EXECUTIVE SUMMARY

1. UK Finance represents nearly 300 of the leading firms providing finance, banking, markets and payments-related services in or from the UK. UK Finance has been created by combining most of the activities of the Asset Based Finance Association, the British Bankers' Association, the Council of Mortgage Lenders, Financial Fraud Action UK, Payments UK and the UK Cards Association. We and our members welcome the opportunity to respond to this call for evidence. The financial sector invests significant effort and resource into tackling economic crime, protecting customers, and working with law enforcement, going far beyond our regulatory or legal requirements. There is a shared desire to ensure the approach of UK PLC is as effective as it can be and work in partnership to detect and prevent economic crime.

2. In many areas, the UK approach is world leading. There is strong commitment from the top of Government, regulators, law enforcement and the industry to work together to tackle economic crime. This has helped develop strong public private partnerships that demonstrate how the system can work more effectively. A good example is the Joint Money Laundering Intelligence Taskforce (JMLIT). Established in 2016 the JMLIT brings together representatives from law enforcement, regulators and industry. It has resulted in the restraint of more than £7 million of suspected criminal funds, granted over 40 Proceeds of Crime Orders and identified more than 2000 suspect accounts previously unknown to law enforcement.

3. However, this should be just the start as despite good progress we must recognise that we are still some way short of where we want and need to be. Members invest over £5 billion in the UK per year on financial crime compliance and hundreds of millions more in protecting customers from fraud. There is significant resource and effort invested across both the private and public sector in tackling economic crime, but the overall outcomes are not as strong as they could be. The public and private sector resource could be used more effectively in partnership to protect the public and disrupt criminals.

4. To that end, we welcome the Home Secretary's set of announcements in December which builds on the close partnership work that has taken place so far. A more joined-up and targeted response to economic crime and stronger strategic oversight with the creation of the Economic Crime Strategy Board should better coordinate this agenda across Government, law enforcement and industry. Stronger public-private partnerships to prevent economic crime will deliver more effective outcomes. There are potential opportunities for better outcomes by the creation of the new Economic Crime Centre (NECC) and fundamental reform of the Suspicious Activity Reporting (SARs) Regime.

5. All parts of the legal and regulatory regime need to work effectively to help tackle economic crime. Presently, they do not, and the current system diverts too much resource towards low value compliance activity that does little to detect criminals or protect customers. The 'all crimes approach' of the SARs regime drives a manual low intelligence value reporting which ties up resource and has an opportunity cost for the public and private sector. The approach needs to be rebalanced so that effectiveness of activity and reporting is not assessed by reference to compliance measures alone but by the value provided to law enforcement in helping to detect and disrupt economic crime.

6. A more holistic intelligence-led approach which empowers our members to focus their resources in a way that better supports priorities on economic crime requires a fundamental look at how the system fits together and the roles and responsibilities within that. The last few years have seen an increase in the volume of initiatives, proposals and requirements, both policy and operational, without a commensurate increase in coordination and effectiveness. There are increasing compliance and reporting obligations which are not matched by an uplift in economic crime prevention. The breadth

of requirements has seen some financial services firms, particularly smaller institutions and new entrants, struggling to keep up with the pace of change and increasing administrative burden.

7. These demands are exacerbated by the absence of prioritisation on competing demands from the public sector on economic crime resource within the financial sector. Firms also note that whilst the financial sector has increased resource on economic crime, there has been a reduction in public sector resource in this area. We have also seen banks, as a highly regulated sector, being increasingly required to deliver functions to supplement that of the State. These include carrying out further checks on other regulated sectors (even where they are regulated by a Government body) or carrying out due diligence that exceeds that undertaken by Companies House.

8. There is a need for more thoughtful and effective implementation of legal obligations. For example, there is significant frustration across both the industry and law enforcement that the current Suspicious Activity Reporting (SARs) Regime drives inefficient reporting. For example, such as when firms are required to make a sanction breach report to the Treasury's OFSI who in turn send them to the National Crime Agency (NCA), but the industry is still also required to file a SAR with the NCA.

9. Ultimately, a more strategic approach needs to ensure that all parts of the system work more effectively together with clearer objectives and prioritisation. Improving information and intelligence sharing is critical as no one sector or institution has all the information they need to prevent and detect economic crime. Criminals exploit this to launder money and commit fraud. Only by sharing information can we identify links and wider criminality which allows us to jointly tackle it. Current laws hamper the ability of firms to share a) between banks; b) between our global affiliates; and c) cross-jurisdictionally.

10. That is why the most fundamental ask from the industry is for new legislation to enable financial services firms to more easily share information, below the threshold of reporting, with each other to better prevent and detect economic crime. This, underpinned by SARs Reform and a refocusing of industry resource towards supporting law enforcement priorities would transform the approach of the UK to economic crime.

11. A more effective approach would provide clearer legal and regulatory frameworks to address competing policy drivers, such as speed of payment versus protecting customers or areas where members currently carry legal risks to ensure public policy outcomes. Such as when banks return money to victims of fraud. In the absence of a court order, there is no easily identifiable legal vehicle that allows banks to do this. However, banks still choose to do it in the best interests of their customers. Given the growing need to work together to tackle fraud, it is wrong that members must carry legal risk for doing the right thing.

12. Ultimately, we believe that the Government's proposed holistic approach to economic crime is the right framework to identify and help resolve these issues and wish to play our part in delivering it. Work to effectively prevent economic crime needs strong public private partnerships underpinned by a robust legal and regulatory regime that supports this approach. Building on the December announcements there is now a need for Government to drive forward these reforms and invest the necessary focus and resource. We stand ready to support them in doing so.

UK Finance
Economic Crime Team

RESPONSE TO CALL FOR EVIDENCE

The scale of money laundering, terrorist financing and sanctions violations in the UK

Understanding the nature of the threat:

13. There is no unequivocal industry assessment on the scale of money laundering, terrorist financing and sanctions violations in the UK, but Government estimates the scale of scale of money laundering impacting the UK exceeds £90 billion a year[1] - the NCA believe this to be a significant underestimate[2]. The most recent NCA Threat Assessment also states that professional enables, particularly around supporting the purchase of property, and in establishing and supporting corporate vehicles are key to a wide range of economic crimes. This includes bribery and corruption where the NCA assesses that the UK is an attractive destination for corrupt PEPs to launder money.

14. The Home Office also estimates that fraud costs individuals in the UK around £6.8 billion a year[3], and the NCA assess that UK residents are more likely to be a victim of fraud than any other crime. We agree all the above findings are a reasonable assessment. We also recognise the HMG National Risk Assessment (NRA)[4] found that the threat of money laundering in the financial sector is high but that there are strong controls in place. At some point illicit funds will need to enter the legitimate financial system, and the number of financial transactions undertaken in the UK each year exceeds 16.8 billion.

15. However, whilst the industry supported HMG in developing this NRA and believe it is an improvement from the previous version, they believe it can be further improved to provide a more comprehensive picture in future. It does not examine available mitigations or their impact on preventing activity. Equally some assessments (such as money laundering in capital markets) have been made without sufficient detail or supporting analysis provided. The ambition should for the NRA to become a shared strategic assessment driving public and private sector activity and clearly states the threats and mitigations that resource should be focused on. The sector would welcome discussing how to achieve this.

The role of regulators in addressing this threat:

16. The FCA has been effective in driving prevention activity within banks - controls and systems are increasingly robust. However, as the NRA identifies, illicit money is now moving out of the banking sector into the non-bank financial system. A good example is Money Service Businesses (MSBs) which the NRA identifies as higher risk.

17. In addition, less stringent supervision by other regulators has seen banks increasingly expected to act as a de-facto regulator. So, one Government regulator (the FCA) can act against a bank who has an MSB as its customer even if the failings are within the MSB which is regulated by another Government regulator (HMRC). However, there is at the same time concern from Government and regulators where MSBs find it hard to access the financial system given the need to ensure financial inclusion and remittances for aid purposes. Members would like to see greater legal and regulatory clarity provided on the right balance as opposed to the sector being asked to manage competing policy demands.

18. Equally, banks must satisfy themselves that holders of pooled client accounts of other sectors present a low degree of risk for simplified due diligence to continue to be applied to these accounts. However, the UK has not yet put in place the necessary measures on supervision of those sectors that enables banks to easily reach this view.
19. As such, the financial sector is required to carry out disproportionate extra anti-money laundering (AML) and counter-terrorist financing (CTF) checks on other sectors, such as solicitors (which are already regulated for AML/CTF) or even Local Authorities (not regulated but inherently low risk for AML/CFT). This increases costs for both firms and their clients; and can, as below, raise questions over the profitability of serving these accounts and influence decisions on access to banking.

20. We urge regulators continuing to think more holistically about desired outcomes and how to rebalance the current system more effectively towards that. Effectiveness should not be set, or assessed, by

[1] https://homeofficemedia.blog.gov.uk/2017/12/11/economic-crime-factsheet/
[2] http://www.nationalcrimeagency.gov.uk/publications/807-national-strategic-assessment-of-serious-and-organised-crime-
[3] https://homeofficemedia.blog.gov.uk/2017/12/11/economic-crime-factsheet/
[4] HMG National risk assessment of money laundering and terrorist financing 2017

regulators by reference alone to compliance criteria; it should be determined by the value the controls, compliance and reporting provides to law enforcement in helping to detect and disrupt economic crime.

21. We also urge regulators to adopt a 'one-view' approach to redesigning the new payments architecture. The PSR are, rightly, overseeing the work of the New Payments System Operator (NSPO) but we recommend they ensure the Home Office and law enforcement are involved to identify opportunities to detect and prevent economic crime.

22. The industry also believes that there are steps that Government could take to improve transparency of ownership. This would free up resource across multiple institutions to be refocused on higher value intelligence-led work. In particular the Government should provide Companies House with sufficient resources and legal powers to (a) validate and verify the person of significant control (PSC) information being submitted including before incorporating a company, and (b) build a capability to identify and report suspicious activity. This would enable Companies House to take a more thorough approach to rooting out inaccurate submissions and assisting the Insolvency Service and law enforcement agencies in investigations into financial crime.

23. The UK Government should review the statutory duty of Companies House to ensure that it can provide at least the same standard of data validation as is required to be undertaken private sector company formation agents. This should be progressed as part of the Economic Crime Reform programme, to identify opportunities to integrate and enhance the overall UK regulatory framework.

The current legislative and regulatory landscape, including weaknesses

SARs Reform and Information Sharing:

24. The Suspicious Activity Reporting (SARs) Regime requires the regulated sector to submit SARs when they know or suspect they are dealing with the proceeds of crime. This is a potentially valuable source of information and intelligence. However, there is widespread recognition, including by Government, that the SARs Regime is not working well.

25. We estimate that our members spend £5 billion per year on financial crime compliance generating 20 million financial crime alerts which all need investigating. More than 630.000 SARs were submitted to the NCA from October 2015 to March 2017 and more than 90% of these reports were made by banks and financial institutions. We estimate that the sector is currently submitting around 460,000 SARs per year. However, many are the result of an inflexible reporting regime; even if SARS are of little use to law enforcement, or reported elsewhere, they must be submitted to comply with strict legal and regulatory requirements.

26. This results in significant public and private sector resource invested for relatively poor outcomes in terms of detection and disruption of economic crime. It increases costs and stops resource being focused in partnership on higher value, intelligence-led, activity.

27. Whilst individual SARs can be extremely valuable to law enforcement, their value is often greatest as a source of combined intelligence. There is a need for a fundamental rebalancing of the regime with a better shared understanding of threat and priorities. Equally Government should examine how more of the data required by law enforcement/regulators could be collected automatically through measures such as transaction reporting or the new payments architecture. This would free up resource for higher value intelligence activity.

28. Our members believe the development of the right legal provisions and gateways should be afforded the highest priority. The key industry ask is to allow information below the reporting threshold to (subject to the appropriate safeguards) be more easily and widely shared within the financial sector for the prevention and detection of economic crime. The view, shared by law enforcement, is that this would be transformative.

29. The new powers in the Criminal Finances Act ("CFA") which allow information to be shared when the threshold of suspicion is reached fell short of both industry and regulatory expectations. By setting the threshold for information sharing as "suspicion" firms can only share information in circumstances where they would need to submit a SAR to the NCA anyway. Consequently, any information sharing

under the powers in the CFA is only supplementing what the NCA know, which can already be achieved through the framework of JMLIT which was established in 2016 as a partnership between law enforcement, Government and the financial sector to combat high end money laundering.

30. We acknowledge the challenges of balancing information sharing with data protection. The timescales of the CFA hampered efforts to work through these, but we have now offered Government a legislative proposal on information sharing that we wish to explore as part of the SARs Reform Programme. This has also been provided to the Law Commission. We have also suggested to Government and the Law Commission a legislative proposal that allows statutory guidance to provide a reasonable defence for not reporting certain types of SARs agreed by law enforcement as low intelligence value. This would free-up public and private sector resource to be refocused into higher value intelligence.

31. Alongside legislative reform, there is a need for an improved operational response and JMLIT shows what is possible. Since 2016 JMLIT has advanced information and intelligence sharing and is the only forum in which there is a mechanism for prioritising and targeting SARs reporting. However, it is relatively small scale, and not all sectors are involved. For JMLIT to build on the good progress already made we believe there is a need to (a) expand JMLIT to other sectors; and (b) delivering an information sharing capability for the benefit of non-members. This would help better share intelligence across the public and private sector on threats and how to mitigate them.

32. A significant upgrade of law enforcement IT and analytical capability and capacity is also needed. Given the scale of the threat, simply replacing the current SARs IT is not sufficient. The NCA needs to have the infrastructure to deliver a transformative approach to financial intelligence on economic crime, including the infrastructure and resourcing to handle and conduct 'big data' analytics. That requires Government, as well as the private sector, to ensure it is investing sufficiently in the capability and capacity required.

Balancing the risk-based approach and access to financial services:

33. As the Committee previously recognised in the 2015 report into the 'Treatment of Financial Services Consumers' there are different views across the public sector over the right balance between keeping risk out of the financial system and identifying and managing risk. This creates a tension between access to banking and exiting relationships.

34. Many issues around exiting accounts or a reluctance to take on higher risk accounts arise where risks cannot be sufficiently mitigated, or not in a way that means the account remains profitable for the bank to operate. If other supervisory bodies are not recognised as consistently effective, the cost of failure by a bank can be too high. A cost versus benefit analysis can thus drive decision making towards reducing risk exposure.

35. To address this, as above, Government should strengthen the consistency of regulation cross other sectors to improve effectiveness. The creation of the Office for Professional Body Anti-Money Laundering Supervision (OPBAS) is welcomed, however, our members would like to feel more confident that HMRC (outside the remit of OPBAS) will also continue to improve standards among those it regulates.

36. There are also legitimate questions whether the Senior Managers Regime, and the criminal liability under the Proceeds of Crime Act have unintended consequences in terms of driving an overly cautious stance by the sector. We welcome the engagement of the FCA and the Law Commission on these questions.

<u>The effectiveness of the Treasury and its associated bodies</u>

37. The industry welcomes the joint leadership role of Treasury in the proposed economic crime reforms as they play a vital role in helping deliver reform. The sector also endorses the proactive approach of the FCA on JMLIT, SARs Reform and in establishing a new forum to allow industry to test new approaches to financial crime compliance.

38. Nevertheless, as above, the current regulatory framework and regulator expectations mean there is significant resource invested in reporting low risk activity or managing tensions between different

regulatory requirements. The sector would urge regulators to provide greater clarity on helping firms manage policy conflicts, and further guidance on what is acceptable for firms in terms of risk management.

39. We would also support regulators providing more clarity and good faith protections on areas that help firms identify and manage risk, helping to better protect customers. An example is the Payment Accounts Directive (PAD) which can facilitate criminals gaining access to the financial system, or Payment Services Directive (PSD II) which can make it harder to intervene on payments.

40. Whilst PAD and PSD II encourage openness and speed, which for most customers is welcome, there is concern that the way these provisions have been implemented fetters the ability to prevent people opening potential money mule accounts or to slow down potential illicit payments unless banks are prepared to carry the full risk. We would welcome wider discussion on how different elements of the financial system work to achieve the right balance between openness and control.

41. An example, where regulatory steers will be particularly important, is the Data Protection Bill (DPB) coming into force. There are concerns that the delay of guidance for implementing the DPB and the implications of this for managing financial crime risk – such as whether firms will still be permitted to screen against lists of Politically Exposed Persons. The EU Data Protection Regulation (GDPR) also presents members with uncertainty as to data sharing; we would welcome secondary legislation, or at the least, regulatory guidance, addressing legal uncertainties by defining when it is in the public interest to share data within the EU and overseas for the disruption of economic crime and the upholding of sanctions regimes.

42. However, whilst we would support work to revolve these tensions, it would be better to avoid them in the first place. We would welcome Government considering, perhaps as part of the impact assessment process, how to better ensure that tensions and conflicts between new regulations and financial crime risks are identified and considered before they are implemented.

The UK's role in international efforts

64. Banks can often hold an entire picture of cross-jurisdictionally criminality but be legally fettered from reporting this holistic overview to law enforcement. Instead firms make multiple reports on separate parts of the picture to Financial Intelligence Units in different countries for them to piece together. We would welcome a more balanced debate at global level about the impacts of this and the right balance between data privacy and financial crime objectives. Given the importance of international data sharing to enable firms and law enforcement to tackle economic crime we believe the should UK take a stronger leadership role to promote information and intelligence sharing internationally. In particular the UK should play a strong leadership role at the Financial Action Taskforce (FATF) to promote and drive international standards around data sharing.

65. On sanctions, UK Finance members operate within an international sanctions landscape which has seen rapid change in a short period of time. As a primary tool for responding to a range of foreign policy threats, the growth and use of sanctions has evolved dramatically over recent years. In turn the financial sector has to carefully monitor the risk, including the political and diplomatic context, across a significant number of jurisdictions.

66. This is not easy. The escalating transatlantic divergence in sanctions policy (such as, the US Russia sanctions applied as part of the Countering America's Adversaries Through Sanctions Act (CAATSA) and the recent US withdrawal from the Joint Comprehensive Plan of Action) have resulted in global financial institutions having to ascertain how best to comply with progressively divergent legal and regulatory sanctions obligations. In response to such divergent requirements, global banks have increasingly committed to complying with the sanctions laws and regulations of the United Nations, European Union and US, plus jurisdictions in which they operate. In this regard, banks set global sanctions policies that define minimum standards for compliance across the group.

67. Given that these banks comply with all applicable sanctions, it may go against the bank's global policy to undertake business that would not be permitted in other jurisdictions i.e. the US. Consequently, each bank's approach to the sanctions and franchise risk will be influenced by a range of factors. For this

reason, the appetite for each bank to engage in certain activities or within jurisdictions subject to some level of non-UK sanctions will vary. In particular, the US experience, where the 'de jure' reach of US sanctions is extremely broad, has in practice had the impact of US sanctions often extending well beyond the legal grasp of US authorities. Consequently, with the interdependence of international financial markets and international spread of large companies, US sanctions have a significant chilling effect even on non-US subjects.

68. The complexity in operating across different licencing authorities means that banks and their clients are currently required to navigate a combination of complex multi-jurisdictional regulatory guidance and an inconsistent licencing regime which has led to a significant impact on the funding of legitimate activity. A notable example relates to the operation of humanitarian projects seeking to send funds and goods into certain conflict zones and other high-risk countries subject to sanctions. In addition, broader financial crime risks arise from the FATF citation of non-profit organisations as targets of terrorist financing. This has led to non-profit organisations becoming increasingly identified as higher risk clients, subject to enhanced due diligence and in some cases, exit.

69. The Sanctions and Anti-Money Laundering Bill appears to offer the ability for the UK to consider greater use of general licences or broader project-based licences for at least transactional related activities (e.g. humanitarian relief activity in otherwise sanctioned territories, or via interaction with otherwise sanctioned governments). It is important that general licences or broader project-based licences permit activity by both UK and non-UK persons (and then permit UK institutions to perform activities ordinarily incidental to the permitted/licenced activity, such as processing a payment for the licenced activity).

70. It is increasingly more challenging to distinguish between relationships or activities which are unequivocally prohibited, from those which are permitted. Ownership and control factors, the introductory of sectoral sanctions, plus expectations on banks to ascertain 'indirect' sanctions risk exposure (i.e. through correspondent banking network relationships) have resulted in more intense risk management responses. To manage this complexity, the sector is seeking the provision of more detailed guidance that sets out a the intended scope of sanctions obligations. UK Finance has worked closely with the UK Government, the EU, the UN and US authorities on how implementation could be improved and made more effective, including addressing important variations across UK, EU and international levels, on how governments view requirements on sanctions obligations.

The scale and nature of economic crime faced by consumers

71. Firms spend millions of pounds in advanced fraud protection systems which help prevent 67 per cent of attempted fraud. However, we acknowledge there is a growing threat from cyber-enabled fraud as criminals operating overseas can target UK customers without stepping foot in the country. Equally within the UK there is a perception that criminals increasingly see fraud as high reward and low risk given the low rates of prosecution for fraud-related offences.

72. The sector has worked closely with Government and law enforcement to ensure there is transparent reporting on the nature and scale of the fraud risk. We have agreed with Government and law enforcement what should be reported, and the UK Finance financial fraud loss figures are included in the ONS's official crime statistics. Our members also report as agreed, all relevant information on fraud via UK Finance to the police's National Fraud Intelligence Bureau. These data reports are included in the recorded crime statistics.

73. UK Finance on behalf of the industry publishes full industry fraud losses twice a year. The latest figures[5] show:
    - Banks and card companies prevented £1,458.6 million of fraud in 2017 – equivalent to £2 in every £3 of attempted fraud being stopped.

    - There were 1,910,490 cases of unauthorised financial fraud, a rise of 3 per cent compared to the year before. However, unauthorised financial fraud loses fell by 5 per cent year-on-year to £731.8 million in 2017. The clear majority of victims, unless they were negligent, such as sharing log in details, will be refunded.

[5] https://www.ukfinance.org.uk/wp-content/uploads/2017/06/UKFinance_2017-annual-fraud-update-FINAL.pdf

- There were 43,875 cases of authorised push payment scams, and a total of £236.0 million was lost through authorised push payment scams in 2017. Financial providers were able to return £60.8 million (26 per cent) of scam losses in 2017.

- This is the first full year that authorised push payment figures have been collected, so a year on year comparison is not possible. However, unauthorised financial fraud loses fell by 5 per cent year-on-year to £731.8 million in 2017.

74. We are working with Government, law enforcement and regulators to identify and address vulnerabilities and share good practice and intelligence to help reduce fraud.

Response of the Treasury and its associated bodies to economic crime consumers face

75. Whilst HM Treasury have an important role to play, the Home Office lead fraud policy work, and chair the Joint Fraud Taskforce (JFT). The JFT is currently being reviewed to make it operate more effectively. Whilst plenty of initiatives and commitments there is need for a refreshed more strategic approach which we would hope the JFT review can deliver.

76. Too often the focus is simply on what banks can do, and there is a need to look at how other sectors or Government can help better prevent fraud. There is a misconception that banks alone can spot and prevent fraud. This ignores any analysis of the drivers of fraud, how vulnerabilities in other sectors can facilitate fraud, or the legal and regulatory restrictions that fetter banks acting.

77. Financial Services firms do not want customers suffering loss and are keen to play their part in reducing fraud. However, other sectors (as recognised in the NCA Threat Assessment) such as retailers, telecoms and Internet Service Providers (ISPS) providers all have a part to play, and all sectors should have a focus on security of data. There is also a need for the right regulatory and legal framework to reduce fraud including:

    - as above, the legal framework to share information more easily. This would help prevent fraud and more effectively trace stolen funds. This could also potentially allow companies in other sectors who have suffered a data breach to share details of their customers with all banks, not just the institution the customer banks with to help prevent identity theft.

    - the ability to slow down more payments where there is concern and be protected when doing so in good faith. The current legislative requirement is for payments to be made within one working day, and the regulatory expectations is within 2 hours. Given there are over 16.8 billion transactions per year, it is not possible to easily spot possible fraud without being able to calibrate payments accordingly.

    - good faith protections for blocking or freezing payments. There are examples where banks believe they have identified fraud and submitted a Consent SAR, but consent has not been refused, thereby leaving the risk of processing or rejecting the payment solely with the bank. As regulations and case law require the payment to be made this places the institution in a difficult position.

    - the legislative and regulatory clarity for banks to return monies to victims and be protected when doing so. As set out above, banks are choosing to return monies to victims even in the absence of a court order because of the good public outcomes of such an approach. Equally the Proceeds of Crime Act (POCA) does not allow victims to easily be refunded as the victim has to go to court. That should change.

Consumer education, responsibility and vulnerability in relation to economic crime

78. Helping customers to protect themselves is essential which is why the industry funds and runs the national Take Five campaign in conjunction with the Home Office and other Joint Fraud Taskforce (JFT) partners. It helps to prevent customers being scammed by raising awareness of how to stay safe. Phase 2 of Take Five was launched in September 2017 with a budget of just over £3m (with members contributing £2.5m and the Home Office £500k). We have carried out a detailed evaluation of the impact of the campaign which showed, as at Annex A, the campaign achieved impressive reach

and recall.

79. We are also now developing Phase 3 which aims to mainstream Take Five through the industry developing and adopting a voluntary code for how participants will implement Take Five as part of everyday communications. We are still working on this with the Home Office and can provide further detail in future if that would be helpful.

80. The industry has also developed and rolled out the Banking Protocol – a ground-breaking rapid response scheme through which branch staff can alert police and Trading Standards to suspected frauds taking place - to every police force area in the UK. In 2017, while it was still being introduced across the country, the Protocol prevented £13.3 million of fraud and led to 129 arrests. We are currently considering with law enforcement how this can be extended to other forms of banking such as telephone banking.

Effectiveness of financial institutions in combatting economic crime consumers face

81. Members invest hundreds of millions of pounds per year to prevent fraud and stop 67% of attempted fraud. They use sophisticated monitoring technology such as biometric profiling and procedures to verify the customer and the devices. For example, flagging fraudulent IP addresses or using geolocation services to check for locations unusual to the customer. Card based transactions are also protected by authorisation processes that use highly sophisticated transaction risk scoring methods and are evolving to utilise the latest artificial intelligence ad machine learning technology. The customer will not always be aware of this technology as it is often used in the background of using online services.

82. In addition to spending on fraud prevention, and communication campaigns, the industry also funds a specialist police unit, the Dedicated Card and Payment Crime Unit, which targets those responsible for remote purchase fraud. This delivered a combined value in savings and disruptions in criminal activity of close to £30 million in 2017.

83. We are also supporting the Payment Systems Regulator (PSR) on its complex work on APP fraud, providing the secretariat for its new steering group on a contingent reimbursement model and taking forward other measures identified by the Payments Strategy Forum to tackle financial crime. Alongside the independent Chair, consumer groups and the broader payments industry, we continue to support the development of the PSR's proposals for a new industry code to clarify the circumstances when banks and others payment service providers would be responsible for reimbursing APP fraud victims who have acted appropriately.

84. However, more needs to be done. That is why members want the power to share more data to better detect and prevent economic crime, including fraud. We also recognise the need to improve how industry supports victims, so have created new Best Practice Standards (BPS) setting out how fraud cases are to be managed in the future to ensure those who have fallen victim to fraud or scams get the help they need. This includes around-the-clock availability of fraud specialists, to make it easier and better for the customer, and improving the likelihood of their funds being recovered. These have already been introduced by many of our members and there are plans to progressive roll these out across our membership and wider payments industry.

85. Ultimately the system needs to be better at stopping fraud. The financial system is designed and regulated to be swift, open and certain which is good for legitimate customers but can fetter the ability of banks to spot fraud before it happens, particularly where the victim is authorising the transaction. Unusual activity is not always suspicious activity and many of the 20 million financial crime alerts per year will be by necessity identified post transaction given the volume of payments and the regulatory expectation of swift payments. As above, we want to work with Government and regulators to examine how the new payments architecture can help prevent fraud.

Potential for technology and innovation in committing and combatting economic crime

86. As the NCA notes[6], criminals overseas are increasingly targeting the UK, and the NCA also notes how technology, particularly where it is exploiting vulnerability in other sectors such as spoofing telephone

[6] http://www.nationalcrimeagency.gov.uk/publications/807-national-strategic-assessment-of-serious-and-organised-crime

numbers or e-mail addresses is an enabler of fraud. Equally data breaches are a key enabler as fraudsters benefit from the exploitation of basic security and human vulnerabilities through social engineering. As the system is currently designed for openness and speed these threats will grow if they are not mitigated.

87. Technology, supported by the right legal and regulatory framework is one part of that mitigation. Whilst currently 67% of attempted fraud is prevented, there is no imminent sole technological solution that would go further and have the equivalent impact on unauthorised fraud as chip and PIN. This is in part because currently the legal and regulatory framework does not fully allow the use of machine learning or artificial intelligence, underpinned by the right flows of information and the ability to disrupt payments to be in place. As above, we believe this should change

88. There are some positives. On APP scams, we believe the introduction of Confirmed Payee by the New Payments Systems Operator (NSPO) could significantly reduce fraud. It will allow customers to see if account details match and enable them to better protect themselves. We also see potential for technology to trace stolen money through the system and recover stolen funds from criminals. The financial sector is taking forward a pilot with Voccalink to swiftly identify and follow stolen money through the financial system. However, barriers to information sharing and recovering money currently limit this work.

89. We believe there should be a shared ambition to make the UK a world leader in protecting customers and driving out dirty money. Technology is key to this, but technology is only as effective as the enabling legal and regulatory framework in which it operates. It will require a lot of support from Government to resolve these issues. However, removing the incentive from economic crime by taking the money from criminals is the most effective way to deter criminals and make the UK a safer place.

The security of consumers' data

90. Members take data security incredibly seriously and believe that one of the most effective ways to protect customers from economic crime is to improve the security and handling of personal data. However, data breaches in other sectors can lead to information being used to target individuals for fraud. We welcome the stronger standards that the DPB will introduce. We have also suggested that fines issued from the ICO over data breaches may be a source of revenue that could be used to reimburse victims of APP scams.

Next Steps

91. We welcome continuing work on all these issues and this important agenda with Government, law enforcement and regulators. We stand ready to provide further evidence to the Committee if this would be helpful.