Treasury Committee Inquiry on Economic Crime

Barclays is a transatlantic consumer and wholesale bank with global reach, offering products and services across personal, corporate and investment banking, credit cards and wealth management, with a strong presence in our two home markets of the UK and the US. With over 325 years of history and expertise in banking, Barclays operates in over 40 countries and employs approximately 85,000 people. Barclays moves, lends, invests and protects money for customers and clients worldwide.

Barclays welcomes the opportunity to response to the Committee's inquiry.

Executive Summary

Consumer Fraud and Scams

Fraud and scams are one of the fastest growing types of crime in the UK, with fraudsters increasingly leveraging online digital platforms (e.g. social media, online marketplaces, and dating websites) to manipulate consumers into willingly sending money as part of an Authorised Push Payment (APP) scam. Unfortunately, fraudsters are now adapting common scam techniques making them relevant to Covid 19, in order to take advantage of the pandemic.

Combatting these criminals, and preventing fraud and scams is a priority for Barclays and the broader financial services sector. Through the Contingent Reimbursement Model Code, the retail banking sector has taken significant action to ensure that scam victims are reimbursed where they take appropriate self-protection measures. However, we firmly believe that further action is required to properly protect consumers.

Firstly, to ensure all customers in the UK are protected by the CRM Code regardless of who they bank with, Government should legislate to make the Code mandatory for all banks and payment service providers.

Secondly, Government should publish a roadmap setting out plans to secure a sustainable long-term funding source for reimbursement of victims in 'no-blame' APP scam scenarios. Two potential funding sources that Government should consider include: i) broader funding from the ecosystem abused by fraudsters; and ii) frozen funds suspected as being the proceeds of crime.

Thirdly, Government should take action to increase the responsibility of key firms and sectors across the ecosystem to prevent scams at their source. Practically, Government should require all relevant organisations across the ecosystem to share information regarding the volume of economic crime related activity undertaken. Government can then assess the role of different sectors in enabling economic crime, and determine appropriate responsibilities of these sectors in both prevention and reimbursement.

Finally, Government should review the relevant legislative framework to address any challenges to the repatriation of funds to victims, where the flow of funds between accounts and banks can be clearly identified.

Anti Money Laundering

Significant progress has been made since the Committee's previous Economic Crime Inquiry in 2018: the Government has established the Economic Crime Strategic Board (ECSB), which has since published the UK Economic Crime Plan for 2019-2022; the Government has consulted on the introduction of an Economic Crime Levy; and the model of the Joint Money Laundering Intelligence Taskforce (JMLIT) has been reviewed to optimise it for the future. While these are all positive developments, further action is required to ensure the UK remains a hostile environment for economic crime.

The most significant action is reform of the current Suspicious Activity Reporting (SARs) framework. An enhanced SARs tool, enabling better data analytics and the efficient flow of information between the regulated sector and the authorities, is critical to ensuring that SARs can be converted into meaningful law enforcement outcomes.

We believe the proposed reforms to Companies House will also have a significant impact in the fight against economic crime and should be prioritised for legislative implementation. In the meantime, it is vital that action is taken under the current framework of rules where possible to reduce abuse of Companies House.

The Government's proposed Economic Crime Levy, would aim to raise approximately £100 million per year from AML regulated entities, to support the economic crime policy agenda. Barclays supports an appropriately designed and effectively administered Levy, which we believe could provide a sustainable funding source for combatting economic crime into the future.

Finally, a key challenge in the fight against economic crime in the UK is the relatively slow pace of reform. To increase the pace of reform, government should consider reform through regulatory guidance, as seen in other jurisdictions.

CONSUMER FRAUD AND SCAMS

The Fraud and Scams Landscape

With £1.2bn stolen by fraudsters in 2019, fraud and scams are one of the fastest growing types of crime in the UK. Digitalisation and the proliferation of the internet into everyday life has enabled this rapid growth. Whereas in recent decades, scams would be undertaken in person, through print media or over the phone, fraudsters are adapting their methods and leveraging online digital platforms (including social media, online marketplaces, technology platforms, and dating websites) to engage and manipulate consumers into willingly sending money as part of an Authorised Push Payment (APP) scam.

The scams undertaken by fraudsters are varied, innovative and can be very convincing, with common examples including purchase scams, romance scams, investment scams, and invoice scams. (See UK Finance report: Fraud - The Facts 2020 for a fuller overview of common scam techniques). Indeed, the issue of fraud and scams is only getting worse with the total value of funds lost through APP scams in 2019 increasing 29%, the number of reported cases increasing 45%[1], and over £207 million lost in the first half of 2020[2].

Stopping these economic criminals - and the pain and loss they inflict – is therefore a key priority for Barclays and the broader industry. The financial services sector has established various initiatives and is taking significant action to both educate consumers and reduce their risk of falling victim to a scam, and combat the criminals directly to prevent their crimes succeeding.

However, there is a limit to how much the financial services sector can practically achieve in preventing scams alone. While making a payment at a bank may be the last stage in the process, victims will often have been manipulated by fraudsters through other channels, before they reach the point of sending funds. Therefore, to effectively prevent and reduce the number of successful scams, these other channels in the ecosystem need to be incentivised to take coordinated and concerted action, and be held responsible where they fail to do so.

A comprehensive solution to the ever growing threat of scams therefore requires a change from the current sectoral and siloed approach, to a comprehensive ecosystem-wide strategy that, we believe, will be far more effective in tackling economic criminals, and protecting consumers.

Fraud and Scams in the Covid 19 Pandemic

Unfortunately, fraudsters are using the sense of uncertainty and fear during the Covid pandemic to take advantage of vulnerable people and businesses. They are adapting common scam techniques, making them relevant to the pandemic, in order to manipulate and deceive consumers. Specific examples include:

- **HMRC refunds or pay-outs -** Texts and emails impersonating HMRC and the government offering a pay-out or a refund, and asking the consumer to click a link, which leads to a fake site.

[1] UK Finance Report: Fraud - The Facts 2020.

[2] UK Finance Report: Half Year Fraud Update 2020

- **NHS Test and Trace –** Fake NHS Test and Trace service communications asking for financial details, PINs or passwords, or requesting consumers click links or move money.
- **Fake adverts -** Fraudsters placing adverts on social media for goods at bargain prices – e.g. protective masks, clothes, and games consoles to pets.
- **Campaigns or charities Raising money -** Fake websites purporting to be raising money for research into cures, or funds for victims, to get donations.
- **Company pay-outs or refunds -** Posing as legitimate holiday, insurance or entertainment companies, fraudsters contact consumers about a genuine refund that they're expecting. They might know some of their personal details and request more information or money.
- **Courier fraud** - Seemingly helpful people offering support with shopping for essentials, and asking for a consumer's bank card and PIN.
- **Scam emails – relating to:**
    - an app tracking coronavirus using an interactive map
    - NHS goodwill gestures
    - Business working conditions or policies
    - Information about hospitals in affected areas
    - Mortgage repayment holidays or rent relief
    - Parcel shipping cancellations
    - Money transfer requests for victims trapped abroad
    - Services claiming they can diagnose coronavirus
    - The World Health Organisation (WHO)

The below table provides the percentage change in the value and volume of various scams taking place since the beginning of the pandemic.

Scam Type	Volume % Increase since Covid	Value % Increase since Covid
Advance Fee Scam	**45%**	**41%**
Impersonation – Other	**58%**	**47%**
Impersonation – Police or Bank Staff	**72%**	**130%**
Investment Scam	**34%**	**107%**
Invoice and Mandate Scam	**-32%**	**5%**
Purchase Scam	**0.30%**	**10%**
Romance Scam	**38%**	**83%**

Authorised Push Payment Scams

As the Committee is aware, in 2019, the retail banking industry introduced the Contingent Reimbursement Model (CRM) Code, a voluntary code which provides measures to help prevent fraud from taking place, and establishing guidelines to determine the circumstances in which victims should be reimbursed by their bank. The Code is a positive step in the fight against scams, and ensures that where customers have taken reasonable self-protection steps, but have still fallen victim to fraud or a scam, they are reimbursed.

However, it is only a first step, and far greater action is required if consumers are to be properly protected. Taken together, we believe these further actions will reduce the prevalence of APP scams, and provide sustainable source of funding for no-blame scenarios.

1. Legislation to Mandate an Updated CRM Code

The Code is currently only a voluntary initiative. While nine firms are signatories and participants to the Code, there are many other significant firms that are not signatories, meaning customers of those firms do not necessarily receive the protections provided for in the Code. We believe that all customers in the UK should be protected under the Code regardless of who they bank with.

Additionally, the Lending Standards Board (LSB) is currently undertaking a review of the Code to see how it could be improved. The Code should provide greater clarity as to what the expected responsibilities of all participants are, and what constitutes effective efforts at prevention by banks. This will remove current uncertainty, and provide a clearer expectation of outcome for all participants.

As an immediate next step, and in line with the Committee's recommendation from its 2018 Economic Crime Inquiry, Government should legislate to make the CRM Code mandatory for all banks and payment service providers. Government should reflect any updates to the Code following the LSB review in any moves to legislate the Code.

2. Securing a Long-Term Funding Solution for 'No-Blame' Scenarios

Currently, scam victims in 'no blame' scenarios (where it has been established that both the bank and the customer took reasonable steps to protect against scams, yet the scam still succeeded) are reimbursed from a temporary central fund. This fund has been voluntary funded by Code signatories as a temporary measure whilst a long-term funding mechanism for such cases is established.

As the Committee may be aware, a range of funding solutions have been explored, but none have proved acceptable to all stakeholders. Whilst we remain of the view that we do not wish to see consumers lose their reimbursement in no-blame cases, we also note that it is not sustainable for Code signatories to continue to fund such cases ad infinitum. Barclays therefore believes that, alongside the legislation to mandate the CRM Code, Government should publish a roadmap setting out its plans to secure a sustainable long-term funding source for reimbursement of victims in 'no-blame' APP scam scenarios.

There are two potential funding sources that Government should consider: i) funding from firms that are also utilised by fraudsters to facilitate scams; and ii) frozen funds suspected as being the proceeds of crime.

i) Funding from Firms Across the Broader Ecosystem

As set out previously, both fraud and scams take place in a complex ecosystem, with fraudsters taking advantage of linkages across firms in many different sectors. All firms across this ecosystem leveraged by fraudsters, should have clear obligations and responsibilities placed upon them to minimise the extent to which fraudsters are able to operate on their platforms. Where firms do not act to meet this responsibility, these firms should be held responsible for any losses incurred by victims as a result of their lack of action. This would most easily be achieved by requiring such firms to make contributions to the existing 'no blame' fund.

This would mean that, unlike the situation today, where banks are responsible for reimbursing victims in situations where it is clear there is no further action they could have taken to prevent the scam, responsibility for reimbursement of victims would be placed on the organisation that facilitates the scam, regardless of their sector.

ii) Funding from the Proceeds of Crime

Alongside funding from other firms across the ecosystem that enable scams, Government should consider the extent to which funds held by firms in suspense accounts - on the basis that they are suspected proceeds of crime - could contribute towards a sustainable funding model for the reimbursement of scam victims in 'no blame' scenarios.

Funds held by banks in suspense accounts include funds suspected to be the proceeds of scams and fraudulent activity. These funds rightfully "belong" to the victims of that criminal activity, but those victims cannot reasonably be identified in order for the funds to be returned. Given that such funds originate in criminal activity, and are currently not being used for any socially beneficial purpose, it would seem logical and appropriate that they be used to reimburse victims of economic crime. Government should explore whether these funds could provide a source of funding for 'no blame' scenarios, potentially using the Dormant Assets framework as a model. Such a use of these funds would sit alongside the commitment in the Government's Economic Crime Plan to repatriate more funds to victims.

3. Increasing Responsibility of Key Firms and Sectors to Prevent Scams at their Source

While action to ensure scam victims are reimbursed is positive from a consumer perspective, significant numbers of scams are still taking place, creating distress for consumers and funding criminals. Barclays therefore believes Government should take a number of actions - which could be achieved by bringing Economic Crime into scope of the Online Harms Bill - to prevent scams taking place in the first place.

As a practical first step, Government should require all relevant organisations across the ecosystem to share information with a central entity regarding the volume of economic crime related activity undertaken through their platforms. Government should then review such data to assess how other sectors are playing an enabling role in economic crime, and determine the appropriate responsibilities of these sectors in both prevention and reimbursement. The routine collection and publication of such data could be achieved via the proposed Online Harms Bill, or through the Home Office's Sector Charters, and would help provide a deeper understanding of fraud and scams.

Further, we believe Government should look to bring together key players across the ecosystem (building on the work of Stop Scams UK and UK Finance) to agree a collaborative approach to stopping scams at their source.

Finally, we believe Government should create a taskforce to establish a detailed understanding of the ecosystem, and devise a series of policy responses designed to combat those responsible.

4. Repatriation of Stolen Funds

As identified by the Committee in its 2018 Inquiry, one of the challenges currently faced by banks is that, whilst they may able to identify where funds could be the proceeds of fraudulent activity using the Mule Insights Tactical Solution (MITS), they are not always able to repatriate those funds back to the victim.

Where a bank suspects that a customer holds proceeds of crime, it cannot take any action in relation to this property without having obtained consent from the NCA, otherwise it risks committing a money laundering offence and creating a civil liability between the banks and the customer. Whilst the Proceeds of Crime Act enables firms to report suspicion to law enforcement, and enables law enforcement to then take steps to restrain and recover such property, it does not provide a clear framework enabling victims to recover their property or guidance to the firm on balancing its obligations. This is significant, particularly given that law enforcement will only restrain and recover a small fraction of all of the suspected proceeds of crime reported to them. This, in part, is why firms continue to hold significant balances of suspected proceeds of crime in suspense accounts.

Government should review the relevant legislative framework to address any challenges to the repatriation of funds to victims, where the flow of funds can be clearly identified.

ANTI-MONEY LAUNDERING

The AML Landscape

Since the Treasury Committee's previous Inquiry on Economic Crime in 2018, the UK has seen substantial progress in the fight against economic crime.

Firstly, the Government has established the Economic Crime Strategic Board (ECSB), a board chaired jointly by the Home Secretary and the Chancellor, and comprising senior leaders from the UK financial services sector, intended to orchestrate the national response to economic crime in the UK. The ECSB has also since published the Economic Crime Plan for 2019-2022, setting out the UK's strategic priorities and ambitious deliverables to provide enhanced capability for the prevention and detection of economic crime in the UK. The plan represents a long-term commitment in the UK to improving efforts to combat economic crime while providing the necessary investment to ensure the UK can combat a constantly changing landscape.

The Government has also recently consulted on the introduction of an Economic Crime Levy, aiming to raise approximately £100 million per year from AML regulated entities, to support the economic crime policy agenda. Barclays supports the proposed Levy, which we believe will provide a sustainable funding source for combatting economic crime into the future.

2020 has been a challenging year but there have been notable improvements in the economic crime landscape. The public and private sector have reviewed the Joint Money Laundering Intelligence Taskforce (JMLIT) to optimise the model for the future, and development of the fusion cell has been accelerated, bringing the aspiration of real-time information sharing closer. This progress, given constraints, demonstrates a real appetite across the public and private sectors to drive forward reform.

Barclays, alongside the other major UK banks, are committed to fighting economic crime. We work closely with law enforcement, regulators and Government partners in various public-private partnership initiatives to ensure that the UK remains a hostile environment for economic criminals. These partnerships, alongside other reforms such as SARs reform, and that of Companies House, provide the best opportunity to tackle financial crime in the UK.

Challenges and Policy Recommendations

SARs Reform

To ensure the UK remains a world-leader in the prevention of economic crime, Government should prioritise reform of the current Suspicious Activity Reporting (SARs) framework. An enhanced SARs tool, enabling better data analytics and the efficient flow of information between the regulated sector and the authorities, is critical to ensuring that SARs can be converted into meaningful law enforcement outcomes. As part of any reform efforts, policymakers should consider how appropriate sharing of broader information between the private and public sectors, and within the private sector itself, could support efforts to reduce economic crime. SARs reform has been an economic crime policy priority for a considerable period of time, and there is widespread belief that

an effective regime will provide the bedrock of a highly effective economic crime framework in the UK. It is therefore fundamental that Government priorities and delivers SAR reform at pace.

Reform Through Regulatory Guidance, Rather than Legislation

A key challenge in the fight against economic crime in the UK is the slower pace of reform. The relatively slow legislative approach taken in the UK can be compared to the regulatory guidance approach taken in the US. In the US, action has been driven through the Bank Secrecy Act Advisory Group (BSAAG) – a group comprised of representatives from federal regulatory law enforcement agencies and financial institutions - which created a specific AML working group in June 2019 to develop recommendations for strengthening the national AML regime by increasing its effectiveness and efficiency. The efforts of this group has already led to FinCEN publishing an Advance notice of proposed rulemaking (ANPRM). The ANPRM introduces a new proposed definition of AML program effectiveness, the concept of Strategic AML Priorities (Priorities), and a possible regulatory requirement for risk assessments. Thematically the ANPRM aligns closely with the ultimate aims of the Economic Crime Plan and wider Economic Crime reform programme in the UK.

The approach of reform through regulatory guidance as opposed to time-consuming legislation may be a model that could be leveraged to increase the pace of reform in the UK.

An Independent UK Sanctions Regime

As the UK moves towards its own independent sanctions regime in January, there will be a substantial administrative change in the sanctions lists used for screening. This is expected to drive a high volume of "re-alerts" for specific cases and there is a likelihood that a significant proportion of cases will have already been investigated and reviewed for sanctions risk. Nonetheless, significant resource will be required to re-work potential matches to ensure compliance with the new sanctions requirements. Government should work with the private sector to ensure the transition to an independent regime is as efficient as possible and avoids any duplication.

The Office for Professional Body Anti-Money Laundering Supervision (OPBAS)

The Office for Professional Body Anti-Money Laundering Supervision (OPBAS) has made a concerted effort over the past two years to level up the regulatory environment across all regulated sectors. Since the end of 2018, proactive supervision of Professional Body Supervisors (PBSs) has also increased from 10% to 81%[3]. This is a significant achievement and represents a substantial improvement in the capacity of OPBAS to deliver a hostile environment for economic crime in the UK.

OPBAS, and other anti-money laundering regulators, could aid efficiency and effectiveness through seeking opportunities to align data sets. In their due diligence processes, a bank may need to understand what a client does and by whom they are regulated. This can be a challenge due to the number of regulators in the UK. A shared database, with similar data fields, would make this process

[3] OPBAS and FCA published 'Anti- Money Laundering Supervision by the Legal and Accountancy Professional Body Supervisors: progress and themes from 2019',

easier for the private-sector and for customers trying to understand who they are engaging with. There are also opportunities for the data to be 'reverse searchable' so that the private sector can take the data and identify their exposure to a particular sector. This is of value where a client may have a small proportion of their business which is regulated, and have elected not to declare it e.g. if a company offers a number of services, one of which is trust and company formation. Given this is not a detail held in Companies house (e.g. BIC code) where it is not declared the financial institution would not be aware of this activity.

Companies House Reform

Companies House, much like OPBAS, is also undertaking significant change, specifically Corporate Transparency and Register Reform. We believe that the proposed reforms will be instrumental in ensuring a reduction in the mis-use of UK companies, and will have a significant impact in the fight against economic crime. Barclays believes Companies House reform should therefore be prioritised for legislative implementation. However, in the interim, it is vital that action is taken to reduce abuse of Companies House, under the current framework of rules. For example, there is scope for Companies House data to be mined to identify profiles of concern e.g. individuals holding disproportionate numbers of directorships, as well as opportunities to work with the private sector to determine how such insights can be developed to understand either the criminal activity behind them, or better understand how the service is being genuinely used.

Economic Crime Levy

An appropriately designed and effectively administered Levy could provide a sustainable funding source to reduce harm, protect the integrity of the UK economy and create a hostile environment for criminals. While we broadly agree with the principles set out in the Government's consultation, we believe there are certain elements that should be considered:

- **Scope** - All AML-regulated firms should be subject to the Levy to some degree, to ensure the entire sector is appropriately incentivised to take action.
- **Spending the Levy funds** – Initially, we believe that SARs reform should be a key priority, given its fundamental impact on the UK's capacity to tackle economic crime. Going forward, the Levy should be used to fund new strategic initiatives, rather than funding existing in-flight activity.
- **Calculating the Levy** - While we understand that a metric for calculating money laundering risk may be required, we would caution against a flat assessment of the number of SARs reported, as this could result in negative market behaviour that is not conducive to tackling economic crime. Further, in order to avoid overly penalising global firms, we believe that the Levy should be based upon UK generated revenue only.
- **Governance** - Potential projects to be funded by the Levy should be properly and transparently assessed to determine whether the costs of delivery are fair and proportionate to the expected impact on the UK economic crime system. To ensure the Levy is appropriately overseen and administered, clear roles and responsibilities should be assigned to a public-private governing body, with relevant, empowered representatives from all key sectors in scope of the levy.