Submission to the Treasury Committee's Inquiry into Economic Crime

Introduction

Barclays welcomes the opportunity to input into the Treasury Committee's inquiry into Economic Crime. Having contributed to UK Finance's submission, we are pleased to provide additional detail on a number of topics, in particular on the strand of the inquiry focussed on 'consumers and economic crime'.

As a transatlantic consumer and wholesale bank, we offer products and services across personal, corporate and investment banking, credit cards and wealth management. We are headquartered in London and New York, operate in over 40 countries and employ 85,000 people globally. However, despite our global reach, our longest consumer markets experience has been in the UK. Barclays has been part of the fabric of the UK for over 327 years, and our success as a business has always been inextricably linked to the progress of the people and the businesses we serve.

This deep connectivity across the UK enables us to have a developed understanding of the causes, enablers and context in which economic crime takes place. We recognise the burden and pain it often causes to victims, and the scourge of it continuing to grow in pace and scale. It is this understanding that has led us to conclude that only a comprehensive, ecosystem-wide approach to tackling economic crime will prevent the significant financial and non-financial detriment it causes consumers and businesses, and we stand ready to support these efforts, alongside parliamentary stakeholders, Government and the wider, related ecosystem.

We also recognise the distinctive role of policymakers in taking a long-term, strategic and holistic view of the steps required from all players in the broader ecosystem to stop economic crime. While there are a number of initiatives currently in train that are helping to tackle economic crime, we are clear that more can be done by all parties. To this end, we welcome the Treasury Committee's consideration of these important topics, and stand ready to provide further support to the Committee.

Emerging trends

The digital revolution is fundamentally changing the way in which businesses operate and consumers manage their lives. Almost all sectors are being impacted by digitisation, with financial services in particular being transformed.

This revolution has led consumers to want to conduct their financial matters quickly and easily, at the time and place of their choosing. They expect to be able to conduct their banking as seamlessly as they update their social status, and not be forced to conform to preselected engagement channels. At Barclays this is evidenced by our consumers undertaking over six million - and growing - digital banking interactions every day (including online and mobile), with the footfall within our branches falling rapidly every year.

This is just one part of a far broader digital revolution that is taking place across the UK economy, which provides many new opportunities for consumers, including the provision of even greater choice and control over their financial matters.

The power of data

As consumers increasingly engage digitally, they also generate a data profile with their providers that develops over time. The amount of data being generated is large, and firms are only just starting to try to better understand it, with advances in technology able to help.

When consumer data can be understood and leveraged appropriately, it has the potential to have significant economic value, both for consumers and firms. In turn, for firms, data can provide greater insights which can be used to create and deliver more tailored - and better value - products and services to their customers.

Privacy and protection of personal data

As increasing quantities of personal data become accessible, however, there is a concern that consumers' knowledge and understanding of how to protect themselves and their data does not keep pace with their appetite for digital access. If anything, because of the way in which digital platforms work (including the obligatory wholesale acceptance of terms and conditions), consumers have become ever more conditioned to automatically sharing their data with a wide range of parties.

Sadly, economic criminals continue to advance their sophistication in targeting consumers and we see the resultant increases in the volume and sophistication of scams. These techniques include social engineering, whereby, via phishing and smishing, (among other techniques) consumers are tricked into giving away their data. Additionally, large-scale data breaches are a primary route for consumers to be targeted and defrauded.

Tackling APP scams

This broad point is clearly evidenced through the ongoing debate regarding the most appropriate way to tackle Authorised Push Payment (APP) scams.

Overview

APP scams are when fraudsters deceive consumers or businesses to send them a payment under false pretences to a bank account controlled by a fraudster. The consumer or business authorises (or 'pushes') the payment, made using Faster Payments, and – being irrevocable - the victims cannot reverse it once they realise they have been victims to fraud. Real-time payments also lower the risk for fraudsters, because the money is received instantly, and therefore fraudsters can quickly extract their funds via this method.

In order to reduce the harm experienced by victims of APP scams, and to incentivise Payment Service Providers (PSPs) to better protect their consumers, a Contingent Reimbursement Model (CRM) is currently being developed. This represents a step forward in providing support and clarity to consumers regarding their rights and responsibilities in the event that they are a victim of an APP scam.

The need for an ecosystem-wide approach

However, when considering how to challenge the fundamental prevalence of APP scams, there are a number of critical issues that - as we explained in our response to the CRM Code Consultation and through our participation on the APP Scams Steering Group – are yet to be adequately addressed. The most important of these, and the one which we would suggest that the Treasury Committee give due consideration to, is the imperative for an ecosystem-wide approach to combating economic crime.

Whilst PSPs have a critical role in relation to APP scams, a far broader range of organisations unwittingly support the facilitation of fraud and scams. This facilitation can take place through the

technology firms who often host or enable the nefarious elements that undertake these criminal activities, along with organisations that allow their security to be breached, therefore placing consumers' data at risk of being used by criminals to enable either fraud or scams. As such, all organisations who unwittingly facilitate and enable economic crime should be suitably accountable for this, and held responsible for the robust tackling of economic crime going forward.

Extending regulation so that these actors ensure that their systems and services cannot be used by fraudsters should be a greater priority. We would urge Government, the PSR and the FCA to consider what further action needs to be taken to ensure that scams are prevented at source. Dealing only with the consequences will have limited effect and it will be very difficult to measure any success, including the effectiveness of the Code. Scams are criminal activity and, as with any other criminal activity, prevention ought to be the primary focus of any policy efforts.

Extension of the CRM Code

We also advocate an extension of the code to third-party Payment Initiation Service Providers (PISPs). Under Open Banking, PISPs will be able to make payments at consumers' requests directly from the accounts they hold, using Faster Payments. If not covered by the CRM, there is a risk that a gap in consumer protection is created, which will likely undermine the success of Open Banking in driving competition in the current account and payments markets. Not having these in scope could create a complex experience for the consumer, who would not have the same protection levels if they were to fall victim to a scam.

Finally, the Treasury Committee should consider whether current legislation is hampering the repatriation of funds and efforts to analyse criminal networks at an industry level. It may be of benefit for the Treasury Committee to consider reviewing the relevant legislation - noting that the Law Commission is currently reviewing the Proceeds of Crime Act (POCA).

Consumer awareness and education

Barclays recognises the critical importance of consumer awareness and education when it comes to Digital Safety, hence the £10m investment into Barclays Digital Safety Campaign, launched in 2017. The Campaign sought to raise awareness of the importance of digital safety amongst the UK public (amidst the rise of fraud and scams), and the many simple ways in which people can better protect themselves online.

We are pleased to have had over five million proactive engagements with our campaign by members of the public. This included visits to our digital safety hub (website), online video views, social media likes and retweets, and digital safety quiz completions.

Other key aspects of our campaign include:

- A multi-million-pound TV and outdoor advertising campaign to raise public awareness of fraud and scams across the UK public.
- A dedicated microsite – www.barclays.co.uk/security - where people can:
    - take a test to understand how digitally safe they are.
    - find information on digitally safe behaviour and how best to save data and share private information.
    - find information on financial frauds and scams.
    - see top tips on what to look out for, as well as what to do and not do.
- Media partnerships with *The Sunday Times*, *The Guardian* and Capital Radio which created content dedicated to helping their readers and listeners avoid financial crime.

- A wider PR programme of activity dedicated to creating coverage to raise public awareness of the risks that exist, the importance of digital safety and how they can protect themselves, their families and (if they are a small business owner) their businesses and consumers.
- Dedicated face-to-face sessions with members of the public around the UK (including working with a large number of MPs to provide digital safety sessions for their constituents).
- Dedicated cyber security clinics for small businesses.
- Partnerships with others to drive additional engagement and awareness, including Citizens' Advice and Age UK.

Alongside this effort, we have taken extra measures to inform, empower and protect our consumer-base with new tools to keep themselves and their families safe online. These have included free security software to protect their devices, and a link to 'Your Cards', where people can set controls on their debit cards to manage their use.

Innovating to find a balance

Despite the good progress that these initiatives have made, we believe that far more is required of all those in the economic crime ecosystem to halt the growth of economic crime more broadly. This includes the deployment of new technologies – such as Confirmation of Payee – and collective industry efforts to offer greater barriers and deterrents to criminals.

Safety delays and slowing inbound payments

Discussions regarding potential protections include the payment 'safety delays' which can help create forms of 'inflight' awareness and give the consumer time to think about the transaction to make sure it's genuine. However, any such changes would require careful thought and must be balanced against consumer expectations for almost instantaneous transaction speeds. It would also be best supported by updates to Payment Services Regulations 2017 and publication of industry guidance. We also note that such changes may conflict with other regulatory initiatives, for example under Open Banking – with a push for seamless and frictionless payments through third parties. It will therefore be important for policy makers to ensure a consistent and coherent approach is delivered.

Barclays have undertaken trials regarding 'stopping' inbound payments to allow verification of source of funds prior to funds being settled into the customer's account. This could provide a route to delay payments on a risk-based approach to reduce the ability of scammers access criminal. Work through UK Finance is also seeking to progress real time controls such as this across the industry. Information sharing in this space is key to ensuring that the analytics used to identify higher risk transactions remain effective across the industry to reduce the impact on genuine customers and transactions, and ensure the industry is best placed to prevent fraud losses.

The cost of data breaches

As organisations within all sectors collect an increasing amount of consumers' data – and as the value of that data increases – the increased likelihood of data breaches will potentially leave consumers' ever-more vulnerable to fraud.

While a data breach may be the result of insufficient cyber security and data protection procedures, it is often banks that must incur the costs of reimbursing consumers, whether it be in pre-emptive action such as the re-issuance of new cards, or in payment following the instance of a fraud or scam.

As such, we recommend that the liability framework for merchant data breaches is reviewed and updated to ensure that those who allow data losses bear the full costs of such losses, including the costs of third parties which can be accurately associated to their data loss. Otherwise, those who allow their perimeters to be breached will never have a robust incentive to protect data in the first place.

We would also suggest that consideration is given to whether more use can be made by the Government and regulators of the new powers they hold under the GDPR with respect to fining firms who allow themselves to suffer data breaches.

The policy approach to economic crime

Barclays understands the importance of driving for a comprehensive approach to tackling economic crime, in all of its forms. The current legislative and regulatory landscape provides some mechanisms to support this objective, and to help ensure that consumers are protected. For example, the formation of the National Economic Crime Centre (NECC) is welcomed, as is the expected collaboration between the public and private sector on its priorities.

Taking the profit out of crime and facilitating collaboration

Barclays believes that a primary focus of any policy effort should be preventing the crime from occurring in the first place. Taking the profit out of crime for criminals will, in turn, reduce attempts, undermine the source of funds for organised crime, and – therefore - weaken their wider negative impacts on the UK.

Whilst limited progress can be made through voluntary cooperation between the public and private sectors, Barclays believe that – to truly offer consumers and businesses real protections – Government and Regulators should create a policy framework that incentivises all those in the economic crime ecosystem to work together, incentivising firms in the economic crime ecosystem to invest in solutions that protect their consumers from fraud by stopping the fraud occurring in the first place.

Recommendations for Government

Government has a critical role to play in driving down the growing rates of fraud and economic crime. To support this work, Barclays – in collaboration with other industry player such as UK Finance, CIFAS and Trainline – have devised a range of public policy recommendations for Government consideration. We would welcome the opportunity to discuss these further with you and the Committee.

No.	Issue	Policy proposal	Detail
Improving the police response			
1.	National approach to combating fraud and scams	That the issue of fraud and scams is consistently handled across law enforcement, with an agile strategy, underpinned by advanced data analytics and technology, developed in order to protect consumers and businesses.	• Fraud and scams are on the rise, now making up half of all reported crime, with 49% of organisations globally saying they've been a victim of fraud and economic crime. • Acknowledgement must be given that a different skill-set and strategy must be deployed to

			tackle this crime, adapting to the fast-evolving modus operandi of these criminals. • The need to harness further insightful information as fraud cases are recorded in order to gain a greater understanding of this criminality and allow robust linkages between individual 'disparate' cases to be connected.
2.	Updated reporting structures and follow-up	A wholesale review of Action Fraud UK, alongside industry and law enforcement, based on desired outcomes vs. delivery to achieve these, with new reporting lines for fraud agreed and widely promoted.	• Given the importance of reducing the number of perpetrators of fraud – reporting and follow-up of reports is critical. However, despite the robust intentions of Action Fraud UK, it is unclear how and whether they have delivered on their objectives, delivering value for UK consumers and businesses in relation to fraud reporting. • Similarly, only 14% of local police forces actually follow-up on reported incidences of fraud, meaning that the vast majority of reported fraud cases are left unmanaged. • It is also not clear where individuals or businesses should report fraud to – their bank, the police or Action Fraud – perhaps as a result of the reporting structures and follow-up not currently working as they should. • The development of the CRM also presents a risk of reporting figures going down, as we have seen with card-not-present fraud, making promotion of the reporting guidelines even more important. • Reviewing the role of Action Fraud in the wider government strategy and agreeing new, clear reporting guidelines for individuals and businesses, is a critical next step. As is ensuring

			the police capability to follow-up on reported cases.
Strategy and accountability			
3.	Integrated approach driven by the NECC	An integrated approach between economic crime and fraud, led by the National Economic Crime Centre.	• It is imperative that the fight against economic crime is driven by the NECC in a co-ordinated fashion which includes fraud and money laundering. • Currently it is unclear whether the work of the Joint Fraud Taskforce and SARS reform, for example, sit alongside the NECC or within it. Our view is that it should sit within it. • This work should span both the public and private sector to not only reduce the scale and frequency of economic crime predicate offences (such as fraud and scams) but also the laundering of illicit funds which allows criminals to access the profits of their crimes as well as invest in future criminal activity e.g. drug supply or human trafficking. • The integrated approach should also consider the holistic laundering process, which includes the facilitation point, increasingly featuring social media platforms.
4.	Ecosystem-wide responsibility for fraud and scams	A polluter-pays principle is applied across the full spectrum of organisations that handle consumers' data, where irresponsible actions lead to an increased likelihood/ occurrence of fraud and scams.	• Solving this problem requires full participation from all those who feature in the "economic crime ecosystem", including the platforms and technology firms who often host or enable the nefarious elements that undertake these criminal activities • Liability should be attributed on the 'polluter pays' principle – whereby if companies (whether tech firms, telecommunications, or even utilities companies) do not take sufficient precautions to protect their consumers' data and have their data hacked or compromised, or permit users to undertake economic crime

			facilitated via their platforms - which leads to scams being perpetrated – they bear some of the financial responsibility for the consumer detriment that follows. • We need clear encouragement of industry to invest in cyber security protections, but, most importantly, enforcement (including material fines) in the instance that consumer data is compromised as a result of poor protections or practices. • All related industries should be encouraged or mandated to participate in efforts to combat economic crime, e.g. through participation in the Joint Fraud Taskforce.
Collaboration to tackle fraud			
5.	Clear and consistent communications to be agreed on fraud	That the Home Office convene industry stakeholders to agree clear and consistent messages on how to, and the importance of, protecting against fraud – for individuals and businesses to accommodate (sharing with colleagues and clients as appropriate), and for local police forces to better understand and accommodate in their own management of the issue.	• There is currently a lack of clear and consistent messaging on fraud – which can uniformly raise awareness amongst individuals, businesses and police forces responsible for tackling the issue, about the increased risk of fraud, and the best way for them to protect themselves from it. • While there are some notable campaigns in the marketplace (including Barclays' DigiSafe Campaign, UK Finance's Take Five Campaign, the Home Officer's Cyber Awareness Campaign, and some existing messages on the Action Fraud Website) it would be helpful to agree a core set of messages which can be accommodated by all parties as appropriate, whose objectives are to: - Increase awareness of the risk of fraud. - Increase accountability felt by individuals and businesses to protect against fraud. - Increase awareness about how to protect against fraud.

			- Clarify legal ramifications for committing or enabling fraud. - Clarify reporting process for individuals who fall victim to fraud.
6.	Data sharing to tackle fraud	The Home Office, technology and telecommunications firms to share relevant data with industry to promote knowledge-sharing and eco-system wide accountability for the tackling of fraud.	• Data sharing is an increasingly common method of collaboration between organisations and industries. Given the criticality of data to preventing and halting fraud, we recommend that data sharing is embraced by the Home Office, technology and telecommunications firms as a means of enabling Government and the broader public and private sector to work together to drive down fraud. • This data sharing links to both the data that the Home Office, technology and telecommunications firms could share, and that other industries can share with each other. E.g. Should firms that suffer a data breach be required to instantly inform other industries as soon as they know which consumers' details had been compromised.
7.	Convene industry to identify policy blockers	The Home Office, HM Treasury and the Police to jointly convene an industry round-table to identify policy and legal blockers and agree actions to remediate.	• There are existing legislative and non-legislative blockers which are preventing the effective identification and halting of fraudsters. In order to identify these, we recommend a convening of stakeholders from across the economic crime ecosystem to identify such blockers. • Participating organisations can provide help in unblocking such obstacles as is useful.

Conclusion

Barclays takes the issue of economic crime very seriously, and is doing all we can to protect consumers from the increasing scourge of economic crime as it relates to them. However, to truly

combat economic crime at its source, collective action is required from across the economic crime ecosystem, including Government, law enforcement, consumer groups and consumers.

We welcome the Treasury Committee's focus on this important issue, and are available to discuss any of these points further as is helpful.