are reported just 3.5 per cent are deemed suitable for a police investigation (Doig et al., 2024). Most victims reporting fraud to the police receive no service at all.

In a 2025 survey<sup>2</sup> of police officers and staff carried out for this paper, we found that:

- 67 per cent of police workers surveyed said that businesses (e.g., banks, retailers, online platforms) hold the most responsibility for reducing fraud.
- 88 per cent of police workers surveyed disagreed with the statement – "Police officers have sufficient resources (time, personnel, budget) to tackle fraud".

- 44 per cent of police workers surveyed don't think the police are doing a good job when it comes to tackling fraud.
- Half (51 per cent) don't believe police officers have the skills to investigate fraud.
- 5 per cent agreed fraud was a victimless crime provided no money was lost.
- 67 per cent agreed fraud should be handled by a single national policing body.
- 37 per cent aren't clear which agency should be investigating fraud cases.
- 41 per cent of police workers surveyed think fraud is low priority for UK police forces compared to other crimes.

The police response to fraud is hampered by:

1. *A lack of resources.* As of March 2021 there were just 866 economic crime officers in English and Welsh police forces, including regional asset recovery teams. This constitutes a mere 0.64 per cent of the total police workforce to respond to 42 per cent of crime.
2. *A predominantly local response to a cross-border crime.* While fraud has become a cross border 'distance crime', often originating overseas, the operational response to it remains largely local. In practical terms there are limits to what local forces can do to investigate complex fraud. Fraud cases are also rarely prioritised over other local crimes such as sexual and violent crimes.
3. *A lack of an ability to identify harm and seriousness.* Fraud cases are disseminated on the basis of the viability of a potential investigation rather than because of an assessment of the harm caused to the victim. There is currently no common framework which would allow the police to triage and prioritise fraud cases based on harm.

1. This strategy was adopted by the previous Conservative government and, while it remains live, is under review by the new Labour government.
2. Figures included are based on a recent survey commissioned by Virgin Media O2 and conducted by YouGov Plc. Fieldwork was undertaken between 31st March - 4th April 2025. The survey was carried out online. A total sample size of 252 adults who work in the police.

4. *A lack of skills.* The police workforce currently lacks the skills to properly investigate fraud. In 22 out of 32 police forces surveyed, generalist local investigation teams dealt with all or most fraud investigations, despite 86 per cent of officers believing fraud should be dealt with by specialists.
5. *The response remains too focused on arrests and prosecutions.* In a world where most fraud originates overseas there needs to be more to the law enforcement approach than trying to achieve traditional criminal justice outcomes. In particular more should be done to proactively disrupt the organised crime networks perpetrating fraud.
6. *There is a lot of data on fraud but insufficient insight is being generated from it.* From the volumes of crimes reported to a variety of different agencies and the wealth of data that exists in the private sector in relation to fraud there is a vast amount of intelligence that could be used to help inform the police response, support investigations and target proactive operations. Yet while there have been improvements in data sharing this could go much further.

The report makes the following recommendations to tackle these problems:

#### **Recommendation 1**

*The government should create a national Crime Prevention Agency charged with taking the national and international action necessary to prevent fraud and cybercrime.*

#### **Recommendation 2**

*Local elected Mayors and Police and Crime Commissioners should develop local fraud prevention strategies, taking a public health approach to building up our collective defences.*

#### **Recommendation 3**

*The City of London Police should be given direct tasking powers in relation to local and regional fraud investigation teams. If the government moves ahead with bringing organised crime and counter-terrorism together in a single body, then fraud policing should also become part of that single national body.*

#### **Recommendation 4**

*There should be a stronger network of Regional Economic Crime Hubs to enable more effective investigation of complex cyber-enabled frauds. These should be tasked directly by the national lead body. Over time the aim should be to develop Regional Economic Crime Super Hubs bringing in a range of enforcement and regulatory bodies and the private sector.*

#### **Recommendation 5**

*The role of local policing in fraud should be clarified. It should have primary responsibility for local frauds where the fraud has been perpetrated face to face and it should play a role in providing crime prevention advice to individuals and business through neighbourhood policing teams.*

#### **Recommendation 6**

*Private companies should be legally required to share data relevant to the prevention and investigation of fraud. Public and private sector data should be brought together in a new National Anti-Fraud Data Centre to enable a better strategic assessment of threat and to support investigations and live operations.*

#### **Recommendation 7**

*There should be a national economic crime workforce strategy to ensure a future pipeline of recruits into the service with the necessary skills and knowledge. There should be an economic crime specials programme to seek to make best use of much needed skills that exist in the private sector.*

#### **Recommendation 8**

*Funding for fraud and economic crime policing should be ring fenced and distributed through the national lead body. Over the next two spending reviews investment in fraud, cyber and economic crime capabilities should be increased.*



# 1. INTRODUCTION

In the last 20 years fraud has been transformed from a largely white-collar crime affecting big business to a volume crime affecting millions of people. The main enabler of this change has been the internet, which means that fraudsters are now able to perpetrate scams on an industrial scale.

At the same time our policing institutions were built for a different era. Local police forces were created to tackle crime committed by local criminals against local victims. They were not designed and nor do they have the skills or resources to pursue fraudsters operating across local and international borders.

This paper asks what we need to do to design a police response to fraud that is commensurate with the scale and nature of the threat. In doing so the author recognises that the best way to reduce fraud is to prevent it from happening in the first place. With 70 per cent of fraud originating from overseas or having an international element, the majority of fraudsters are beyond the reach of UK law enforcement. In that context we need to do much more to reduce the opportunities to commit fraud, to raise public awareness of the risk posed and to reduce the harm caused to victims. In short, we need to significantly strengthen our defences against fraud, and that requires action way beyond policing.

Nevertheless, policing has a critical role to play. It is important that we seek justice for those victims most seriously impacted by fraud. Even where fraudsters are overseas the police and partners can disrupt their activities and make it harder for them to operate. Successful police investigations send a message to those involved in fraud that they run the risk of being caught. And where fraud

is committed by local offenders there is no reason why the police should not pursue it with the same vigour as other local crimes.

This paper does three things. First, it lays out the context by describing the scale and nature of fraud and the harm it causes. Second, it makes the case that our current policing response to fraud is inadequate. Third, it describes how our policing institutions could be re-designed so that they match up to the significance of the fraud epidemic we face.

## 1.1 METHODOLOGY

The paper is based on the following research:

1. A review of the recent academic and policy literature on the UK police response to fraud.
2. Interviews with 15 senior police, government and stakeholder leaders working on the UK's fraud response. These included senior leaders from City of London Police, the National Crime Agency, the Home Office, Parliament, Cifas, Regional Organised Crime Units and local police forces.
3. A survey of 252 police officers and staff undertaken by YouGov between 31st March and 4th April 2025.
4. Previous Police Foundation research into the harm caused to victims of fraud, the profile of fraud offenders, the nature of international organised fraud and the role of online anonymity as an enabler of fraud. This research is brought together on our Online Fraud Research Hub <https://www.police-foundation.org.uk/online-fraud-research-hub/>



## 2. CONTEXT

Fraud can be defined in general terms as “obtaining something of value or avoiding an obligation by means of deception” (Duffield and Grabosky, 2001). INTERPOL has emphasised the importance of intent in defining fraud, describing it as the “aim at the procurement of a financial gain through deliberate, deceitful actions against individuals and to their detriment” (INTERPOL, 2024). The 2006 UK Fraud Act defines fraud as a criminal offence committed by false representation, failing to disclose information or abusing a position of trust, with the aim of gaining an advantage or causing loss (Fraud Act, 2006).

While in the past fraud tended to be a white-collar business crime with limited impact on most members of the public, today fraud affects millions.<sup>3</sup> In this section we set the context for the rest of the paper by describing the volume and costs of fraud, the harm it causes to victims and some of the key characteristics of fraud that should structure our response to it.

### 2.1 THE VOLUME AND COST OF FRAUD

Most people in the UK receive emails or phone calls from fraudsters. It is no exaggeration to say that attempted scams have become part of the ‘background noise’ of everyday life. In 2024 4.1 million people were victims of fraud - up 33 per cent on the previous year - and fraud alone constituted 43 per cent of all crime affecting those aged over 16 in England and Wales (ONS, 2025).<sup>4</sup> In the same year frauds reported to and recorded by the police totalled 1.3 million or 32 per cent of total fraud (*ibid*).

The UK government’s National Fraud Strategy<sup>5</sup> estimates that fraud costs UK society £6.8 billion a year, including direct financial loss, the impacts on people’s health and productivity and the costs of the police response (UK Government, 2023).

### 2.2 THE HARM CAUSED BY FRAUD

Fraud is very far from the stereotype of a ‘victimless crime’. The National Fraud Strategy, set by the previous government, states that 18 per cent of fraud victims in 2022 had been victims before, although an empirical study from the West Midlands police force area suggest this could be as high as 42 per cent (UK Government, 2023; Levi et al., 2023). Industry sources estimate that average personal losses from authorised frauds (where the victim approves a payment) could be as much as £3,000 per person (UK Government, 2023).

Fraud is a very broad category of crime, containing within it many distinct *modus operandi*. As such the harms caused by fraud are varied. Some people don’t lose any money (because they are compensated by their bank for instance), while others lose hundreds of thousands of pounds.<sup>6</sup>

The impact on victims goes well beyond financial loss. Crime Survey for England and Wales data shows that almost three quarters of victims experience some kind of emotional impact from being defrauded (*ibid*). Action Fraud, the UK’s police fraud reporting centre, deals with 300 calls a year where someone is deemed at risk of suicide (*ibid*).

3. We should distinguish volume fraud affecting individuals and businesses from public sector fraud, which is also significant in terms of volume and cost but is a distinct challenge and not the subject of this paper.
4. The Crime Survey for England and Wales does not include sexual offences in its aggregate crime figures. Offences against children under the age of 16 are also excluded.
5. This strategy was adopted by the previous Conservative government and, while it remains live, is under review by the new Labour government.
6. We should note that banks vary in their approach to compensation. New regulations mean that in cases of Authorised Push Payment (APP) fraud banks are obliged to compensate up to £85,000 within five days.



A recent survey of fraud victims<sup>7</sup> conducted by the Police Foundation and the University of Portsmouth found that, as a result of fraud:

- 92 per cent experienced emotional or mental health symptoms.
- 57 per cent experienced a physical health symptom.
- 63 per cent experienced behaviour change.

In terms of specific impacts:

- 58 per cent felt worried.
- 52 per cent worried they might be re-victimised.
- 56 per cent experienced stress.
- 46 per cent felt vulnerable and unsafe.
- 46 per cent felt anger.
- 40 per cent felt guilt and shame.
- 44 per cent said it made them less trusting of others.
- 32 per cent experienced anxiety.
- 18 per cent experienced depression.
- 5 per cent experienced feelings of self-harm.
- 45 per cent reported problems sleeping.
- 24 per cent reported excessive tiredness.
- 10 per cent reported high blood pressure.
- 4 per cent reported heart problems.
- 19 per cent said they had become socially withdrawn.
- 3 per cent reported excessive use of drugs and alcohol.<sup>8</sup>

## 2.3 THE KEY CHARACTERISTICS OF FRAUD

While fraud is a large and diverse category of crime it is worth highlighting some important general characteristics that should structure society's response to it.

### **Fraud is a cross-border crime**

According to the National Fraud Strategy 70 per cent of fraud either originates overseas or involves some international element (UK Government, 2023). Fraud also crosses police force boundaries within this country. A Police Foundation examination of frauds allocated by the National Fraud Intelligence Bureau (NFIB) for investigation in 2016-17 found that 78 per cent involved a victim and an offender who did not live in the same police force area (Skidmore et al., 2018).

We should note of course that some types of fraud may resemble more traditional local crimes. The same Police Foundation study found that the victim and offender resided in the same police force area in 56 per cent of corporate employee frauds, 45 per cent of retail frauds, 54 per cent of abuse of position of trust frauds and 35 per cent of door-to-door sales frauds.

### **Cybercrime is a key enabler of fraud**

The internet is a key enabler of fraud and explains why fraud is now committed on an industrial scale.

A Police Foundation study of 64,857 fraud cases passed on for enforcement action in 2016-17 found that:

- 69 per cent included at least one indicator of cybercrime.
- 27 per cent were intrinsically cyber-enabled.
- 43 per cent were cases where first contact was made online.
- 49 per cent involved money being transferred from an online bank account (Skidmore et al., 2018).

7. The survey was distributed to every fraud victim resident in two neighbouring police regions in England and Wales. The sample included victims who reported to the police during a continuous 14-week period.

8. All data from Skidmore et al., forthcoming.

The 2018 Crime Survey for England and Wales found that 54 per cent of fraud had a link to cybercrime, defined as fraud in which the internet or any online activity were involved in any aspect of the offence. Frauds that used bank or credit accounts linked to the victims were by far the most prevalent type of fraud experienced (69 per cent) and 44 per cent of this category was classified as cybercrime (ONS, 2018).

A lot of fraud is recorded by the business sector (especially financial services). From data provided by Cifas, nearly two-thirds (65 per cent) of over 320,000 frauds reported by industry in 2016-17 were perpetrated using the internet. The vast majority was comprised of identity fraud which makes up 65 per cent of all fraud recorded by industry and was predominantly perpetrated using the internet (87 per cent) (Skidmore et al., 2018).

### **Fraud is often perpetrated by organised crime groups**

An 'organised criminal group' is defined in article 2 (a) of the Organised Crime Convention as a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with the Convention, in order to obtain, directly or indirectly, a financial or other material benefit (UNODC, 2024).

There is no doubt that on that definition a considerable amount of fraud is perpetrated by organised crime groups. Nonetheless as a recent United Nations Office on Drugs and Crime (UNODC) paper points out, fraud offending looks different from the stereotypical image of organised crime: it is about monetary theft rather than the

production or distribution of illegal goods, it is generally carried out remotely unlike traditional forms of organised crime, it often relies on victims willingly providing access to funds instead of involving force or coercion and it is often perpetrated within legitimate organisations and occupations (UNODC, 2024).

Just as fraud is varied so too are the ways in which organised crime groups work to perpetrate it. They can operate largely locally or across international borders. There can be varying relationships between co-offenders, ranging from more remote transactional networks (in which people with specialist skills may be paid for providing a particular service) to groups with durable social bonds. In some cases, the profits from fraud will simply stay with the fraudsters, while in others they will be used to support other criminal activities, including terrorism (*ibid*).

### **Fraud is a diverse crime type**

It is worth underlining a point made several times above. Fraud, like theft and violence, is a broad and overarching category that encompasses very different types of crime. The most common frauds often involve relatively small personal losses, with the money being made by repetition at scale. Other types of fraud such as investment scams can involve a personal loss of hundreds of thousands of pounds. Some are undertaken by transnational networks, others by local door to door scammers. Our response to fraud, therefore, needs a 'gearing' quality, to be able to respond adequately to different patterns of offending and victim experience.





# 3. THE POLICE RESPONSE TO FRAUD

The police response to fraud does not match the level of threat to the public. In 2024 there were 4.1 million frauds committed against adults over the age of 16 in England and Wales. Less than a third of frauds are reported to the police. Of those that are reported just 3.5 per cent are deemed suitable for a police investigation (Doig et al., 2024). Most victims reporting fraud to the police receive no service at all.

Turning to criminal justice outcomes, a mere 4,406 offenders were sentenced for fraud in the year to June 2021 with 1,120 receiving a prison sentence (*ibid*). While some of those will have committed multiple offences, that nonetheless represents a massive level of attrition in terms of the numbers of frauds reported and the numbers that actually took place.

44 per cent of police workers we surveyed didn't think the police are doing a good job when it comes to tackling fraud.

One academic specialist in fraud interviewed for this paper queried whether the overall police approach is generating tangible outcomes for victims:

*"If an arrest doesn't lead to a trial or prosecution, what is the point of it? Does this activity have any benefit? What's it all for? A nothing outcome is a really bad outcome. I am deeply suspicious of intelligence empire building without any appreciable results."*

So, why does the police response to fraud seem so wildly out of kilter with the volume and seriousness of the crime? From our reading of the literature, previous research, interviews with senior law enforcement stakeholders and our YouGov survey of police officers and staff we identify six problems with fraud policing in the UK, which any package of reforms will need to address.

## 3.1 A LACK OF RESOURCES

As of March 2021 there were just 866 economic crime officers in English and Welsh police forces, including regional asset recovery teams. This constitutes a mere 0.64 per cent of the total police workforce to respond to 40 per cent of crime.

In the same year Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) concluded there were

*"...too few examples of the police and other agencies coming together to prevent and protect the public from fraud; there are far too few officers working on it; there are far too few investigations into it; and there are far too few criminals brought to justice. All this leads to far too few victims receiving the service, and the justice, they want and are entitled to expect" (HMICFRS, 2021).*

88 per cent of police workers we surveyed disagreed with the statement – "Police officers have sufficient resources (time, personnel, budget) to tackle fraud".

## 3.2 A PREDOMINANTLY LOCAL RESPONSE TO A CROSS-BORDER CRIME

While fraud has become a cross border 'distance crime', often originating overseas, the operational response to it remains largely local. While the reporting and analysis is done centrally via the City of London Police, which runs Action Fraud and the NFIB, most investigations are then disseminated to local forces (92 per cent in 2016-17, see Skidmore et al., 2018). Most of those that are disseminated result in no further action.

Why do local forces do so little with the fraud cases disseminated to them? There are a number of reasons. First, complexity. Fraud investigations, even with good local leads, may lead investigators into complex territory, with challenges securing evidence

and negotiating cooperation across borders. Local forces often feel they cannot justify the level of resource required to bring such cases to a conclusion.

Second, fraud struggles to compete with other more pressing local concerns, such as sexual and violent crime. Understandably these physically harmful crimes tend to take precedence. 41 per cent of police workers we surveyed thought fraud is low priority for UK police forces compared to other crimes.

Third, the absence of a local victim means that police forces have less commitment to resolving fraud cases than they do with other offences. When a fraud is disseminated to a force it is because the suspect resides there. The victims are likely to be spread out across the country and may live in other countries. This lack of a local victim to whom the force is accountable for delivering a service reduces the sense that this is ‘our crime’ and one that a force is morally obliged to pursue (Skidmore et al., 2018).

Moreover, the agency that owns the problem of fraud at the centre (the national lead force, City of London Police) has no mandate to ‘task’ local police to take on investigations. As one senior police leader told the author:

*“We need more tasking from the centre to drive consistency. To make the existing system more effective we need mandation, standards and direct tasking.”*

While fraud is in the Strategic Policing Requirement (SPR), which is supposed to ensure local forces are delivering against national security threats, practically nothing is done if a force does not meet its requirements under the SPR. As one senior police leader told the author, “The SPR has no teeth.” A senior National Crime Agency (NCA) official added:

*“There is a need for greater clarity as to what is done locally, regionally and nationally. We need to have some sharpening there.”*

In our 2025 survey of police officers and staff 37 per cent weren’t clear which agency should be investigating fraud cases.

So, we have a cross-border crime whose overall costs tend to manifest nationally but for which our primary mode of operational delivery and the

main locus of decision-making and accountability remains local. In that context it is unsurprising that fraud investigations are not prioritised.

### 3.3 A LACK OF AN ABILITY TO IDENTIFY HARM AND SERIOUSNESS

Fraud cases are disseminated on the basis of the viability of a potential investigation rather than because of an assessment of the harm caused to the victim. There is currently no common framework which would allow the police to triage and prioritise fraud cases based on harm. Many forces simply do not investigate frauds that fall below a crude level of financial value irrespective of the impact on the victim. Given that harm assessment is the core metric for determining priorities in local policing this is a major problem for ensuring high harm fraud cases are adequately resourced.

### 3.4 A LACK OF SKILLS

The police workforce currently lacks the skills to properly investigate fraud. In its 2018 report (Skidmore et al., 2018) the Police Foundation found that in 22 out of 32 police forces surveyed, generalist local investigation teams dealt with all or most fraud investigations. Only a small number reported that Economic Crime Teams dealt with all or most fraud investigations. It is also notable that many specialist teams had a limited role in investigating fraud, with respondents reporting local cybercrime (75 per cent), financial investigation (61 per cent) or regional teams (79 per cent) conducting few or no fraud investigations.

This may have changed somewhat since then with the recruitment of 300 additional economic crime officers as set out in the previous government’s National Fraud Strategy, but given the volumes of cases this investment is unlikely to have broken the overall pattern.

In a survey of strategic leads for fraud, 69 per cent felt that a lack of knowledge in the workforce was one of the most challenging factors in delivering local fraud investigation. A high proportion of the

strategic leads in the police believed insufficient training was provided to practitioners in their local investigation (61 per cent), neighbourhood (62.5 per cent) or response teams (71 per cent) (Skidmore et al., 2018). A senior Regional Organised Crime Unit (ROCU) officer told the author:

*“Some DIs and DCIs are not even aware of the fraud investigation model. They’ve never heard of it.”*

In our workforce survey 81 per cent agreed that fraud policing requires a different set of skills to other crimes, and most agreed that they needed more training to deal with fraud (78 per cent) and cybercrime (81.5 per cent) (Skidmore et al., 2018). In the Police Foundation’s 2025 survey half (51 per cent) do not believe police officers have the skills to investigate fraud.

In interviews conducted for this paper there was some push back against seeing fraud investigations as too complex or specialist. Some interviewees felt that there was still a role for local uniformed policing but that the workforce needed training and support. One said:

*“Every PC should know how to take down a website, and should know what intelligence to look for.”*

An academic specialist commented:

*“There are very simple local frauds that every police officer should be able to deal with.”*

A senior ROCU officer commented:

*“It is seen as specialist and hugely complicated and for the headquarters team. But there are dangers in specialising it, it should be everybody’s business. It’s not complicated. It’s pimped up theft.”*

### 3.5 THE RESPONSE REMAINS TOO FOCUSED ON ARRESTS AND PROSECUTIONS

As a recent RUSI paper on economic crime policing stated, “the government’s strategy remains fixated on outdated metrics of arrests and prosecutions” (Wood and Baxter, 2022). The authors’ point, which is surely correct, is that in a world where most fraud originates overseas there needs to be more to the law enforcement

approach than trying to achieve traditional criminal justice outcomes. Most of these offenders will not end up in British courts. As one academic commentator told the author:

*“We are never going to investigate our way out of it. We need more prevention and more disruption.”*

The Fraud Targeting Cell, a joint NCA and City of London Police initiative, should facilitate more proactive work, by enabling sharing of multi-agency intelligence data across the fraud network.

There is work ongoing across policing and other agencies in terms of offensive cyber activity, although information about this is generally not in the public domain. With respect to offensive cyber activity one senior police leader acknowledged to the author “there is more that could be done.”

The UK government’s Economic Crime Plan notes a recent increase in the amount of criminal assets seized to £354 million, the highest on record. But given estimates of overall financial losses of £3.1 billion a year, there is clearly scope to go further (UK Government 2022, 2023).

### 3.6 THERE IS A LOT OF DATA ON FRAUD BUT INSUFFICIENT INSIGHT IS BEING GENERATED FROM IT

From the volumes of crimes reported to a variety of different agencies and the wealth of data that exists in the private sector in relation to fraud there is an ocean of data that could be used to help inform the police response, support investigations and target proactive operations.

There has been progress in this space. The Joint Fraud Taskforce has enabled greater sharing of information between the police and the private sector. A new Online Crime Control Centre will bring together public and private sector data, including law enforcement intelligence, enabling real time responses and informing a strategic response to emerging threats. As one police leader said:

*“Action Fraud data will be at its core, but it could expand to deliver a wider range of outputs and outcomes.”*



However, there could be more data fusion to make the best of the information the public and private sectors collectively possess on fraud. As one police leader said:

*"The law allows data sharing across organisations, but there are a lot of negotiations. The banks will share with us, but they don't like to share with each other, because of perceived risks to customers data and because of a fear it will put them at a commercial disadvantage."*

They added:

*"We need inter-sector data sharing. For example, Meta will say 'we have the story, but the banks have the transactions'."*

An academic specialising in fraud pointed out that the private sector resource focused on fraud dwarfs what exists within public policing:

*"Lloyds Bank has 8,000 staff working on economic crime. That is a huge capability. We need to bring them into the fold in an effective way. That includes data and intelligence sharing."*

# 4. RE-DESIGNING OUR POLICE INSTITUTIONS TO TACKLE FRAUD

In this final section we set out what we could do to redesign our policing institutions so they are much better equipped to tackle fraud.

## 4.1 THE IMPORTANCE OF PREVENTION

Because fraud is high volume and much of it originates overseas there are limits on what policing is able to do to counter it. The most effective way of reducing levels of fraud is to build up our individual and third-party defences. Most of the effort to do this will be in the Prevent and Protect space and much of it far from the remit of the police. 67 per cent of police workers surveyed said that businesses (e.g., banks, retailers, online platforms) hold the most responsibility for reducing fraud.

It is worth highlighting some of the ways in which this might be done, before we go on to explore how the police response could be improved.

One of the major problems in our crime prevention landscape is that nobody truly ‘owns’ the problem of preventing crimes like fraud, and hence efforts tend to be ad hoc, poorly coordinated and project dependent. To deliver a more systemic and strategic approach the Police Foundation has called for the establishment of a national Crime Prevention Agency (CPA).

The role of the CPA would be to:

- Provide an independent assessment of the state of crime and related harms and the preventative measures required to tackle them.
- Provide strategic advice to the government on the policies required to improve public safety. In particular, it would develop guidance and regulations for priority sectors.

- Establish national level partnerships in those industries and sectors where concerns are highest, and ensure these partnerships are sustained and effective, with their own preventative strategies. In particular, a core focus should be on bringing down the volumes of fraud and cybercrime.
- Develop and maintain key international relationships, such as with US-based tech companies, to ensure ongoing dialogue, data sharing and joint work.
- Oversee strategic communications around crime prevention so that the public receive consistent messages in areas where behaviour change is required.
- Look to the future to understand what new products and technologies are in development and what their criminogenic impact might be. This should lead to something analogous to an ‘early warning system’ and prompt earlier intervention to ensure crime is designed out at source.
- Provide a research function that would work with universities and practitioner groups to support primary research, systematic reviews, evaluations and practice guidance. This would develop the evidence base around effective interventions and share findings in a way that is useful to practitioners.

The CPA would have a focus on reducing fraud and cybercrime, which require national action and the leveraging of the UK’s international relationships. It could be made the core agency accountable for a national fraud reduction target, such as reducing fraud by 10 per cent by the end of the parliament.<sup>9</sup>

9. This was the target adopted in the previous government’s Fraud Strategy.

### Recommendation 1

*The government should create a national Crime Prevention Agency charged with taking the national and international action necessary to prevent fraud and cybercrime.*

Finally preventing fraud also requires a bottom-up community oriented approach. Levi et al., 2023 argue convincingly that a ‘public health approach’ could be taken to fraud prevention locally, similar to the way bodies such as Violence Reduction Units are taking a public health approach to tackling violent crime. This approach would focus on building up personal and third-party defences against fraud, potentially coordinated by Police and Crime Commissioner or elected Mayor offices.

Such an approach would be characterised by:

- Data sharing and analysis to enable the targeting of vulnerable and repeat victims to help build up their resilience.
- Awareness raising campaigns utilising trusted local third-party institutions.
- The use of Police Community Support Officers (PCSOs) to provide cyber security reviews to individuals and small businesses.
- Wider training of frontline public service professionals and others to provide simple cyber-security and counter-fraud advice, particularly where they interact with susceptible groups.

### Recommendation 2

*Local elected Mayors and Police and Crime Commissioners should develop local fraud prevention strategies, taking a public health approach to building up our collective defences.*

## 4.2 ORGANISATIONAL REFORM

The fundamental problem with the way our fraud policing system is set up is that we are trying to fight a cross border cyber-enabled crime predominantly through a local police force system designed in the 1960s.

There have been reforms to this system in recent years, including the establishment of Action Fraud

and the NFIB within the City of London Police to enable central reporting and triaging of cases, the creation of the National Economic Crime Centre within the NCA to coordinate intelligence and the recent strengthening of regional fraud investigation teams.

The latest innovation, announced by the previous government, was the establishment of the so-called National Fraud Squad. However, it seems this is merely a wrapper label for increased numbers of fraud specialists working within the existing organisations (the NCA, the City of London Police and the Serious Fraud Office), rather than the establishment of a new fraud policing body. Tellingly when the author asked a senior police officer what exactly the National Fraud Squad was, this officer simply laughed.

So, what needs to be done to reorganise the fraud policing landscape so that we develop a stronger response?

### The national lead body

We need a single national body that can lead and coordinate our response to fraud, based on a comprehensive strategic intelligence picture. This is backed by the members of the police workforce we surveyed, 67 per cent of whom felt fraud should be handled by a single national policing body. Currently there is a degree of overlap and duplication between the respective roles of the NCA and the City of London Police and crucially the City of London Police lacks any levers to direct the operational response within the wider policing landscape.

There are three options for reform.

The first is to continue to expand and develop capability through **the national lead force**, the City of London Police. This has the benefit of going with the grain of recent developments, which have seen the City of London Police gradually accumulate new capabilities over time, including the imminent relaunch of Action Fraud. The City of London Police also has the advantage of strong private sector relationships, particularly with banking. As one senior City of London Police officer told the author “the relationship with the private sector is unique to this space, that’s where the reductions in fraud will

come from. Integration and relationships with the private sector are more important than integration with the rest of policing.”

If this were maintained however, the City of London Police would need to become a proper command structure, with direct tasking powers in relation to both regional fraud teams and local forces. Greater public awareness of its national lead responsibility could be gained by re-branding it as a National Fraud Headquarters.

The disadvantage of this approach is that it retains current confusion and overlap over the role of the City, which leads on fraud, and the NCA, which has responsibility for economic and cybercrime. It also appears at odds with the government’s wider police reform agenda, which envisages a new National Centre of Policing. Ministers have aspirations that this might over time become a ‘44th force’ or a new national police force, working with the existing 43 local forces, but providing support and enabling capabilities to local policing, while also bringing together counter-terrorism and serious organised crime into a single national operational body. The advantage of convergence and even a merger is that there are so many overlaps and interdependencies in the fight against terrorism and organised crime, and in the fight against fraud and cybercrime, that it would make sense to build capabilities in the same place.

A second option therefore is to move the national leadership for fraud into **a new national policing body**. This would support cross sector working across a range of threats. It would facilitate a shared intelligence picture across the full range of serious crime threats. It would make little sense to have counter-terrorism and serious and organised crime (including economic and cybercrime) brought together, but to leave fraud as a standalone body.

A third option is to establish a **new national fraud force**. Some interviewees raised concerns that if fraud were subsumed into a larger body like the NCA or a national police force it would be deprioritised compared to other serious and organised crime threats. There is also a case for saying that fraud sits somewhat uncomfortably in a serious organised crime body, because while it

is generally organised, a lot of volume fraud is not serious, in that the personal losses are low.

The author recommends that gradually the national leadership responsibility should be brought into the same policing body as counter-terrorism and serious and organised crime (including economic and cybercrime). Given the interdependencies between the different threat areas, particularly the link between fraud and cyber, it makes little sense to keep fraud outside such a combined structure. A shared data and intelligence picture across these serious and cross border threats would generate real operational benefits.

If this were to happen, it should happen gradually as the current police reform programme progresses. It would make sense in the meantime to retain leadership and coordination responsibilities within City of London Police, but provide it with the ability to task regional and local teams.

Whatever the organisational host, the national lead body must have:

- Strong partnerships with the private sector, including data fusion to bring together all the information held on fraud across law enforcement, regulators and the private sector.
- Ownership of a common threat picture and strategic intelligence collection.
- Direct tasking powers in relation to regional and local fraud investigation teams.

### **Recommendation 3**

*The City of London Police should be given direct tasking powers in relation to local and regional fraud investigation teams. If the government moves ahead with bringing organised crime and counter-terrorism together in a single body, then fraud policing should also become part of that single national body.*

### **Regional economic crime hubs**

The recent expansion of regional fraud teams, based in the Regional Organised Crime Units, is very welcome. This is because more complex, cyber-enabled and cross border frauds benefit from specialist expertise (particularly in areas like securing evidence from overseas third parties



and navigating international law enforcement cooperation). These cases should not be handed to local police forces who lack the skills and incentives to pursue them. These regional fraud teams should be expanded further as resources allow. They should be directly tasked by the national lead body.

In the future these units could be developed into regional economic crime ‘super-hubs’, as envisaged in Wood and Baxter (2022). These hubs would bring together policing, government, statutory bodies such as HMRC and the Crown Prosecution Service and the private sector (with an ability to share information in real time to prevent crime).

#### **Recommendation 4**

*There should be a stronger network of Regional Economic Crime Hubs to enable more effective investigation of complex cyber-enabled frauds. These should be tasked directly by the national lead body. Over time the aim should be to develop Regional Economic Crime Super Hubs bringing in a range of enforcement and regulatory bodies and the private sector.*

#### **Local policing**

Local police forces have a role to play in tackling fraud, though at the moment this role is confused and poorly conceived. They are not best placed to be carrying out investigations into complex, cyber-enabled and cross border frauds, which are better handled regionally or nationally.

However, they should be responsible for:

- Investigating local frauds where it seems highly likely that the offender and victim both reside in or near the force area (such as when the fraud has been perpetrated face to face rather than online, as with doorstep fraud cases).
- Playing a role in a local ‘public health’ approach to strengthening people’s defences against fraud. For example, PCSOs are ideally suited to providing cyber-security advice to local small businesses and to identifying and visiting vulnerable and repeat victims.

#### **Recommendation 5**

*The role of local policing in fraud should be clarified. It should have primary responsibility for local frauds where the fraud has been perpetrated face to face and it should play a role in providing crime prevention advice to individuals and businesses through neighbourhood policing teams.*

### **4.3 COLLABORATION WITH THE PRIVATE SECTOR**

Tackling fraud requires extensive collaboration between law enforcement and the private sector. It should be emphasised that most work to counter fraud takes place in the private sector, in for example financial institutions, telecommunications companies and in the cyber-security sector. Two examples of the private sector supporting work to identify fraud are given in Case Studies A and B below.

#### **Case study A: Private industry cyber-security and AI-enabled data analytics<sup>10</sup>**

Technology company IBM manages a vast technological infrastructure with a global reach. The IBM X-Force Exchange platform monitors huge volumes of cyber-security events across more than 130 countries and collects real-time intelligence on a range of cyber threats that includes spam and phishing attacks and data on malicious IP addresses. They have the technical and human resources to analyse vast amounts of data to produce intelligence that can be shared with state agencies and other private entities.

They have developed advanced techniques in data analytics that can be used as investigative tools to detect patterns and anomalies that indicate suspicious or fraudulent activities. This includes AI-powered tools that the police can use to monitor transactions in financial intelligence.

10. Lilli, E. (2021) Redefining deterrence in cyberspace: Private sector contribution to national strategies of cyber-deterrence, Contemporary Security Policy, 42(2), pp.163-188; <https://exchange.xforce.ibmcloud.com/hub/>

### Case study B: Microsoft Digital Crimes Unit<sup>11</sup>

Microsoft operates a vast data network and cloud infrastructure. In monitoring activity across their systems, they produce intelligence and evidence related to digital fraud and cybercrimes. The Microsoft Digital Crimes Unit collaborates with law enforcement agencies such as the FBI, Europol, Interpol, and the national cybersecurity units in various countries. Furthermore, this team works in tandem with law enforcement to investigate and disrupt malware-facilitated cybercrime such as fraud, by taking control of, or shutting down cyber-infrastructure; for example, they worked with international law enforcement in 2020 to disrupt the Trickbot botnet which was targeting organisations with fraud and other illegal activities. Other examples include joint operations to monitor, disrupt, and take down online criminal marketplaces, such as those hosting stolen financial credentials.

One vital focus for collaboration between the police and the private sector on fraud relates to intelligence sharing. The private sector possesses vast amounts of data that contain vital fraud intelligence.

While there has been some progress on data sharing, particularly in terms of the banks sharing information with the police, there is still a challenge of encouraging private companies to share data with each other. As one senior police leader told us: “There are still concerns about privacy and about commercial confidentiality. We may need greater mandation.”

Additionally, the overseas based tech sector has been criticised for not playing its part in sharing data and intelligence, as well as taking action to remove content related to fraud. Many fraudulent advertisements for example are promoted on social media platforms. As one parliamentarian told us: “The tech sector should be considered to be in the last chance saloon on fraud”.

There is therefore a case for legal mandation, with a new legal requirement on companies to share

fraud data, so that we can build up a much more powerful shared picture through a National Anti-Fraud Data Centre. This should enable not just a stronger strategic assessment of the threat, but should also generate operational insights, including in real time.

#### Recommendation 6

*Private companies should be legally required to share data relevant to in the prevention and investigation of fraud. Public and private sector data should be brought together in a new National Anti-Fraud Data Centre to enable a better strategic assessment of threat and to support investigations and live operations.*

## 4.4 SKILLS

The huge rise in public facing fraud requires a police service that has much greater knowledge of the digital world and the financial system, alongside skills in areas such as data science, digital forensics and financial investigation. The challenge is that it is very difficult for the police and the public sector more widely to compete with the private sector for these specialist skills.

The police service needs a national strategy for its economic crime workforce to try to attract and retain people with the right skills to meet current and future threats. This should be coordinated through the new National Centre of Policing. There will need to be innovative partnerships with the private sector, such as through an expanded cyber specials programme, which can bring in private sector expertise to work on investigations and proactive operations.

#### Recommendation 7

*There should be a national economic crime workforce strategy to ensure a future pipeline of recruits into the service with the necessary skills and knowledge. There should be an economic crime specials programme to seek to make best use of much needed skills that exist in the private sector.*

11. Ibid; <https://news.microsoft.com/on-the-issues/2022/05/03/how-microsofts-digital-crimes-unit-fights-cybercrime/?msockid=1cd5f80b1f4f6d37271cecd21ef46c83>

## 4.5 RESOURCES

There should be a single ring-fenced fund for tackling fraud and economic crime, distributed through the national lead body. This would fund not just the activities of the lead body but also the regional hubs, which currently operate under enormous financial uncertainty, inhibiting the ability to plan and recruit and retain staff. Over the next two spending reviews the country needs to significantly increase its investment in tackling fraud, cyber and economic crime.

### **Recommendation 8**

*Funding for fraud and economic crime policing should be ring fenced and distributed through the national lead body. Over the next two spending reviews investment in fraud, cyber and economic crime capabilities should be increased.*

# 5. CONCLUSION

Fraud has become the single biggest form of crime affecting people in the UK and yet our policing institutions have not caught up with the scale of that change. We have a 1960s local policing structure trying to fight a 21st century cyber-enabled cross border crime. As a result the police are achieving limited success and victims are receiving too little by way of service.

Most of the work on reducing fraud must be in the prevention space, simply because so many of the offenders operate overseas and beyond the reach of UK law enforcement. We need a much more systemic approach to fraud, economic and cyber-crime prevention both nationally (through a new Crime Prevention Agency) and locally (through a bottom-up public health approach).

By 2030 we need to have reformed the way the police respond to fraud by strengthening national and regional capabilities. A new National Anti-Fraud Data Centre should be powered by

both police and private sector data to create a strong strategic intelligence picture and real time operational insights. A new national police body should be charged with tackling fraud, economic and cybercrime. A network of regional hubs should bring together police investigators with public and private sector partners to undertake both proactive operations and reactive investigations.

Local policing must play its part too, in terms of pursuing simple local frauds and using its links into communities to provide prevention advice. All of this must be underpinned by a workforce strategy to create a pipeline of recruits with the necessary skills.

While money is tight at present over the next two spending reviews we must as a country invest more in tackling the single biggest form of crime affecting the public. We need more officers doing more investigations, more proactive operations making life more difficult for those perpetrating fraud and more justice and support for victims.



# REFERENCES

Doig, A, M Levi and Luker, J. (2024) Will the future policing of fraud be 'a fundamental shift in our approach to tackling fraud' or largely more of the same? Reviewing the 2023 UK fraud strategy through evidence on the ground *Security Journal* 202538(8), pp.1-33.

The Fraud Act (2006) available at: <<https://www.legislation.gov.uk/ukpga/2006/35>>

Duffield, G. and Grabosky, P. (2001), *The Psychology of Fraud*, Trends and Issues in Crime and Criminal Justice Series, No. 199, Canberra: Australian Institute of Criminology.,

HMICFRS (2021). *Spotlight report. A review of Fraud: Time to choose. A revisit of the 2018 fraud inspection to assess progress of the recommendations and areas for improvement*. London: HMICFRS.

INTERPOL (2024) *INTERPOL Global Financial Fraud Assessment*. Available at: <[https://www.interpol.int/en/content/download/21096/file/24COM005563-01%20-%20CAS\\_Global%20Financial%20Fraud%20Assessment\\_Public%20version\\_2024-03\\_EN\\_v3.pdf](https://www.interpol.int/en/content/download/21096/file/24COM005563-01%20-%20CAS_Global%20Financial%20Fraud%20Assessment_Public%20version_2024-03_EN_v3.pdf)>.

Levi, M., Doig, A., Luker, J., Williams, M. and Shepherd, J.(2023) *Towards a Public Health Approach to Frauds. Volume I: The West Midlands Police Area Fraud Report*. Available at: <<https://www.westmidlands-pcc.gov.uk/wp-content/uploads/2023/03/NW260123-Fraud-report-V1-PCC-final-140323.pdf?x48388>>.

ONS (2025) *Crime in England and Wales: year ending December 2024*. Available at: <<https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingdecember2024>>.

ONS (2020) *Nature of fraud and computer misuse in England and Wales: year ending March 2019*. Available at: <<https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2019>>.

ONS (2018) *Crime in England and Wales: Additional tables on fraud and cybercrime*. <<https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesexperimentaltables>>.

Skidmore, M., O'Connell, F., Halkon, R., Meenaghan, A., and Button, M. (forthcoming). *Exploratory research to examine the impact of fraud on victim health*.

Skidmore, M., Ramm, J., Goldstraw-White, J., Barrett, C., Barleaza, S, Muir, R.and Gill, M. (2018) *More than just a number: improving the police response to victims of fraud*. London: The Police Foundation. Available at: <[https://www.police-foundation.org.uk/wp-content/uploads/2010/10/more\\_than\\_just\\_a\\_number\\_exec\\_summary.pdf](https://www.police-foundation.org.uk/wp-content/uploads/2010/10/more_than_just_a_number_exec_summary.pdf)>.

UK Government (2022) *Economic Crime Plan 2*. London: Home Office. Available at: <[https://assets.publishing.service.gov.uk/media/642561b02fa8480013ec0f97/6.8300\\_HO\\_Economic\\_Crime\\_Plan\\_2\\_v6\\_Web.pdf](https://assets.publishing.service.gov.uk/media/642561b02fa8480013ec0f97/6.8300_HO_Economic_Crime_Plan_2_v6_Web.pdf)>.

UK Government (2023) *Fraud Strategy: stopping scams and protecting the public*. London: Home Office. Available at: <<https://www.gov.uk/government/publications/fraud-strategy/fraud-strategy-stopping-scams-and-protecting-the-public>>.

UNODC (2024) *Organized Fraud, Issues Paper*. Vienna: UNODC. Available at: <<https://www.unodc.org/documents/organized-crime/Publications/IssuePaperFraud-eBook.pdf>>.

Wood, H. and Baxter, K. (2022) *Towards a New Model for Economic Crime Policing. Target 2030*. London: RUSI. Available at: <<https://static.rusi.org/towards-a-new-model-for-economic-crime-policing.pdf>>.



© 2025 The Police Foundation

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, without the prior permission of The Police Foundation.

Enquiries concerning reproduction should be sent to The Police Foundation.

Email: [info@police-foundation.org.uk](mailto:info@police-foundation.org.uk)

[www.police-foundation.org.uk](http://www.police-foundation.org.uk)

Charity Registration Number: 278257