Tackling Fraud and Scams: An Ecosystem-Wide Approach

Research conducted on behalf of Barclays

March 2022

Barclays Foreword (1/2)

The UK is in the midst of a scams epidemic, with devastating consequences for individuals, businesses and the economy as a whole.

More and more of our lives are digital, from working and socialising to gaming and dating – that trend has long been evident, and has been accelerated by Covid-19. But criminals are adapting to take advantage of this and defraud innocent victims, with 2021 expected to have been a record year for the number of financial scams, with victims losing more to fraudsters than ever before.

Retail banks have taken a number of steps in anticipation of and response to these developments, including voluntarily introducing the Contingent Reimbursement Model (CRM) Code, which guarantees that victims will be reimbursed if they have taken reasonable steps to protect themselves against the possibility of a scam.

Scams can have life changing impacts on their victims, and those innocent people deserve a mechanism through which to be reimbursed. But reimbursing customers does not – and will not – fix the fundamental problem we all face. The simple fact is that criminals still benefit from the proceeds of their crime, which are then reinvested in creating even more subtle ways of defrauding other innocent people. This is a pernicious and vicious cycle that must be broken. The challenge also runs deeper – public trust in the digital economy is being eroded; and the emotional and mental health impacts on victims are long lasting, even when their money is returned.

The challenge facing society today, therefore, is how to prevent scams from happening in the first place. An ongoing problem is not resolved by continually repairing its negative impacts, but by tackling the underlying causes and enablers. In other words, we must focus on finding the right cure, not just treating the symptoms.

That challenge seems self-evident, so the question we ask ourselves repeatedly is “why isn’t it getting more attention?”.

I see two key reasons: first, ‘scams’ - where the victim voluntarily and unwittingly makes a payment to a criminal – are far more complex to detect and prevent than ‘fraud’ – where the victim does not authorise the payment. With fraud, banks can use transactional monitoring capabilities to detect and stop most unusual activity. But with scams it is the legitimate customer making a payment, which means it is not just a question of detecting unusual behaviour, but often then convincing the customer to change their mind, after they’ve been convinced by the fraudster that the action is in their best interest.

Second, the challenge of scams cannot be solved by one organisation or even industry acting on its own. Criminals explicitly and purposely exploit multiple technologies and infrastructures across a variety of industries because they know how hard it is for actors across those sectors to coordinate their activity.

It will only be through collective, coordinated intervention, from all those with the ability and need to take action, that we can succeed against these criminals. All relevant actors – …

Barclays Foreword (2/2)

government, regulators, law enforcement and key sectors across the ‘scams ecosystem’ (including payment providers, telecommunications firms, technology platforms, and others), along with customers – must come together as part of a comprehensive, collaborative national effort to tackle this shared problem, prevent scams at their source and – ultimately – protect consumers and society.

Recent years have seen a range of innovative and collaborative responses to this challenge. These include: an ambitious retail banking sector-wide strategy to tackle and prevent fraud and scams, coordinated by UK Finance; individual initiatives from payment providers, telecommunications firms and technology platforms; as well as cross-sectoral efforts such as Stop Scams UK (SSUK) and the Online Fraud Steering Group (OFSG).

A number of governmental and regulatory initiatives have also served to enhance the policy framework firms operate in – for example, Government’s expansion of the Online Safety Bill to include fraud, and its commitment to treat fraud as a ‘priority illegal offence’. These represent welcome developments that should be supported and accelerated.

In order to build on these initiatives, and determine where further and greater action is required, we asked Frontier Economics to speak with experts from across the ‘scams ecosystem’ to devise a policy framework setting out what a truly comprehensive response would look like. We have then taken their research and put forward nine recommendations – our ‘Scams Manifesto’ – that we believe are the necessary steps required to significantly enhance how the UK as a whole responds to scams and protects society, building on recommendations others have made.

Barclays is wholeheartedly committed to playing our part in the solution, and working constructively with all parties to stamp out the scourge of scams in the UK.

We hope that these recommendations accelerate the UK’s response to this scams epidemic and enable a decisive new phase in tackling economic criminals before they can even reach their potential victims.

Matt Hammerstein
CEO, Barclays UK

Barclays' Scams Manifesto makes nine recommendations for actions, based on Frontier's research (1/2)

		Recommendation	Success measure
Coordinated Framework	1	**A single Government entity or appointed individual should be designated as the 'Scams Lead'** to align Government, regulators and industries' responses to tackling scams, with defined responsibility to drive meaningful change in legislative, regulatory and firms' strategies.	Appointment of a single entity or individual tasked with delivering a comprehensive response to tackling scams that aligns the activity of different policy makers, regulators and industries.
	2	**Legislative, regulatory and industry actions to tackle scams should be aligned by a single overarching framework** (led by the Scams Lead).	Delivery of a framework that provides a comprehensive response to tackling scams (by aligning existing activity of different policy makers, regulators and industries, highlighting gaps that require further action, and setting clear responsibilities on designated entities to take action).
Regulation and Enforcement	3	**Where voluntary industry action is insufficient**, **gaps in the prevention of scams should be resolved** through mandated legislative or regulatory intervention.	Government and regulators make timely interventions across the ecosystem to require or enable action to prevent scams.
	4	**Customers should be guaranteed consistent protections from scams from all payment providers.**	All Payment Service Providers (PSPs) implement the requirements of the Contingent Reimbursement Model (CRM) Code, enhancing the prevention and detection of scams, and aligning reimbursement approaches.
	5	**Data on the extent to which scams are enabled by or take place on different platforms should be regularly published**	Scams ecosystem participants publish regular data on scam activity on their platform. There is clear visibility across the ecosystem where scams are occurring, enabling policymakers and industries to act accordingly.

Barclays' Scams Manifesto makes nine recommendations for actions, based on Frontier's research (2/2)

		Recommendation	Success measure
Data and Information	6	**More scams should be stopped at source by increasing preventative interventions** across the scams ecosystem, enabled by cross-sectoral intelligence and information sharing systems.	A new cross-sectoral data/intelligence sharing framework is created, providing all parties with a clearer understanding of ecosystem vulnerabilities and informing preventative action.
	7	**Payment providers should enhance their abilities to detect scams before they take place** by establishing **real-time data sharing** mechanisms.	Payment providers are enabled (including where necessary through change in legislation and regulation) to make more targeted and impactful interventions to stop scams from succeeding, while allowing legitimate payments to continue unhindered.
Education and Awareness	8	**People should be given better and more regular guidance and education** on the risks of scams, delivered by a coordinated, comprehensive and ongoing education and awareness campaign.	A single unified education campaign on the dangers of scams, and how people can best protect themselves is designed and delivered across sectors of the scams ecosystem. Metrics of customer understanding increase.
Victim Support	9	**People who fall victim to scams, but who have undertaken adequate due diligence, should be reimbursed, funded on the 'polluter pays' principle.**	The creation of a central "ecosystem" funding pot, funded by firms in the scams ecosystem relative to the extent that they enable scams to take place.

Frontier Executive Summary (1/2)

Financial scams are a large and growing problem in the UK…

- **Financial scams in the UK have risen to become a significant problem,** and one beset by challenges in tackling, including; the international nature of fraud and scams, continually evolving fraudster tactics, and difficulties engaging consumers and stakeholders to take action.
- **The problem is getting worse,** with authorised push payment (APP) scams increasingly common**.** This type of scam involves convincing victims to make payments to accounts controlled by a fraudster. **In 2020, APP scam losses reached a record high. In addition to financial losses, victims tend to experience a range of additional emotional harms**.
- As economic activity continues to move online, **digital channels have become the main channel through which contact with victims takes place**, although other channels – particularly Telecoms - continue to be important.

…involving a wide range of sectors

- **While scams ultimately involve a payment being made, the success of a scam relies on finding victims, gaining their trust, and convincing them to make the payments.**
- Fraudsters have developed sophisticated techniques to gain trust and trick victims. These interactions tend to **happen over a prolonged period of time and involve multiple sectors** in a wider 'scams ecosystem'.
- Criminals evolve their tactics to target the weakest link in the chain, and exploit vulnerabilities wherever these arise. **No single action or sector will reduce or eliminate fraudulent activity through acting alone**.

To understand different perspectives on the key problems and potential actions that would make a difference, Frontier interviewed 17 senior individuals from organisations across the scams landscape.

Frontier Executive Summary (2/2)

Those interviewed called for more central leadership

- Those interviewed suggested that **while much has been done to date to tackle scams, in the absence of a different approach scams levels will continue to rise**.
- Stakeholders believe the key to this new approach will be **greater central leadership** to prioritise, standardise and drive the large number of actions being taken, to facilitate **greater information sharing** and better data analytics, **increase the urgency** of actions through building even **greater political support**, and **coordinating consumer messaging** to make it more effective.

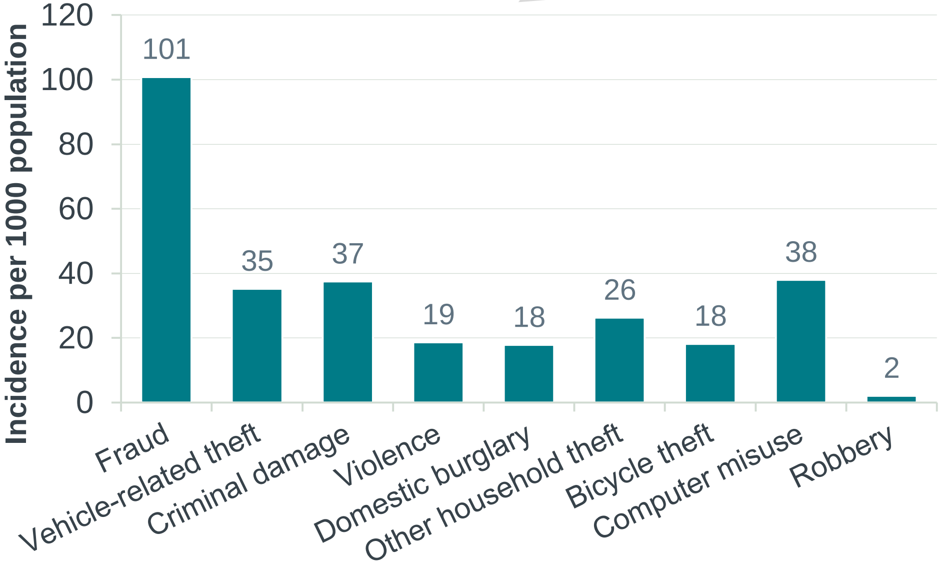
Stakeholder views indicate a new policy framework should drive greater cross-sectoral action across five areas

1. **Data sharing.** Those interviewed suggested more effective data and information sharing within and across industries is required to improve identification, prevention, and disruption of killchains.
2. **Regulation and enforcement.** Stakeholders see a continued important role for regulators and enforcement agencies to coordinate sectoral activities, and remove barriers to effective collaborative actions, where these arise.
3. **Technology.** Stakeholders were clear that all sectors should continue to invest to improve system security, improve detection and prevention, and aid enforcement activity.
4. **Education.** The view of those interviewed was that better joined-up cross-sector efforts to improve messaging would improve engagement, and be more effective in providing individuals with the skills and confidence to spot scams and avoid becoming victims.
5. **Victim support.** Stakeholders believe that all sectors have a role to ensure financial compensation processes work to support victims, and should continue to find better ways to provide greater emotional support for victims of financial scams.

Fraud (including scams) is the most prevalent type of crime in the UK

- The **UK is generally considered to have become a global centre for financial fraud (including scams).** As an English speaking country with a highly digital population, an ageing demographic, and a strong economy, the UK is an attractive source of potential victims for criminal gangs.
- While good progress has been made on tackling ‘unauthorised’ fraud, **criminals have turned their focus towards ‘authorised push payment fraud’, otherwise known as** (and referred to throughout as) **scams** (see box).
- **A number of issues make tackling scams challenging**:
  - There is a strong international element to the activities: **criminal gangs tend not to be based in the UK, and funds that are successfully defrauded are typically moved quickly offshore**.
  - **This means prevention and enforcement measures require significant time and resources**: tracking funds outside UK payment systems is more challenging, and there are added complexities involved in international investigations.
  - Given the potential rewards involved, **criminals have strong incentives to engage in the activity, and continually evolve their processes and scams in order to evade the controls and law enforcement activities** designed to protect individuals.
  - **Scammers often exploit behavioural biases**, making it difficult for consumers to recognise a scam. Engaging consumers around the issue of financial scams is therefore challenging, with consumers often only considering risks after they have fallen victim.

Fraud (inc. scams) has the highest incidence of any type of crime in the UK, more than double the incidence of the next highest categories.

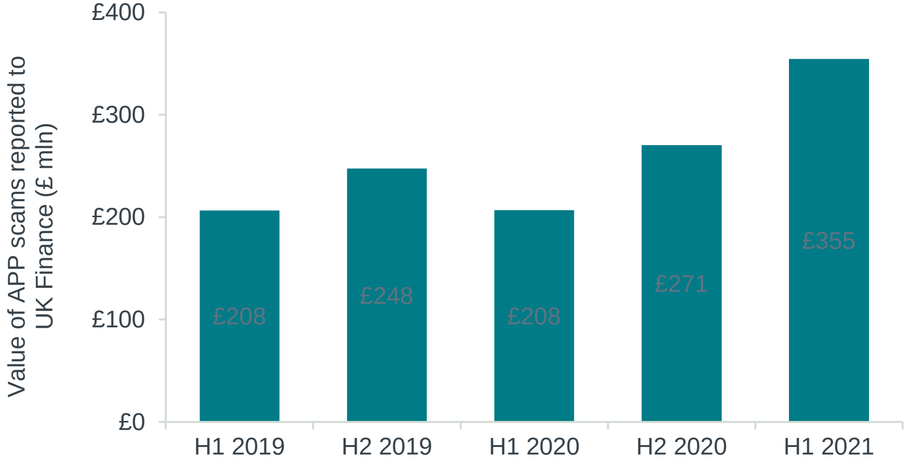


Source: Crime Survey for England and Wales, data coverage May 2020 to April 2021

- **Unauthorised Fraud:** a bank acting on fraudulent requests or instructions that are not authorised by the customer *(e.g. a criminal steals a victim’s card and uses it to make purchases)*.
- **Authorised Push Payment (APP) Fraud (Scams):** a bank acting on genuine customer instructions, but where the customer is being is being convinced to take action not in their best interests by a malicious third party who has gained their trust solely for that purpose *(e.g. a criminal convinces a victim that they are a relative in need, with the victim voluntarily making the payment to them).*
- **Scams ecosystem:** the different stakeholders who are involved or whose systems and platforms are leveraged to perpetrate a scam.

Scams are a growing and worsening problem and victims suffer a wide range of harms - both financial and emotional

Authorised Push Payment (APP) scams are a growing concern, continuing to rise in volume

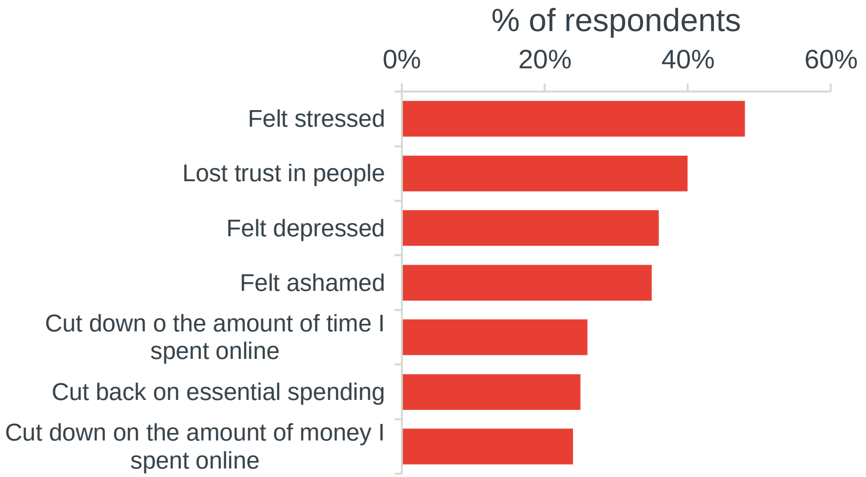


Source: UK Finance 2021 Half Year Fraud Update

- **In an APP scam** victims are tricked into making a payment to an account controlled by a fraudster. This type of scam has become increasingly common.
- **APP scam losses reached a record high of £479m** in 2020 (UK Finance). The true figure is likely to be significantly higher, given many scams go unreported.
- APP scams now **account for almost 50% of all financial frauds** reported by banking institutions to UK Finance.

Victims of these scams suffer a range of emotional harms in addition to potential financial losses

- Whilst most scams are for small amounts of money and victims can be compensated or reimbursed financial losses, **some victims can lose life changing amounts of money.**
- But **financial losses represent only one element of the impacts of scams**. A range of wider emotional harms are reported by victims, with many reporting **significant negative impacts on mental health**. Being scammed often **destroys confidence** and the ability of victims to **trust** people. 40% of online scams victims have felt **stressed** and more than 30% have felt **depressed** as a result of being scammed.

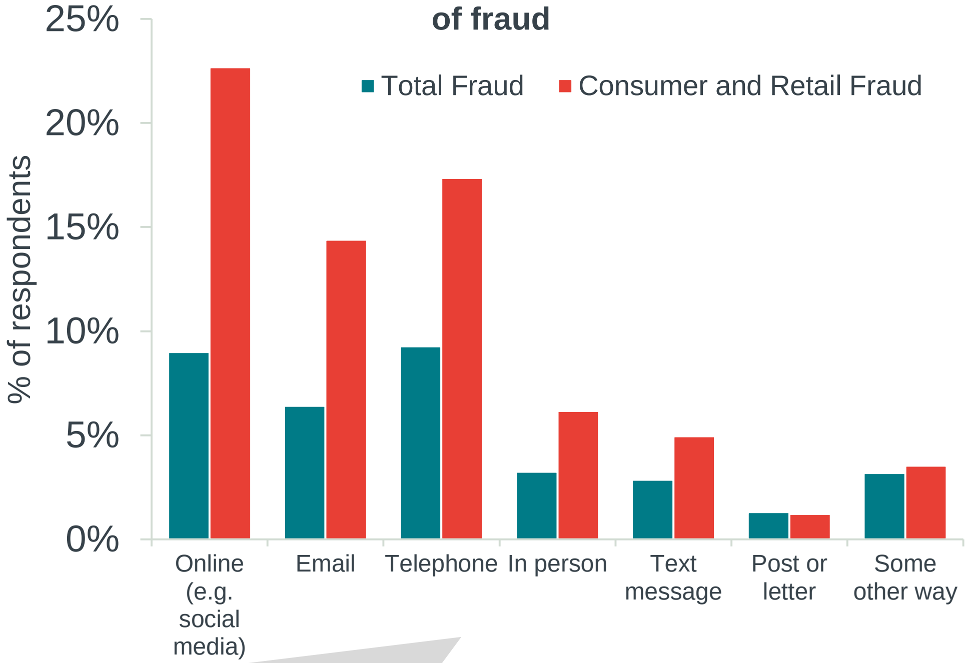


Source: Money and Mental Health analysis of Opinium online survey

Most contact with victims is now initiated online, with the most common scams relating to buying or selling items

As more economic activity moves online, digital channels have become the most common channel through which victims are contacted

First method of contact with offender in incidents of fraud



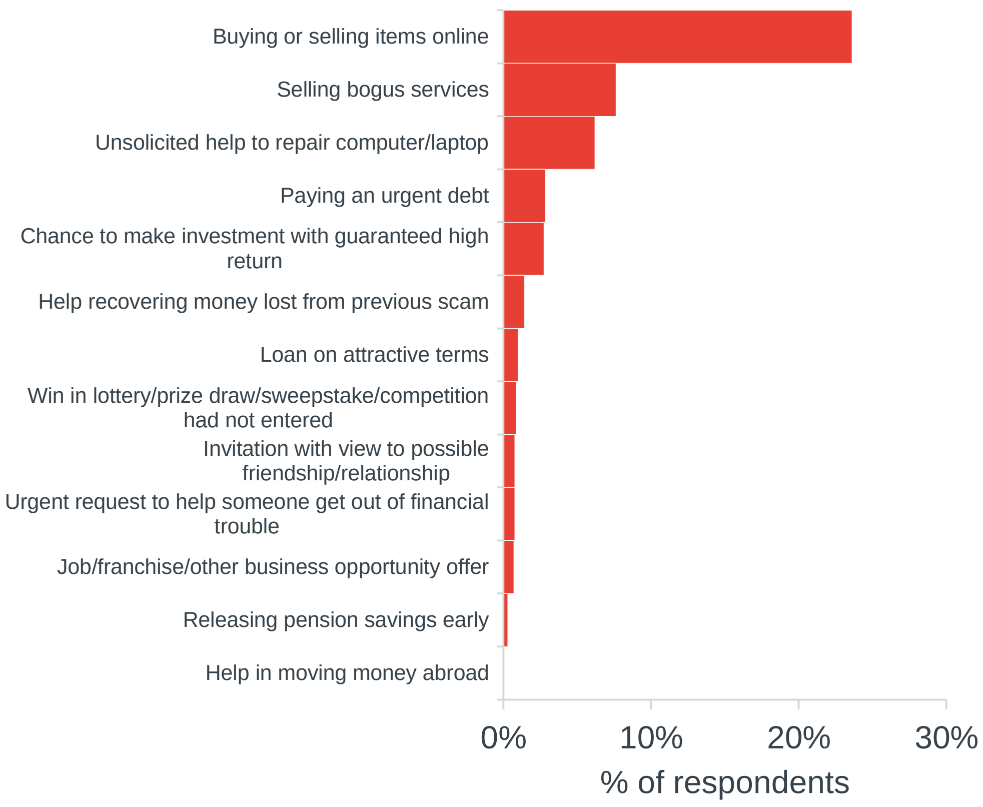
But in general, **scammers will look to exploit all opportunities available.**

Telephone and email remain important channels through which scammers reach their victims.

Source: Crime Survey for England and Wales (2020)
Note: it excludes the category 'no contact'. Figures may not sum up to 100 as more than one response is possible.

Buying or selling items online is by far the most common interaction scammers use to approach and defraud potential victims

Reason for contact with offender in incidents of fraud



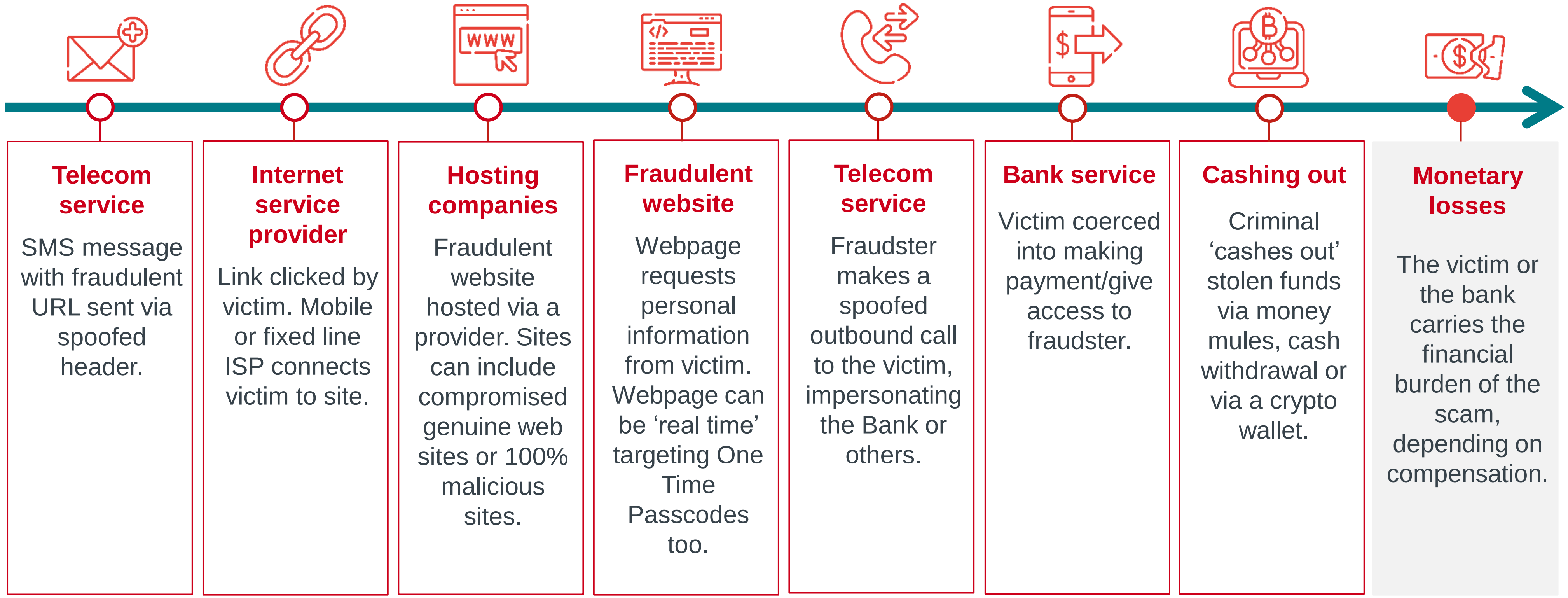
Source: Crime Survey for England and Wales (2020)
Note: it excludes the category 'some other type of request'. Figures may not sum up to 100 as more than one response is possible.

Authorised payment scams rely on finding victims, gaining their trust, and convincing them to make the payments

Fraudsters have developed **sophisticated techniques** to trick victims into making payments. They spend a lot of time and resources finding victims, gaining their trust, and ultimately convincing them to make the payment. This involves **multiple interactions** with the victim.

A helpful way to understand the development of a scam is looking at the 'killchain', which traces out the steps involved.

The diagram below represents an illustrative killchain for Smishing fraud (a scam where fraudsters use mobile phone text messages to trick victims into opening a malicious attachment or link). Similar diagrams can be drawn for other types of scam. As described, there are a range of sectors involved in the initial identification and contact with victims, the route through which actions are taken to build credibility, leading to the fraudulent payment being made.



Telecom service

SMS message with fraudulent URL sent via spoofed header.

Internet service provider

Link clicked by victim. Mobile or fixed line ISP connects victim to site.

Hosting companies

Fraudulent website hosted via a provider. Sites can include compromised genuine web sites or 100% malicious sites.

Fraudulent website

Webpage requests personal information from victim. Webpage can be 'real time' targeting One Time Passcodes too.

Telecom service

Fraudster makes a spoofed outbound call to the victim, impersonating the Bank or others.

Bank service

Victim coerced into making payment/give access to fraudster.

Cashing out

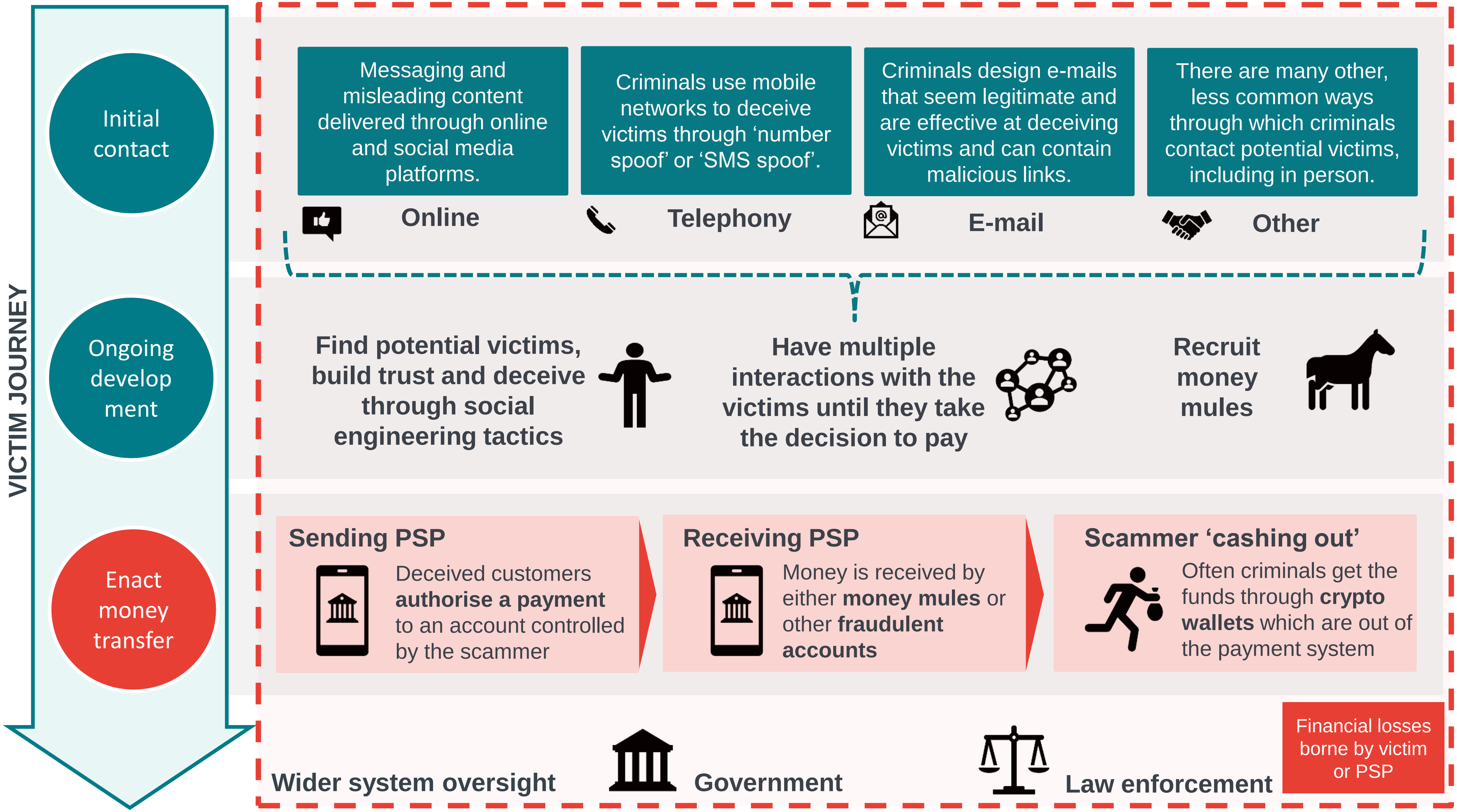
Criminal 'cashes out' stolen funds via money mules, cash withdrawal or via a crypto wallet.

Monetary losses

The victim or the bank carries the financial burden of the scam, depending on compensation.

Source: Based on illustrative example of Smishing fraud killchain, UK Finance

Scams therefore involve multiple sectors and touchpoints between victim and scammer across a wider ‘scam ecosystem’



VICTIM JOURNEY

Initial contact

Messaging and misleading content delivered through online and social media platforms.

Online

Criminals use mobile networks to deceive victims through ‘number spoof’ or ‘SMS spoof’.

Telephony

Criminals design e-mails that seem legitimate and are effective at deceiving victims and can contain malicious links.

E-mail

There are many other, less common ways through which criminals contact potential victims, including in person.

Other

Ongoing develop ment

Find potential victims, build trust and deceive through social engineering tactics

Have multiple interactions with the victims until they take the decision to pay

Recruit money mules

Enact money transfer

Sending PSP

Deceived customers **authorise a payment** to an account controlled by the scammer

Receiving PSP

Money is received by either **money mules** or other **fraudulent accounts**

Scammer ‘cashing out’

Often criminals get the funds through **crypto wallets** which are out of the payment system

Wider system oversight

Government

Law enforcement

Financial losses borne by victim or PSP

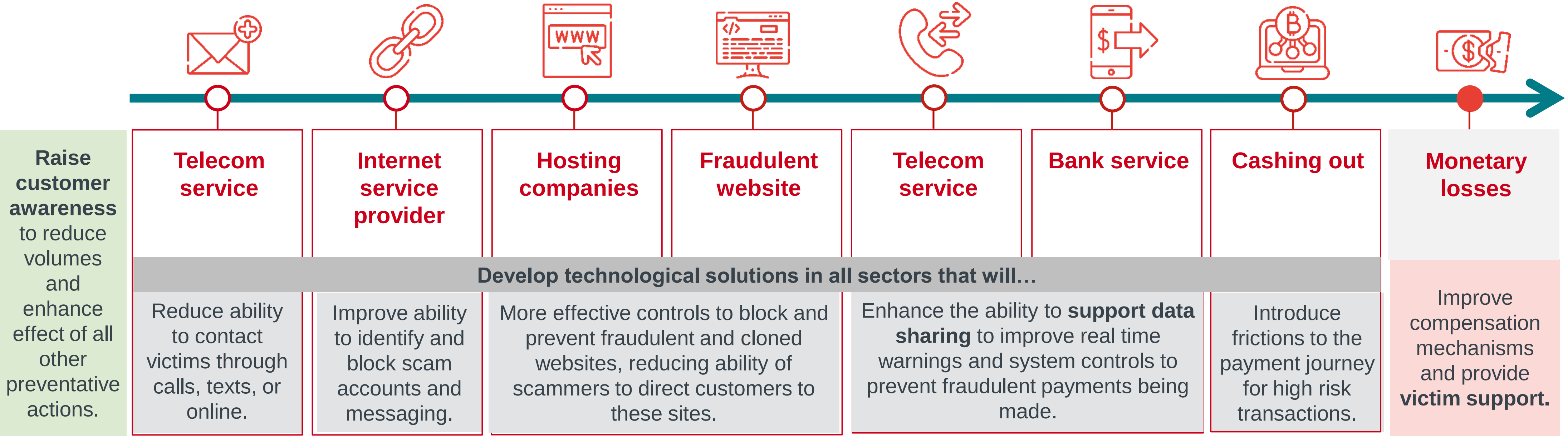
To successfully reduce scams, actions need to take place at all levels of the wider ecosystem

Reducing scam activity requires reducing the incentives for criminals. This can be done by making it **more difficult for the scammers to succeed at all levels of the killchain**, and **reducing the expected rewards** through more effective prosecution and/or fund recovery.

The killchain spans multiple sectors, with multiple entry points and pathways. **Fraudsters evolve their tactics to target the weakest links in the system, and exploit vulnerabilities as and where these arise.**

This suggests successfully reducing the volume of scams activity will require actions at each and every level of the ecosystem

Illustrative actions based on Smishing killchain



Raise customer awareness to reduce volumes and enhance effect of all other preventative actions.

Telecom service

Internet service provider

Hosting companies

Fraudulent website

Telecom service

Bank service

Cashing out

Monetary losses

Develop technological solutions in all sectors that will…

Reduce ability to contact victims through calls, texts, or online.

Improve ability to identify and block scam accounts and messaging.

More effective controls to block and prevent fraudulent and cloned websites, reducing ability of scammers to direct customers to these sites.

Enhance the ability to **support data sharing** to improve real time warnings and system controls to prevent fraudulent payments being made.

Introduce frictions to the payment journey for high risk transactions.

Improve compensation mechanisms and provide **victim support.**

Source: Based on illustrative example of Smishing fraud killchain, UK Finance

We spoke to senior representatives from across the ecosystem to understand their views on how best to tackle financial scams

Given the complex nature of scams and the variety of the elements of the ecosystem, we adopted a two-step approach to our research.

Step 1: desk research

Desk research to map existing trends, describe the ecosystem, understand the range of existing actions and initiatives underway today.

Step 2: stakeholder engagement

In-depth interviews with 17 senior representatives from across the ecosystem to understand difference perspectives.

Synthesis of views from across the ecosystem on the status quo, initiatives to date, and further actions that could be undertaken to help tackle financial scams.

Stakeholders suggest a new approach involving stronger central coordination is required to address the existing upward scams trends

STAKEHOLDER VIEWS

The **description of the ecosystem** and the roles played by the various parties, the scale of the initiatives that have been undertaken over recent years, and the **upward trends in case numbers are all well understood** and are uncontentious for members of the ecosystem.

But while according to them the scale and pattern of activity to prevent and disrupt financial scams has been significant, **this has clearly not been sufficient to control and reduce scams levels**.

There is widespread pessimism among stakeholders that **scams levels will continue to rise, in the absence of a different approach.**

Stakeholders believe the key to this new approach would be **more central ownership and leadership**. This is critical to help prioritise, standardise and drive the large number of actions being taken.

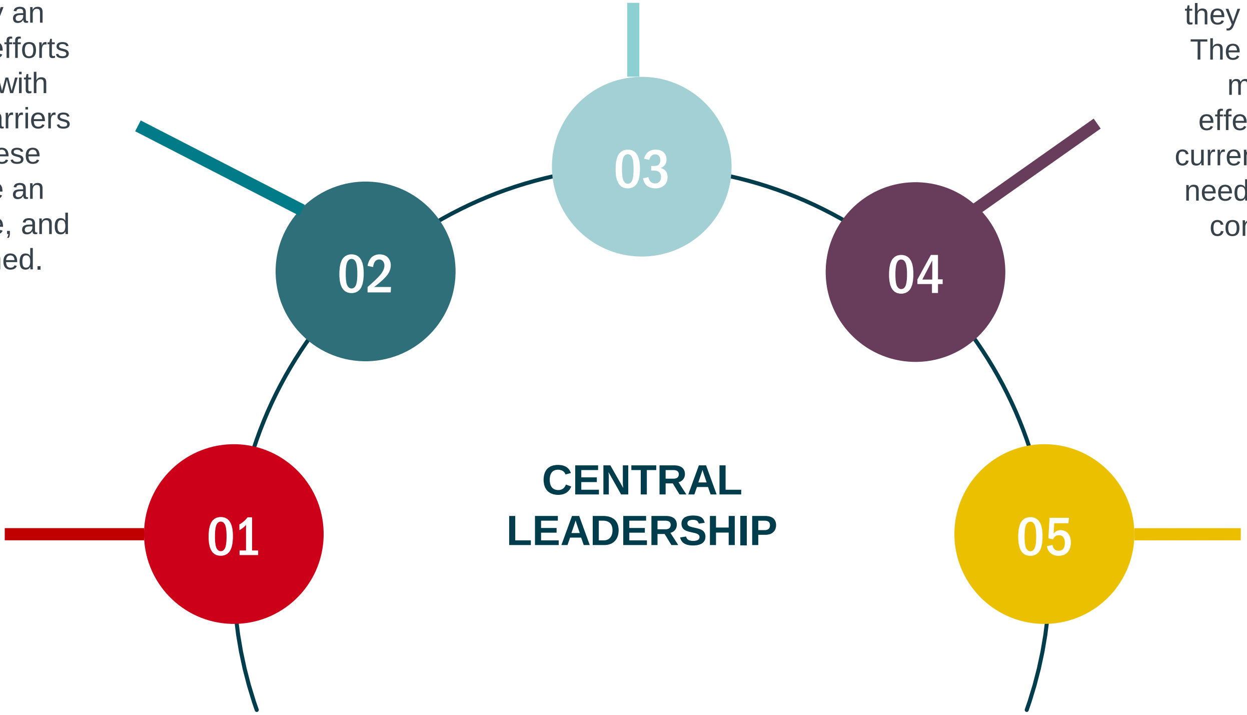
Coordination and central leadership is required to help drive and target efforts, and facilitate greater **cross-sector** collaboration.

Stakeholders' priorities for central coordination would include:

- facilitating **greater information sharing** and joint initiatives to **create better data analytics** and actionable insights to disrupt the killchain e.g. setting up a centralised system to enable data sharing across industries (similar to the proposed EU MISP);
- **greater clarity in the legal requirements in relation to data**, to allow all relevant organisations to share more data with one another;
- making tackling **financial scams a higher Government priority,** pushing it up the political agenda;
- greater emphasis on **Government-led education campaigns;**
- **coordinating consumer messaging** to a central voice, increasing cut through with a consistent simple messages, designed through behavioural insight;
- **setting up a long-term funding solution for victims of scams**; and
- **scaling up successful disruption practices more quickly** to spread learning faster.

Stakeholder views indicate a new policy framework should cover five specific areas for greater cross-sectoral action

Beyond the general call for greater central leadership, **discussions with stakeholders raised a large number of actions** that different parties believe would have a positive impact on tackling financial scams. These views, together with Frontier desk research suggests a **new policy framework would cover five specific areas** where the ecosystem believes efforts should focus to have the most impact.



Data and information sharing

Those interviewed suggested that data and information sharing across and within sectors should be improved to better identify fraudulent activity at the outset, and help providers build and deploy more effective tools to prevention and disrupt killchains.

Regulation and enforcement

Stakeholders believe that regulatory and enforcement bodies play an important role in coordinating efforts within their sector, engaging with other sectors, and removing barriers to effective actions where these arise. This will continue to be an important role as scams evolve, and new interventions are designed.

Technology

Stakeholders were clear that better technology is at the heart of an effective fight against scams. Continued improvements to the systems already in place is required, and new technological solutions will need to be designed to keep pace with criminal innovations. These actions will be needed to increase the security of existing systems, improve detection and prevention, and aid enforcement activities.

Education and awareness

When customers are aware of scams, they are less likely to fall victim to them. The view of those interviewed was that more can be done to improve the effectiveness of campaigns which are currently disparate. Better engagement is needed to give individuals the skills and confidence to spot scams and avoid becoming victims.

Victim support

More can be done to improve financial compensation processes. Stakeholders believe that providing emotional support for victims will continue to be important, and more should be done to improve on existing actions.

Barclays’ Scams Manifesto Recommendation: 1

Coordinated Framework

A single Government entity or appointed individual should be designated as the ‘Scams Lead’ to align Government, regulators and industries’ responses to tackling scams, with defined responsibility to drive meaningful change in legislative, regulatory and firms’ strategies.*

Success measure

Appointment of a single entity or individual tasked with delivering a comprehensive response to tackling scams that aligns the activity of different policy makers, regulators and industries.

- **Recent years have seen a range of different policy, regulatory and industry-led actions** to combat the growth in scams. This is welcome; such activities are absolutely necessary as part of tackling those who perpetrate these crimes. However, **action is currently fragmented**, with initiatives operating in silos and enabling criminals to adapt and continue targeting victims.

- Building on the Treasury Select Committee’s recommendation that policy responsibility should be centralised into a single Government department, we recommend that Government should go further and **appoint a Scams Lead- a single Government entity or appointed individual to coordinate and drive all legislative, regulatory and industry action to tackling scams** across all sectors, enabling a comprehensive response that closes vulnerabilities being exploited by criminals, and therefore prevents scams at source.

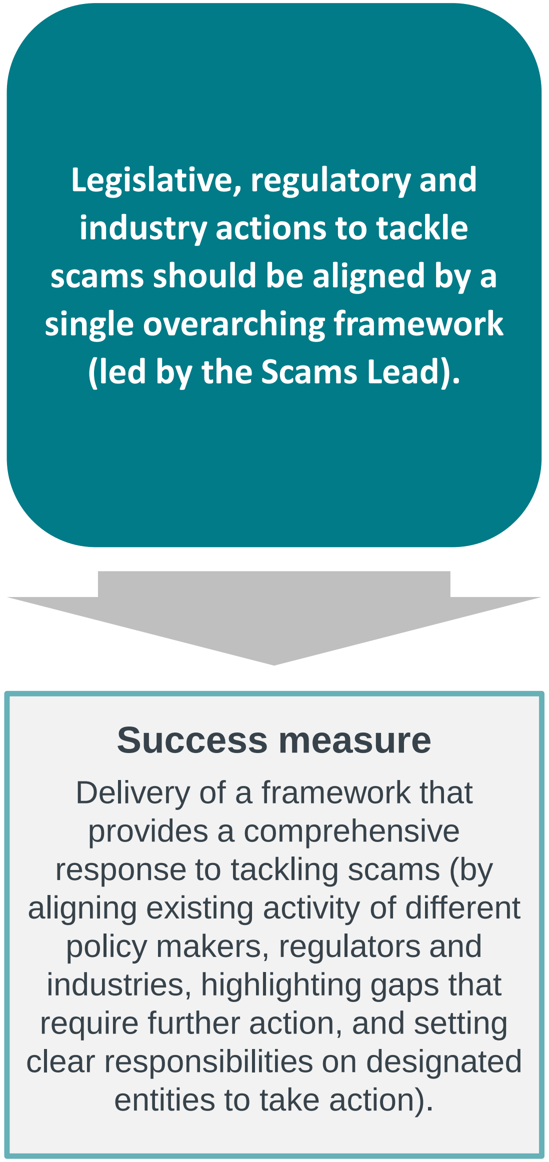
- The **Scams Lead should be afforded sufficient competencies and authority to define and actively deliver the required outcomes**. They would work with industry on voluntary actions, as well as the relevant Government departments and regulators to drive change (through existing political and regulatory powers where these exist today, and recommending new powers where they do not).

- The Scams Lead would operate on a comparable (but broader) basis to the leadership of the Access to Cash Action Group (CAG); jointly accountable to the Chancellor, Home Secretary and FCA CEO, or alternatively to the Economic Crime Strategy Board (ECSB) for delivery.

** The term ‘industries’ refers to all sectors and firms that are part of the “scams ecosystem”, including but not limited to: retail banking and payment firms; technology platforms; social media and e-ecommerce sites; telecommunications firms and dating websites.*

Barclays’ Scams Manifesto Recommendation: 2

Coordinated Framework



Legislative, regulatory and industry actions to tackle scams should be aligned by a single overarching framework (led by the Scams Lead).

Success measure

Delivery of a framework that provides a comprehensive response to tackling scams (by aligning existing activity of different policy makers, regulators and industries, highlighting gaps that require further action, and setting clear responsibilities on designated entities to take action).

- A **single overarching response framework is required to tackle scams**, bringing together the various Government, regulatory and industry initiatives and supplementing them as required.
- To enable this, the **Scams Lead should review the current landscape**, then set out how and where scams occur and the current legislative, regulatory and industry responses. They should then **identify gaps that exist, or where further action or coordination is required**.
- **Government, regulators, consumer groups and industry stakeholders should all contribute**, as well as existing scams focused organisations, including Stop Scams UK (SSUK), the Cyber Defence Alliance (CDA) and UK Finance (UKF).
- The output of the review should be **authoritative recommendations on the actions required** to address any issues presented. This response **framework should be sector-agnostic**: specifying the overall actions required to minimise the prevalence of scams, establishing the actors best placed to enact these, and placing sufficient incentive or requirements on them to ensure this takes place. It should also be endorsed by the Economic Crime Strategy Board (ECSB) and guide its focus.

Barclays’ Scams Manifesto Recommendation: 3

Regulation and Enforcement

Where voluntary industry action is insufficient, gaps in the prevention of scams should be resolved through mandated legislative or regulatory intervention.

Success measure

Government and regulators make timely interventions across the ecosystem to require or enable action to prevent scams.

- It is only through concerted effort from all members of the scams ecosystem that scams can be prevented at source and customers can be protected. **All sectors should therefore take action** to close these vulnerabilities.

- The **preferred approach to preventing scams is for relevant industries to take voluntary action** to close down any vulnerabilities, either unilaterally or through working through cooperative forums such as Stop Scams UK (SSUK), the Cyber Defence Alliance (CDA) and UK Finance (UKF). These organisations have made good progress in recent years, and their efforts should be supported and continued

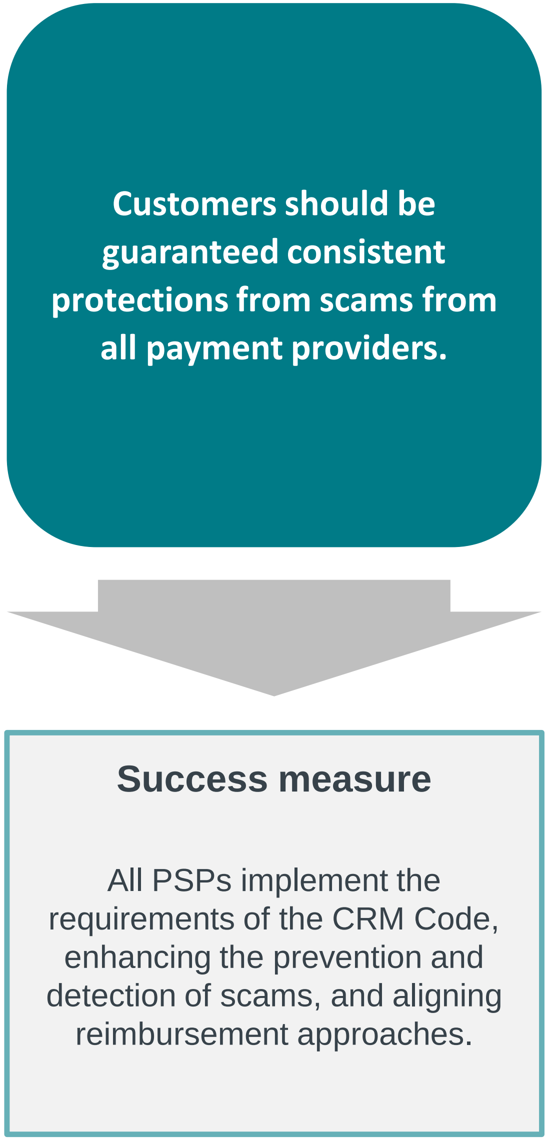
- But where the **Scams Lead’s review identifies gaps in the current response to tackling scams**, where there is insufficient and/or inconsistent voluntary action being taken by industry, or where the nature of the challenge means that a voluntary response is not practical or possible, **Government and/or regulators should take legislative or regulatory action to address this.** This could include common outcome focused minimum standards to ensure a consistent and uniform approach is taken to closing vulnerabilities.

- This should be an **ongoing and dynamic requirement**, responding to emerging vulnerabilities and changes in tactics by criminals.

- Recognising that implementing legislative and regulatory changes will necessarily take some time, **the new framework should be accompanied with a ‘comply or explain’ approach from Government and regulators**, to help incentivise rapid adoption of the new framework.

Barclays' Scams Manifesto Recommendation: 4

Regulation and Enforcement



Customers should be guaranteed consistent protections from scams from all payment providers.

Success measure

All PSPs implement the requirements of the CRM Code, enhancing the prevention and detection of scams, and aligning reimbursement approaches.

- Payment providers play a key role in detecting and preventing scams. While the voluntary creation of the **Contingent Reimbursement Model (CRM) Code** was a welcome step forward in aligning the actions of signatories to create consistent customer experiences, it **should be made mandatory by the PSR** for all payment providers so that customers can be guaranteed of its protections regardless of their provider.

- While this new requirement is implemented, the **Scams Lead and/or regulators should highlight those firms that have signed up to the Code, and those that have not**, enabling consumers to take informed choices.

Barclays’ Scams Manifesto Recommendation: 5

Regulation and Enforcement

Data on the extent to which scams are enabled by or take place on different platforms should be regularly published.

Success measure

Scams ecosystem participants publish regular data on scam activity on their platform. There is clear visibility across the ecosystem where scams are occurring, enabling policymakers and industry to act accordingly.

- Policymakers, regulators and industry require data to understand how and where scams are occurring, and the role that different organisations play in enabling them, to inform appropriate responses.

- The **PSR’s recent proposals* for payment providers to publish data on their reimbursement approach are welcome, but should be expanded** to require them to also include data regarding the enablers of scams – namely the vulnerabilities in the wider ecosystem that allow APP scams to take place.

- Similarly, **other participants across the scams ecosystem should be required to publish data on how their platforms and infrastructure are being exploited** to enable scams to take place, and the preventative action they are taking in response.

- As with Recommendation 3, this should **initially be on a ‘comply or explain’ basis**, while steps are taken to require this by law or regulation.

- The routine publication of such data would enable a clear assessment of the key vulnerabilities that are being exploited by criminals to perpetrate scams, and would enable Government, regulators and industry to take appropriate steps to close them.

- More broadly, it is likely that the very act of having such information in the public domain would be enough to incentivise the relevant firms and sectors to proactively take action, closing down vulnerabilities and therefore protecting customers without intervention from others.

* https://www.psr.org.uk/publications/consultations/cp21-10-authorised-push-payment-app-scams-consultation-paper/

Barclays’ Scams Manifesto Recommendation: 6

Data and Information

More scams should be stopped at source by increasing preventative interventions across the scams ecosystem, enabled by cross-sectoral intelligence and information sharing systems.

Success measure

A new cross-sectoral data/intelligence sharing framework is created, providing all parties with a clearer understanding of ecosystem vulnerabilities and informing preventative action.

- Individual firms’ abilities to prevent scams are today necessarily limited as they are only able to monitor and assess the parts of the ‘scam journey’ that they have sight of. For example, a bank will only see the victim’s activity from the point at which they attempt to make a payment. An online social media platform may only see the victim’s initial engagement with the criminal.
- The **systematic (including real-time) sharing of data between different sectors** of the ecosystem (e.g. between payment providers, technology and telecommunication firms) will **create a richer dataset that could be analysed by all parties to identify more impactful preventative strategies**. This would build on good practice already established in the field of cyber-security.
- For example, a telecommunications firm could share data regarding numbers potentially compromised in a smishing attack with payment providers, enabling them to proactively enhance impacted customers account protections. Similarly a social media firm could share data regarding customers who have engaged with fraudulent adverts.
- It **would also enable policy makers and regulators to understand in more detail the specific interventions that they can undertake** to have the maximum impact in preventing scams from occurring in the first place.
- There is already **good work underway between a number of firms and organisations to enable such data sharing**, including Stop Scams UK (SSUK) and the Online Fraud Steering Group (OFSG). These organisations’ efforts should be supported and extended in developing effective processes for more comprehensive data sharing across sectors.

Barclays' Scams Manifesto Recommendation: 7

Data and Information

Payment providers should enhance their abilities to detect scams before they take place by establishing real-time data sharing mechanisms.

Success measure

Payment providers are enabled (including where necessary through change in legislation and regulation) to make more targeted and impactful interventions to stop scams from succeeding, while allowing legitimate payments to continue unhindered.

- **Payment providers should implement the ability to share real-time data with each other** that indicates a scam is likely to take place (whether with respect to a sending or receiving account), allowing the data's recipient to take preventative action.

- The **adoption of such technologies would enable more advanced detective processes to be implemented**, allowing more targeted intervention that prevents criminal activity without impacting genuine payments.

- As a specific example of this, **all payment providers should adopt Confirmation of Payee** (CoP), ensuring that regardless of which provider a customer looks to make (or receive) a payment via, the payment is assessed to ensure that the recipient's information is as expected.

- There is **already good work underway between different payment providers to design and build richer data sharing**, including that coordinated by UK Finance (UKF) and Pay.UK. Such work should be supported and continued

Barclays' Scams Manifesto Recommendation: 8

Education and Awareness

People should be given better and more regular guidance and education on the risks of scams, delivered by a coordinated, comprehensive and ongoing education and awareness campaign.

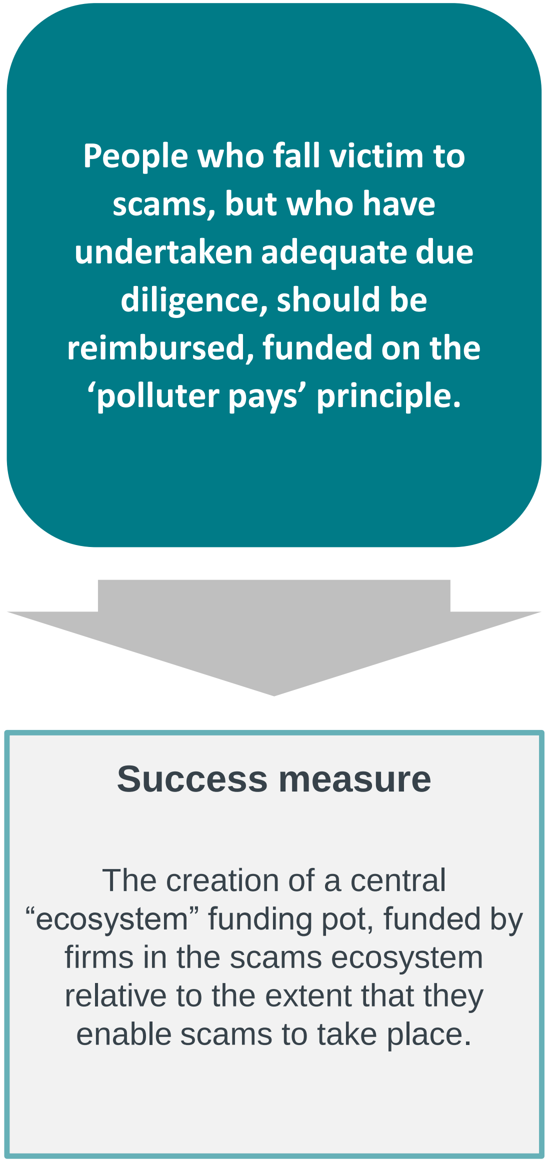
Success measure

A single unified education campaign on the dangers of scams, and how people can best protect themselves is designed and delivered across sectors of the scams ecosystem. Metrics of customer understanding increase.

- A **critical element in preventing scams is educating people** to reduce the risk that they fall victim to criminals.
- A wide range of education initiatives are underway today from different organisations, entities and firms, using different messages and approaches. There is a risk this variation creates opportunity for scammers to exploit uncertainty or that different messages fail to cut through.
- **Simplified and aligned messaging** delivered across the scams ecosystem (in a contextual manner and as close to real time moments of risk as possible) **would likely be much more successful than uncoordinated and unaligned messaging**.
- **All participants in the scams ecosystem should therefore collaborate and coordinate** efforts to educate customers on the risks of scams, through a unified messaging campaign. This could be delivered through support from a wider range of organisations for the "Take 5" education and awareness campaign.

Barclays’ Scams Manifesto Recommendation: 9

Victim Support



People who fall victim to scams, but who have undertaken adequate due diligence, should be reimbursed, funded on the ‘polluter pays’ principle.

Success measure

The creation of a central “ecosystem” funding pot, funded by firms in the scams ecosystem relative to the extent that they enable scams to take place.

- Victims who have acted responsibly (i.e. who have taken appropriate self-protection steps, but have still been defrauded) should be guaranteed reimbursement.
- Where payment providers have been at fault it is right that they have a legal obligation to reimburse victims.
- **For cases where payment providers are not at fault, and where the victim is also deemed not to be at fault, a central “ecosystem blame” pot should be established** to fund reimbursement. This should be funded on the “polluter pays” principle, whereby those who enable a scam to take place provide funding. This aligns with the Treasury Select Committee’s suggestion that Government should seriously consider requiring online companies to contribute compensation when fraud is conducted using their platforms.
- The mechanism by which such contributions are determined should be designed as part of Recommendation 2 (the overarching scams framework), and can be based on data provided as part of Recommendation 5 (publishing data about the scams ecosystem). This will appropriately incentivise firms across the scams ecosystem to do more to prevent their infrastructure from being exploited by criminals.