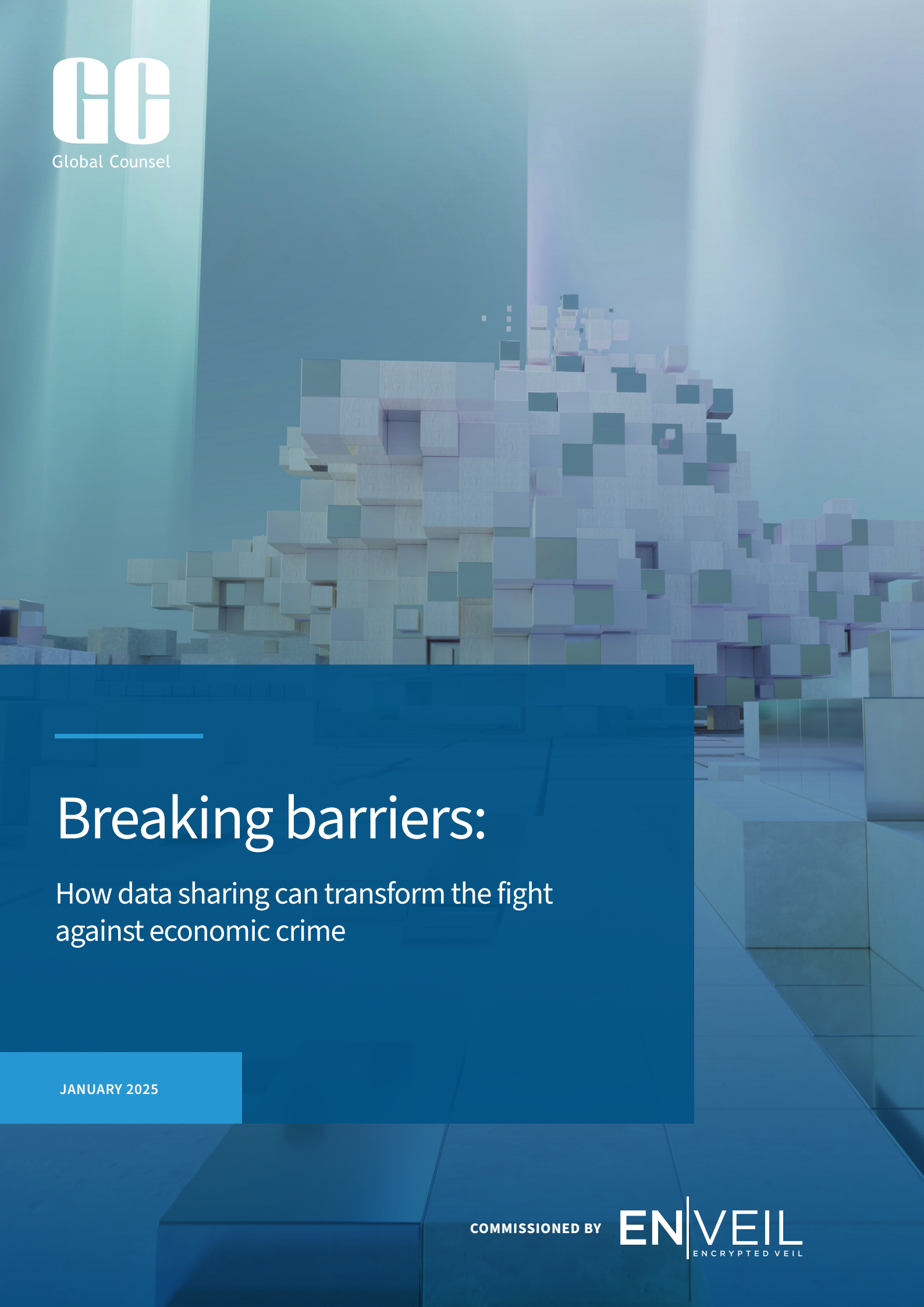


Global Counsel

Breaking barriers:

How data sharing can transform the fight against economic crime

JANUARY 2025

COMMISSIONED BY ENVEIL ENCRYPTED VEIL

Table of Contents

Foreword	3
Executive Summary	4
Methodology	5
The case for action – The impact of economic crime	6
Economic crime prevention – Identifying the challenges	9
Recommendations	15
About Global Counsel	18
About Enveil	19

Foreword

We live in a world where economic crime is prevalent, painful, and pervasive. It has, unfortunately, become a part of our daily lives to the point that headlines which should be shocking hardly garner attention. Most businesses and individuals have or will be affected by these criminal acts at some point, a fact that we seem to now tolerate to some degree as much of the fight is focused on discovery and mitigation rather than prevention.

This is not because preventative measures are beyond reach. As you'll find highlighted in this report, there have recently been positive movements in both discussion and action across the public-private divide. We live in a data-rich, technology-enabled world that is ripe with opportunity to evolve, and we've started to recognise areas where groundbreaking tools and capabilities can drive positive outcomes. This includes Privacy Enhancing Technologies (PETs), which are currently being explored and leveraged in sandbox and real-world deployments on a global scale. All very encouraging, however, the scope of this progress does not yet align with the sheer size of the challenge. The lack of a clear, collective focus on economic crime prevention policy and practices by stakeholders across this space was the primary driver for undertaking this research effort.

While one might assume that the far-reaching impact of economic crime — spanning regions, socioeconomic status, and industries — would be enough to elevate its importance among policy makers and business leaders alike, its breadth may actually be having the opposite effect. The number of stakeholders involved has led to fragmented initiatives and a lack of ownership and urgency. The challenge feels large (because it is), which can make it easy to write off efforts by any given organisation as too small to warrant pursuit. But, we must avoid bureaucratic inertia and act at scale so bad actors can no longer operate with such ease.

Further, the commonality of these crimes also makes them easier to ignore. To some degree, the parties at the forefront of activity, including the financial industry, have come to accept financial crime as part of business as usual, a stance that leads to less urgency in driving solutions. If the risk and financial impact of such activity is built into a business' bottom line, it is hard to imagine they see addressing these challenges as critical.

The current economic crime climate necessitates bold action by both policy makers and industry stakeholders. The time to do more, collectively, is now — and a sustainable, near-term solution will be found at the intersection of policy, technology, and a commitment to action. This means working to leverage the cross-boundary data and technology-enabling capabilities that will allow stakeholders to collaborate and fight economic crimes more effectively.

By working together to reorient our approach from reactive to proactive, we can reduce the economic, societal, and personal impact of these pervasive criminal activities.

ELLISON ANNE WILLIAMS

CEO, Enveil

Executive Summary

Economic crime costs the UK economy an estimated £8.5bn a year. Fraud alone has become common, with direct costs put at more than £1bn. The lasting emotional damage done to victims has an incalculable cost that bears down on society. Yet economic crime has, until recently, not been a priority for politicians and law enforcement.

For this white paper, we interviewed a wide range of senior stakeholders from organisations which are at the forefront of economic crime detection prevention and mitigation. In particular, we focused on cultural and policy barriers to better collaboration, data sharing and technological innovation.

Insufficient funding remains a major obstacle. But so is the proliferation of bodies involved in fraud detection and prevention. The current Government has committed to a new fraud strategy, and in this paper we make the case for a specific focus on improving and normalising information sharing.

We've identified four obstacles to data and intelligence sharing. First, a lack of clear incentives that address cost and regulatory risk: firms want to help, but they need legislative clarity to make it easy and inexpensive to do so. Second, legal ambiguity: firms need legal clarity, for example around terms such as 'economic crime', to help them manage legal risk. Third, a better understanding of new technologies: criminals move fast to adapt to technological change but firms sometimes are slow to adopt new methods, particularly third-party solutions such as Privacy Enhancing Technologies (PETs). And fourth, a fragmented data-sharing environment, where wide differences between cross-sector pilots due to inconsistent governance and data requirements where a standardised approach would make participation easier and cost lower.

Progress can be made if the Government and law enforcement between them provide greater direction on data and intelligence sharing. We recommend a three-staged approach. First, the Financial Conduct Authority (FCA), the Information Commissioner's Office (ICO) and National Economic Crime Centre (NECC) should run operational pilots, testing new technologies such as PETs, including a wide range of public and private stakeholders, to produce a common understanding of how technology can help. Second, the Government should call time on voluntary agreements and mandate information sharing in the financial services sector. And third, the Government should authorise the ICO and other regulatory bodies to oversee a standardised lexicon for UK data and intelligence sharing.

Our research shows that a broad consensus exists to take these steps forward. We are confident that, taken together, the measures set out here can help government, regulators, law enforcement and firms make the UK a hostile environment for criminals.

Methodology

This report has been supported by interviews with regulatory, law enforcement and private sector stakeholders active in fraud information sharing policy.

Interviewees were selected to ensure a breadth of opinion is reflected across the economic crime sphere, including government, regulators, law enforcement, the financial services industry and other impacted sectors. A selection of those interviewees is listed below.

To support comparison between interviewees, they were asked a series of structured questions before entering a longer discussion on the role of technology in preventing economic crime. This has ensured the interview process enabled comparison between individuals, institutions and sectors. The report was also augmented by desk-research across existing third-party sources, such as recent government and parliamentary reports around economic crime.

Organisations interviewed include:

- Centre for Finance, Innovation & Technology (CFIT)
- City of London Police
- Department of Science, Innovation & Technology (DSIT)
- Information Commissioner's Office
- Three
- CIFAS
- Cyber Defence Alliance
- National Economic Crime Centre (NECC)
- Stop Scams UK

01

The case for action – The impact of economic crime

01

The case for action – The impact of economic crime

£100bn
laundered in the UK

£1.7bn
lost in direct costs to fraud

Once considered a marginal threat, economic crime now operates as a sophisticated enterprise that evolves minute-by-minute. It is of such a scale today that estimates of its cost vary significantly, although all project steep losses to the UK's economy and society.

Government estimates suggest that at least £8.4 billion is lost to economic crime each year, finding that it is 'serious and organised'[1]. Elsewhere, the Treasury Select Committee found that economic crime could 'reasonably be said to run into the tens of billions of pounds' and that it is growing quickly. Previous National Crime Agency estimates suggested over £100 billion is laundered in the UK alone while the Treasury Select Committee is clear that the scale of economic crime is growing. Looking at fraud specifically, the latest figures from UK Finance's 2024 Fraud report shows £1.17bn was lost in direct costs to fraud in 2023.

The evidence suggests that the public and the private sector are increasingly concerned about economic crime. The government's most recent survey on economic crime found that 39% of businesses thought fraud was very common[2]. Equally, there is strong evidence that certain types of economic crime like fraud are rarely a one-off, with 46% of businesses which were victims of fraud experiencing more than one incident.

While these estimates represent the prevalence and cost of economic crime, they do not reflect the wider damage it causes. Economic crime can leave a harrowing emotional impact on its victims, from small business owners to pensioners. These victims often lose significant amounts of money in an instance, leaving them both vulnerable and unsupported. Even victims who are able to recoup losses typically do so at the cost of experiencing an upsetting and lengthy ordeal. Despite this, by the nature of its intangibility, economic crime is often subject to less political focus than other public safety priorities, although there are signs this is changing.

A rising tide of criminality is increasingly being met by a wave of technology innovation and collaboration between the private and public sector to move away from reactive measures and focus on proactive initiatives that will make the UK a difficult operating environment for fraudsters. There has been a groundswell in recent years of interest across law

1. https://www.gov.uk/government/publications/economic-crime-survey-2020/economic-crime-survey-2020#introduction
2. https://www.gov.uk/government/publications/economic-crime-survey-2020/economic-crime-survey-2020#perceptions-and-risks-of-experiencing-economic-crime

enforcement, regulators and the private sector to test how technology can be adopted to prevent, mitigate and tackle economic crime. However, while progress has been made, scaling this work to match the industrialisation of economic crime has not yet occurred.

This white paper looks at how we can build on the significant progress that has been made through initiatives like the National Fraud Database run by CIFAS and the recent data fusion pilot led by the National Economic Crime Centre (NECC), to remove further barriers to information sharing and improve the prevention activity that better data sharing can enable.

It also seeks to address whether recent efforts to tackle economic crime go far enough, what the existing policy barriers are and the possible solutions. Our research highlights how cultural and institutional barriers can be overcome with a mix of expanded pilots and use of solutions such as privacy enhancing technologies (PETs). In highlighting these barriers and solutions, the paper aims to act as a catalyst for action to be taken so that collectively, institutions can make the UK a hostile environment for criminals, where the huge financial risk and exposure they bring is no longer tolerated.

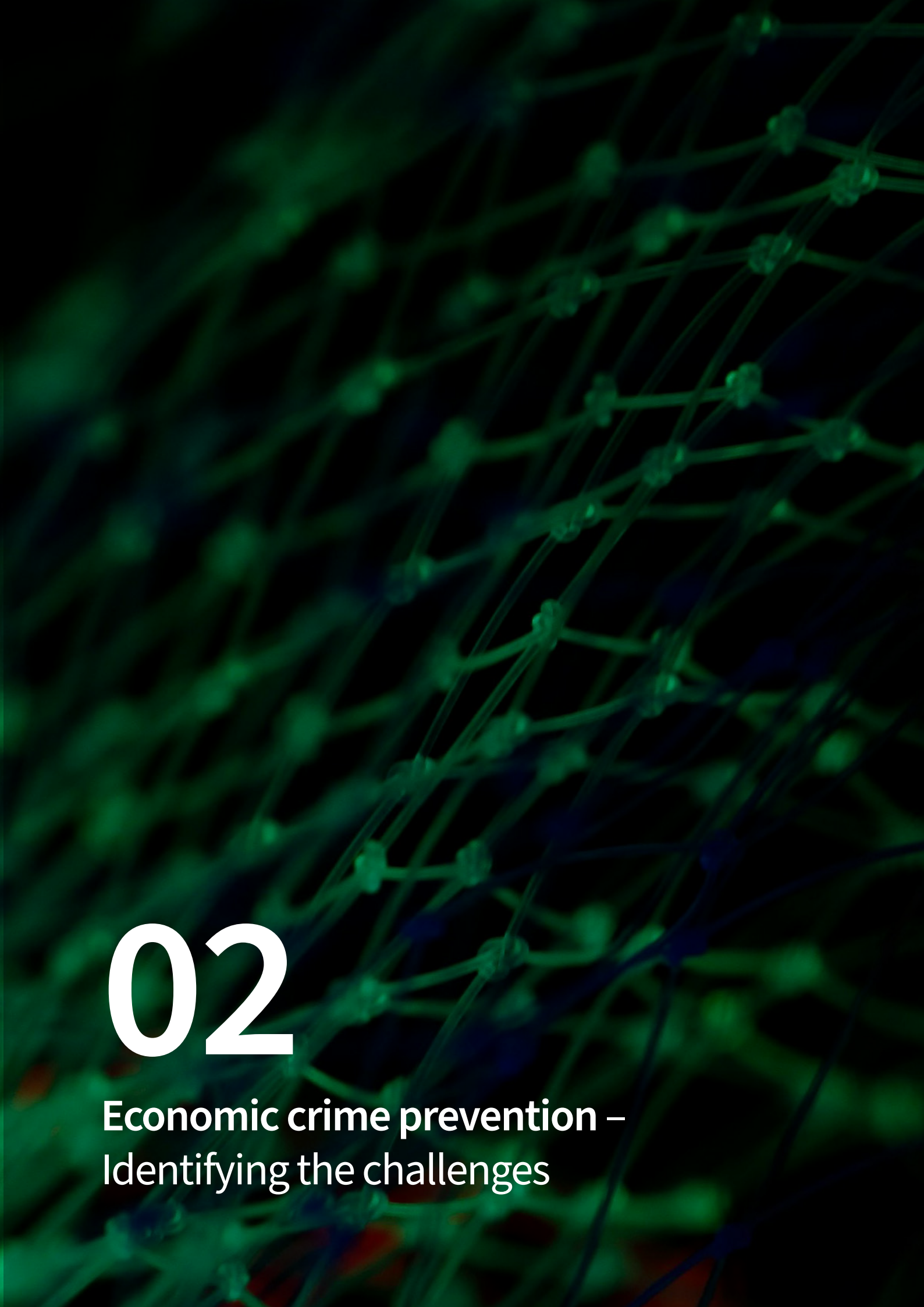
> *PETs can help organisations across a range of sectors unlock more value from data and drive innovation in ways that can protect people's privacy[3]"*
>
> **REGULATOR**

> *Is PETs actually the right word? It's less about enhancing privacy and more about enhancing collaboration without making privacy worse"*
>
> **POLICY OFFICIAL**

What are privacy enhancing technologies?

Privacy Enhancing Technologies, or PETs, enable, enhance and preserve the privacy of data throughout its lifecycle, securing the usage of data. They allow for the use, analysis and sharing of information - such as data critical to preventing economic crime - whilst minimising risks to data privacy and security.

3. https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/11/using-privacy-enhancing-technologies-pets-to-unlock-value-from-data-responsibly/



02

Economic crime prevention – Identifying the challenges

02

Economic crime prevention – Identifying the challenges

Government designed frameworks always help when you've got so many players, not least from other sectors that don't normally interact with one another"

INDUSTRY

Context on progress

Government and law enforcement struggle against a constantly evolving threat from fraud and economic crime – although crucial progress has been made. Policymakers have put considerable effort into modernising the legal framework, delivering two major pieces of primary legislation on economic crime and enhancing corporate transparency in recent years. Increased public-private partnership, particularly between law enforcement and the banking sector has led to improvements in data and intelligence sharing in the UK. Specialists have noted that the debate has now shifted from - why data sharing is important – to how we can do it.

The barriers to addressing economic crime appear well-understood by regulators and industry, from fostering a culture of mutual trust to encouraging cross-sector public-private collaboration, legal clarity on data and the sheer financial cost involved. While there are differing views on emphasis across the industry, it is clear that a combination of cultural, legal and technological capacity challenges has hampered the UK's efforts to combat economic crime which has grown over a decade into a thriving criminal industry.

01 | **Barriers to further progress**. In the Economic Crime Plan for 2023-26, the previous government committed to delivering £400m in additional funding to tackle economic crime over the next spending period[4]. The Plan included commitments to introduce additional specialist staff for law enforcement agencies to combat money laundering and tackle complex threats from emerging technologies such as cryptoassets[5]. However, while these interventions are welcome, it is patently clear that this additional funding is insufficient to support law enforcement agencies such as the NCA who are struggling to properly resource the UK's fight against economic crime[6]. The fact remains, it is far more cost effective to prevent economic crime at source. While industry has worked for a long time with regulators and law enforcement agencies to flag suspicious activities, block fraudulent accounts and cross-reference evidence of bad practice with peers, these tools are insufficiently agile to prevent crimes from occurring in the first place. For example, the confusion of law enforcement agencies, sectoral regulators and industries involved in the fraud ecosystem, such as the National Economic Crime Centre (NECC), Serious Fraud Office, Home Office, FCA – often poorly coordinated - has been a significant and often-cited obstacle to the government's efforts to deliver a powerful national strategy of fraud prevention[7].

02 | **An opportunity to resolve these challenges.** The government has committed to delivering an ambitious new fraud strategy in this parliament and has placed increasing cross-sector data sharing and intelligence at the heart of its approach to updating the strategy[8]. This is promising, although it will take a sustained focus from government ministers and officials on this agenda to deliver meaningful change. Our research with senior figures representing organisations leading this work has identified four core challenges to tackling economic crime through meaningful information sharing.

4. Economic crime plan 2023 to 2026 - GOV.UK
5. Economic crime plan 2023 to 2026 - GOV.UK
6. https://www.spotlightcorruption.org/wp-content/uploads/2024/09/SoC_IBFK_final.pdf
7. Economic Crime — APPG on Fair Banking
8. Take back our streets – The Labour Party

Four major challenges were identified by those surveyed in relation to data and intelligence sharing:

01 | **Challenge One:** Lack of incentives. Ultimately, there remains little incentive for industry to support voluntary data sharing schemes that risk exposing internal system failings or data irregularities, with often intangible benefits in return. The high volume of mandatory regulatory reporting requirements that bank economic crime prevention teams must deal with has a major impact on prioritisation. Our research has found that several organisations are concerned about how they can both adhere tightly to data protection law and appropriately share valuable information; they don't feel sufficiently incentivised to take a risk. This is especially true in 'pre-suspicion' contexts. There was said to be far greater clarity over the legal responsibilities financial institutions have to share intelligence with law enforcement and the FCA once a crime had already been committed - creating adverse incentives for banks to engage 'after the fact'.

For other sectors including tech platforms and telecoms operators, there remain potential challenges around incentives, such as the lack of existing industry data flows compared with the banking sector and the lack of direct financial incentive in the form of the Economic Crime Levy or Authorised Push Payment fraud reimbursement legislation.

02 | **Challenge Two:** Legal & regulatory ambiguity. Those participating in and directly coordinating information sharing initiatives believe that the existing legislative framework setting out exemptions from the UK Data Protection Act for the purposes of tackling economic crime are broadly sufficient. The creation of guidance such as the government and ICO's cost-benefit awareness tool also helps [9].

However there remains a widespread view that further legal clarity, building on the Home Office guidance published in October focused on provisions in the Economic Crime Act on information sharing to combat money-laundering, would be valuable[10]. The reasons for this varied considerably between those who wanted further guidance in order to 'remove excuses, not barriers' and those for whom ongoing legal ambiguity was a clear barrier to participation. Specifically, there were calls for greater clarity on the definition of economic crime and what constitutes an 'offence'. Regulatory sandboxes such as the Digital Regulation Cooperation Forum (DRCF) also have a critical role to play in providing regulatory clarity, allowing the trialling of new technological solutions in collaboration with regulatory bodies including the FCA, ICO and OFCOM.

> *It is less that there are hard regulatory barriers to data sharing, and more that there's a tension between the motivations of different stakeholders"*
>
> **POLICY OFFICIAL**

> *Legislation actually enables a lot of sharing, subject to legal counsels accepting that there is always a certain amount of legal jeopardy around free suspicion"*
>
> **LAW ENFORCEMENT**

9. Cost-benefit awareness tool, DSIT and ICO
10. Information sharing measures in the Economic Crime and Corporate Transparency Act - GOV.UK

03 | **Challenge Three:** Lack of education on technological solutions. As the technology used by fraudsters rapidly evolves, with the emergence of generative AI adding further fuel to this challenge, so must the technology used to share crucial data and intelligence ahead of time[11]. New technologies that can assuage concerns on data compliance risks and provide simple solutions will be vital in achieving the new government's vision. However, this paper has identified inadequate understanding of the potential of technology to fix common problems constraining progress. Both regulators and the private sector are clear that banks continue to use outdated technology and systems to tackle sophisticated threats.

For instance, in relation to the use of Privacy Enhancing Technologies ("PETs") to solve existing data sharing challenges, interest is high, but adoption is low. Regulators and law enforcement tended to have a working knowledge of PETs, but were unsure about their applicability or whether legacy systems could support their use. That said, two clear use cases identified by interviewees for PETs included rapidly querying specific data points 'in situ' and circumnavigating data protection challenges associated with sharing data across jurisdictional boundaries. The private sector appears to have a clearer understanding on PETs but again there was a widespread hesitancy about engaging with third party solutions.

04 | **Challenge Four:** Scaling a fragmented data-sharing 'industry'. The status of counter fraud data and intelligence sharing initiatives was repeatedly described in interviews as a 'boutique industry'. The landscape is dominated by a range of cross-sector pilots involving the banks, tech sector and telecoms coordinated by different organisations including CIFAS, UK Finance and StopScams. There is significant support from regulators, law enforcement and industry in maintaining a 'federal approach', allowing different pilots to foster innovation, determining 'winners and losers'. However, at the same time, the lack of consistency in governance and data requirements across fragmented pilots was identified as a barrier to encouraging participation; private sector legal teams have to make an individual risk decision, without being able to rely on the comfort of a standardised approach. While the lack of a single entity overseeing the landscape was seen as a challenge, the resourcing implications of addressing this problem remains a constraint.

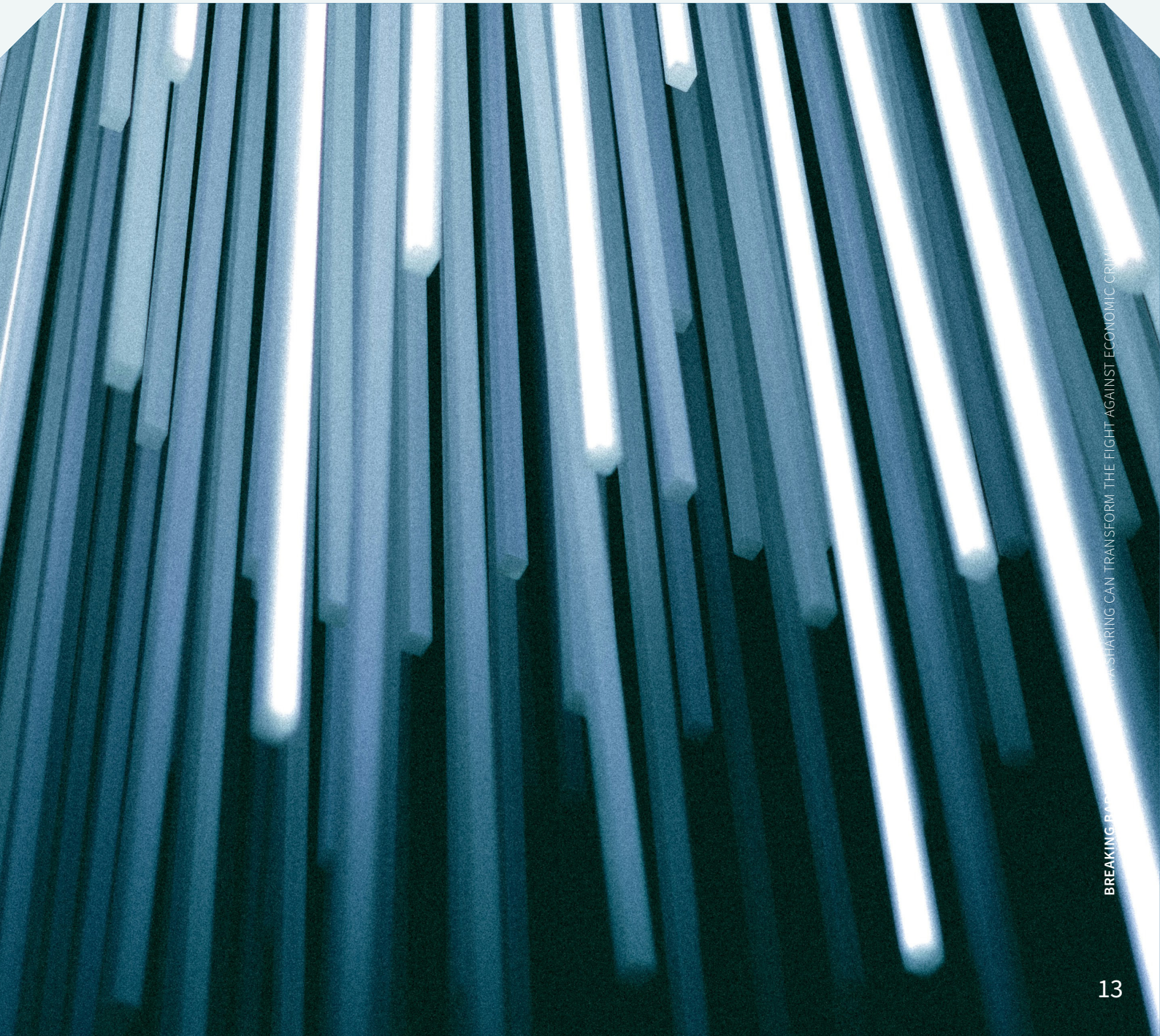
> *If somebody says to me, you now have a mandatory requirement to share data, there is a requirement, right? Great. Now I can have funding, which means I can now get money and get people. I can now shift it from the side of a desk to it being someone's job."*
>
> **INDUSTRY**

11. Impact of Artificial Intelligence on Fraud & Scams, PwC

Case study of privacy enhancing technologies

Enveil was engaged by a large, EU-based financial institution to validate how PETs can be used to facilitate the secure and private data sharing needed to build a trusted collaboration network between entities. The capabilities addressed specific customer pain points by enabling users to match customer profiles and enriched data across parties, and query for indicators and AML typologies across entities, to offer additional insights on financial crime activity and behaviours.

Enveil enabled encrypted queries across 2 billion transaction records, as well as horizontal scaling capable of handling large datasets. The engagement verified how PETs-powered solutions can be used to overcome legal and compliance boundaries by ensuring that sensitive data remains encrypted during processing and ensuring underlying data holdings are never compromised.



Timeline of initiatives to support information sharing

Both industry and enforcement agencies have made concerted efforts to improve the level of information sharing in recent years. Recent initiatives include:

2015

Joint Money Laundering Intelligence Taskforce created.

2017

Joint Fraud Taskforce launched.

2018

FCA Digital Regulatory Reporting Pilots.

2021

UK Finance Information Sharing Pilot Sandbox launched.

2024

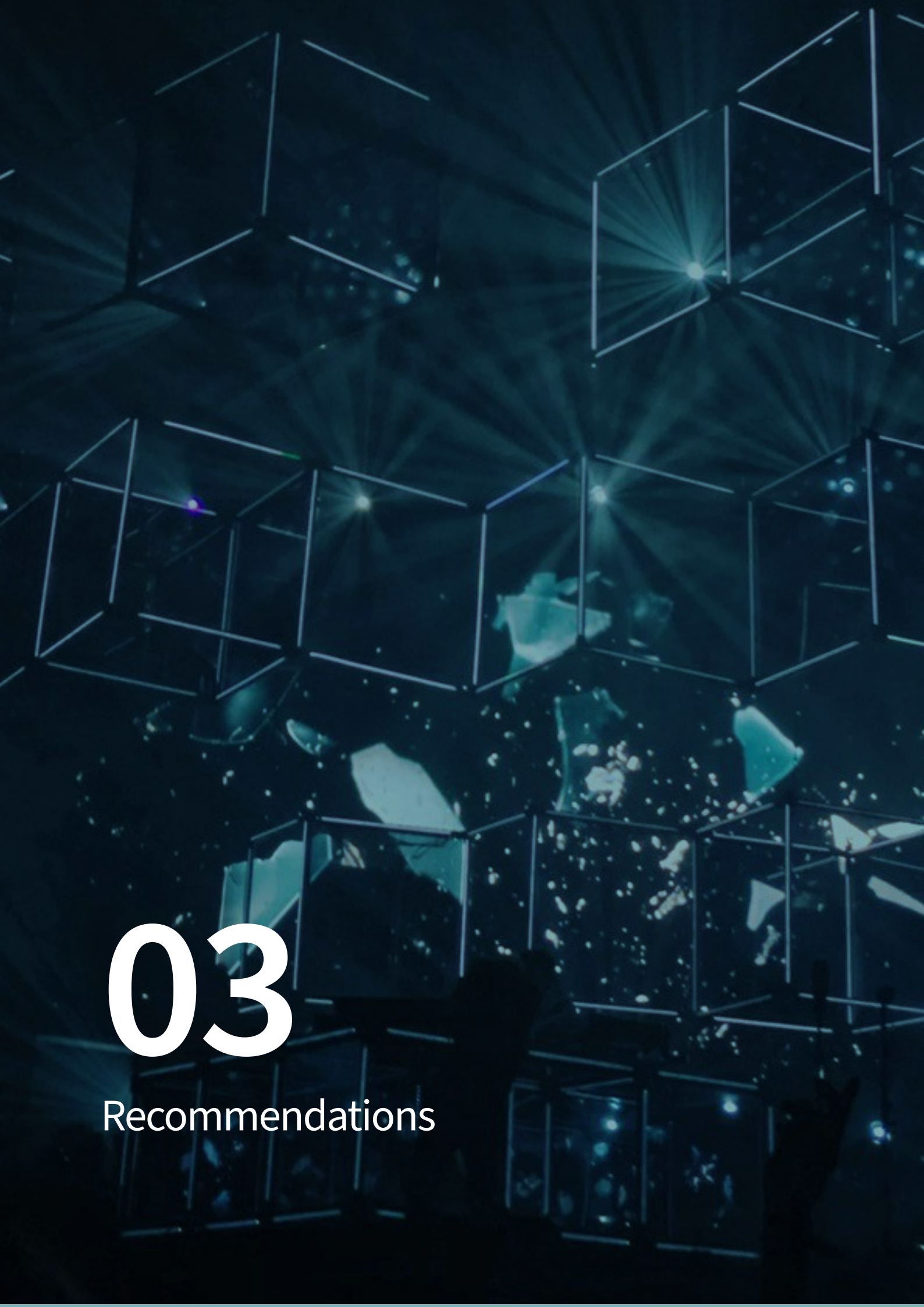
Which? Coalition between banks and telecoms launched.

2024

NCA Data Fusion Project.

2024

Meta UK Fraud Intelligence Reciprocal Exchange (FIRE).



03

Recommendations

03

Recommendations

International data sharing remains highly fragmented. PETs could act as a bridging connection in a more federated system."

CIVIC SOCIETY

What a potential solution should seek to achieve.

In the context of ever-growing compliance costs and limited resources to allocate, the current approach to data and intelligence sharing risks hitting its ceiling in usefulness without further direction from government and law enforcement.

Any solution should be modest to prove its use case in a specific sector and present clear ROI for its participants on both sides of the public and private divide before being expanded elsewhere. In that spirit, while international collaboration remains critical to fighting economic crime and the UK should remain ambitious in tackling threats head-on with its global partners, solutions should initially be domestic focused to prove effectiveness before expanding to cross-border data flows.

Our research, based on extensive conversations with senior figures working across the economic crime prevention landscape has informed this white paper's recommendations for a three-stage strategy that tackles many of the cultural and institutional barriers identified in earlier sections.

While ensuring scalability and cross-sector applicability remains core to its design, any solution should be tested in the financial services sector first, as the sector with the greatest level of maturity and sophistication in tackling economic crime. However, it is crucial that in parallel, technology and telecommunications firms increase access to their own data; many interviewees cited filling this gap as the most impactful step towards tackling fraud and economic crime, even while recognising that the data types might be different (e.g. URLs rather than transaction data).

Data sharing pilot case studies:

FIRE programme

Social media platform Meta has partnered with the likes of NatWest and Metro Bank under the umbrella of Stop Scams UK on its Fraud Intelligence Reciprocal Exchange (FIRE) programme - allowing banks to share intelligence with the platform about potential scams online. As of October 2024, the early-stage pilot has led to action against tens of thousands of accounts run by scammers[12].

NCA's data fusion project

The National Crime Agency (NCA) has partnered with seven major UK banks on a major public-private data fusion pilot. A joint team made up of law enforcement specialists and subject matter experts from participating banks has been analysing both bank transaction data and NCA data sets to disrupt criminality and minimise risk. Since the project went live in May 2024, the NCA has reported that eight new criminal networks have been identified.

12. Meta Partners with UK Banks to Combat Scams, Meta

Recommendations

Using operational pilots to drive technological adoption.

There is clear sense in the private sector that data protection concerns and a perceived institutional nervousness to expose organisations' systems to regulators has acted as a drag on effective information sharing. Several pilots between regulators and the private sector have worked well to resolve this issue, but the increasing urgency of our economic crime threat means the UK must be bolder. The Financial Conduct Authority, Information Commissioner's Office and National Economic Crime Centre should expand and deepen their existing schemes by running operational pilots to trial new technologies – PETs being one example – on real data to demonstrate how they optimise effective information sharing and data protection. These pilots would have the merit of bringing in a wider range of stakeholders – across government, regulators and the private sector – to help with a common understanding of the strengths and weaknesses of technology in tackling economic crime.

Mandating information sharing in the financial services sector

Our research indicates that voluntary agreements have reached the end of their usefulness and have failed to address the fundamental problem of incentives. The FCA should mandate information sharing among a selection of major critical institutions in the financial services sector and evaluate the impact 12 months after the mandate comes into force. Mandating these flows is critical but should be targeted sectorally so that regulators are not subsumed by information and are able to focus on the areas at highest risk of economic crime.

Standardising industry's approach to data and information sharing; creating a common lexicon.

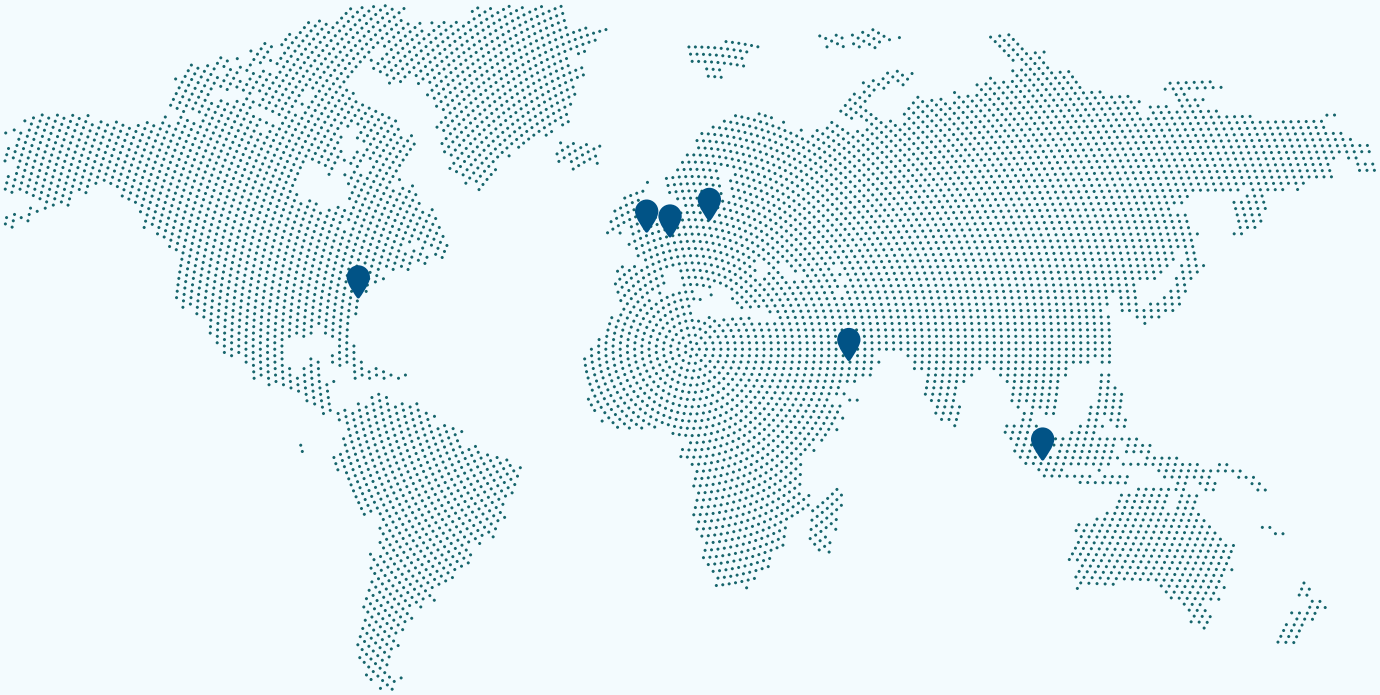
At present, data controllers take an individual legal decision on firm participation, where the commercial consequences of a procedural error are significant, thereby diluting incentives to increase data sharing. Developing a standardised approach, led by industry bodies and endorsed by a third-party such as the ICO would increase comfort levels within the financial services industry to participate in data sharing at scale. This would provide a more granular best practice guide for firms, potentially in the form of a standardised initial Data Protection Impact Assessment (DPIA). This would supplement current high-level government guidance and feed into the creation of a standard lexicon for data and intelligence sharing. Its development would be led initially by the financial services industry and would provide a solid platform to build new innovative operational pilots.

About Global Counsel

Global Counsel is a strategic advisory business.

We help companies and investors across a wide range of sectors anticipate the ways in which politics, regulation and public policymaking create both risk and opportunity — and to develop and implement strategies to meet these challenges. Our team has experience in politics and policymaking in national governments and international institutions backed with deep regional and local knowledge.

Our offices in Berlin, Brussels, London, Singapore, Washington DC and Doha are supported by a global network of policymakers, businesses and analysts.



About Enveil

Enveil is a pioneering Privacy Enhancing Technology company protecting Data in Use and changing the paradigm of how and where organizations can leverage data to unlock value. Defining the transformative category of Privacy Enhancing Technologies (PETs), Enveil's award-winning ZeroReveal® solutions for secure data usage, collaboration, monetization, and Secure AI protect the content of the search, analytic, or model while it's being used or processed. Using these business-enabling and privacy-preserving capabilities, customers can extract insights, cross-match, search, analyze, and utilize AI across boundaries and silos at scale without exposing their interests and intent or compromising the security or ownership of the underlying data. A World Economic Forum Technology Pioneer and Gartner Cool Vendor, Enveil is deployed and operational today, revolutionizing data usage in the global marketplace.

LEAD AUTHORS

Harry Palmer
Senior Associate, Global Counsel

Fergus Cameron Watt
Senior Associate, Global Counsel

CONTRIBUTORS

Rebecca Park
Managing Director, Global Counsel

Conan D'Arcy
Senior Practice Director, Global Counsel

Megan Stagman
Director, Global Counsel

CONTACT

info@global-counsel.com

Global Counsel