House of Commons

Treasury Committee

Economic Crime: Consumer View: Government and Regulators' Responses to Committee's Third Report of Session 2019

Second Special Report of Session 2019–21

Ordered by the House of Commons to be printed 10 March 2019

HC 91
Published on 13 March 2019
by authority of the House of Commons

The Treasury Committee

The Treasury Committee is appointed by the House of Commons to examine the expenditure, administration, and policy of HM Treasury, HM Revenue and Customs and associated public bodies.

Current Membership

Mel Stride MP (Chair) *(Conservative, Central Devon)*

Rushanara Ali MP *(Labour, Bethnal Green and Bow)*

Mr Steve Baker MP *(Conservative, Wycombe)*

Harriett Baldwin MP *(Conservative, West Worcestershire)*

Anthony Browne MP *(Conservative, South Cambridgeshire)*

Felicity Buchan MP *(Conservative, Kensington)*

Ms Angela Eagle MP *(Labour, Wallasey)*

Liz Kendall MP *(Labour, Leicester West)*

Julie Marson MP *(Conservative, Hertford and Stortford)*

Alison McGovern MP *(Labour, Wirral South)*

Alison Thewliss MP *(Scottish National Party, Glasgow Central)*

Powers

The committee is one of the departmental select committees, the powers of which are set out in House of Commons Standing Orders, principally in SO No. 152. These are available on the internet via www.parliament.uk.

Publication

Committee reports are published on the Committee's website at www.parliament.uk/treascom and in print by Order of the House.

Evidence relating to this report is published on the inquiry publications page of the Committee's website.

Committee staff

The current staff of the Committee are Emily Buckland (on secondment from the Bank of England), John-Paul Flaherty (Second Clerk), Sarah Goodwin (on secondment from the Prudential Regulation Authority), Rachel Kift (on secondment from the National Audit Office), Dan Lee (Senior Economist), Gosia McBride (Clerk), Aruni Muthumala (Senior Economist), Matt Panteli (Senior Media and Policy Officer), Yasmin Raza (on secondment from the Financial Conduct Authority), Baris Tufekci (Committee Support Assistant), Adam Wales (Chief Policy Adviser), Maciej Wenerski (Senior Committee Assistant), Marcus Wilton (Senior Economist), and Tony Verran (on secondment from HM Revenue & Customs).

Contacts

All correspondence should be addressed to the Clerk of the Treasury Committee, House of Commons, London SW1A 0AA. The telephone number for general enquiries is 020 7219 5769; the Committee's email address is treascom@parliament.uk.

You can follow the Committee on Twitter using @commonstreasury.

Second Special Report

On 1 November 2019, the Treasury Committee published its Third Report of Session 2019, *Economic Crime: Consumer View* (HC 246). On 5 February 2020 we received the Government Response to the Report, on 31 January we received the Payment Systems Regulator Response to the Report, and on 12 February we received the Financial Conduct Authority's Response to the Report, all of which are appended below.

Appendix 1: Government response

Introduction

The government has considered the Treasury Select Committee's comprehensive report titled 'Economic Crime: Consumer View' published on 1 November 2019 and has carefully considered the Committee's recommendations, which highlight important issues on economic crime and consumers.

The UK's standing as a global financial centre, its openness to overseas investment and its embrace of new and innovative technologies create a vulnerability to economic crime. Economic crimes like fraud, corruption and money laundering enable and fund other crimes which cause lasting harm—such as child sexual exploitation, drug dealing, human trafficking and modern slavery. Our communities are left damaged, and often our most vulnerable citizens are harmed.

It is therefore imperative the UK is world-leading when it comes to responding to economic crime. In 2018, the Financial Action Task Force found that the UK had one of the strongest systems for combatting money laundering and terrorist financing of over 60 countries it has assessed to date. Criminals, however, are continuously adapting their methods and we know there is more work to be done. Last year, the government and private sector jointly published a landmark Economic Crime Plan, which encompasses our response to the recommendations made by both FATF and the first part of the Treasury Select Committee inquiry. This Plan provides a collective articulation of actions being taken by both the public and private sectors over the next three years to ensure the UK cannot be abused for economic crime. The public-private partnership approach ensures a joined-up response to economic crime and maximises the capabilities, resources, and experiences of both the public and private sectors.

The government has also transposed the 5th Anti-Money Laundering Directive into UK law, which came into force on the 10th January this year. This includes bringing letting agencies and art dealers into regulation for the first time, as well as implementing a comprehensive and world-leading approach to regulating cryptoasset exchanges and custodian wallet providers.

As a commitment of the Economic Crime Plan, the government will also publish an updated National Risk Assessment of Money-Laundering and Terrorist Financing by July 2020. This will serve as a stocktake of our understanding of these risks, including how they have changed since the 2017 NRA. The assessment is the result of an extensive consultation across government, including law enforcement, intelligence agencies, supervisors as well as the public and private sector.

Government response to the Committee's recommendations

This paper sets out the government's response to each of the Committee's conclusions and recommendations to government. The Committee's recommendations are in bold and the government's response is in plain text. Paragraph numbers refer to those in the report. Where a recommendation is for the FCA, this has been referenced.

1. The type and scale of economic crime affecting consumers

It is clear, both in terms of financial losses and in the variety of scams suffered by consumers, that economic crime is a serious and growing problem in the UK. Trends need to be identified quickly. In order to ensure a clear picture of the scale and types of economic crime facing consumers, the FCA should publish data on economic crime within six months. It should evolve its data collection practices to ensure they allow for emerging trends, while still enabling year-on-year comparisons. (Paragraph 15)

The FCA will address this recommendation in their response.

2. Prevention

Data sharing

The government has not been listening to concerns that data sharing requirements for financial services firms are too restrictive and unfit for purpose. We welcome the establishment of the public-private working group. Its remit must include assessing whether the current data sharing requirements are fit for purpose. If not, the working group must make detailed proposals to reform those legal requirements including considering using existing subordinate legislation-making powers under the Data Protection Act 2018 to amplify or clarify exemptions in the Act. The group should report to us every six months on progress made. (Paragraph 24)

In recognition of the importance of data-sharing in combatting economic crime, improving information-sharing is one of the key strategic priorities in the Economic Crime Plan. The UK has been a world-leader in promoting the legitimate information-sharing on economic crime and its architecture includes the Joint Money Laundering Intelligence Taskforce (JMLIT), the provisions of the Criminal Finances Act 2017, the Data Protection Act 2018, and the Suspicious Activity Reporting (SARs) regime which is currently subject to an ambitious reform programme. Effective, legitimate and targeted sharing and use of information can only be achieved with the appropriate powers, gateways, frameworks and culture in place.

A public-private steering group has been established to oversee mapping work that examines whether the existing information sharing gateways, powers and partnerships are appropriate, clearly defined and universally interpreted. This mapping work is also identifying what barriers exist to information sharing and examining whether these barriers are legal, arising from regulatory expectations, technical, financial and/or cultural.

The steering group is further considering the case for any new provisions on information-sharing between private sector institutions. This must consider whether a new provision would be necessary and effective in delivering the objectives of information-sharing:

to better prevent crime, protect potential victims, detect crime quickly, conduct investigations promptly and prosecute in a timely manner. The review must also take account of data subjects' rights, considering data protection legislation and the Information Commissioner's Office's (ICO) data-sharing code of practice. Other ethical implications and competition risks will also be considered in making the steering group's eventual recommendations.

The steering group is also overseeing the implementation of the commitment in the Economic Crime Plan to promote sharing of information in corporate groups. This will culminate in a statement setting out the government's expectations on information-sharing within corporate groups, including between different business units, for economic crime purposes. This will help ensure that firms' determination of risk encompasses global considerations and be used as a basis to promote greater international consistency in cross-border information-sharing.

The review is scheduled to result in a report shortly that sets out recommendations for reform. The government will share a copy of that report with the Committee and, if the review does propose any legislative changes, will update the Committee every six months on the progress made in delivering them.

Response Time

We are concerned over the length of time some accounts used in economic crime remain active once intelligence has been received on their potential misuse. Whilst we understand that prescribed timeframes could delay how quickly banks act, the difference in time each bank takes to act creates weakness in the UK financial system. The FCA should work with financial institutions to ensure consistency across the sector. We recommend that the FCA uses its powers to set a timeframe in which an account must be frozen when evidence has been received by a bank that it is receiving money fraudulently. (Paragraph 28)

The FCA will address this recommendation in their response.

Confirmation of Payee

Confirmation of payee will not solve economic crime alone, and as such the onus will always be on financial firms to develop further methods and technologies to keep up with fraudsters. (Paragraph 39)

The fact that banks were not previously confirming payees is a serious failure to protect customers from harm. Asking for such information but not using it would have created a false sense of security among some customers when sending payments. It might have been better for banks to not ask for this information at all if they were not going to use it for fraud prevention. (Paragraph 40)

We therefore recommend that Confirmation of Payee should be introduced as a matter of urgency. Every delay leaves more people vulnerable to falling victim to economic crime. If the implementation date of March 2020 begins to look in doubt, regulators should consider introducing sanctions, such as fines, to firms who have not met the deadline. (Paragraph 41)

The government agrees with the Committee that introducing Confirmation of Payee represents a positive step towards combatting crime.

As the Committee's report notes, in August 2019 the Payment Systems Regulator (PSR) gave a direction to the UK's six largest banking groups to fully implement Confirmation of Payee (CoP) by 31 March 2020. This direction applies to Payment Service Providers (PSPs) who collectively accounted for 90% of the total volume of transactions over FPS and CHAPS in 2018 and, as the PSR has noted, should therefore have a significant impact in countering APP fraud.

Should it prove necessary, under the Financial Services (Banking Reform) Act 2013, the PSR has powers at its disposal, including warning notices and financial penalties, for use in the event that a directed participant fails to comply with a direction.

The arguments put forward that Confirmation of Payee implementation could be harmful for competition if large firms implemented before small ones, is without merit. Competition in the banking sector exists for the benefit of customers, not for the benefit of firms. Customers should not be put at risk of becoming victims of fraud, in order to protect slow adopting firms from implementing protections for their customers. The Payment Systems Regulator should therefore ensure that all relevant firms can implement Confirmation of Payee by the end of 2020. (Paragraph 42)

The government welcomes the implementation of Confirmation of Payee as a means of combatting Authorised Push Payment (APP) scams and the August 2019 PSR direction mandating full implementation by many of the largest firms by the end of March 2020.

With the first phase of CoP implementation underway, Pay.UK has announced that it is considering further applications for CoP, including the potential of the proposition for bulk payments, PSPs using Head Office Collection Accounts (HOCA) or other corporate applications. Indicative timelines for agreeing a model and implementation period for this second phase are currently under review.

The PSR will work with industry to determine a proportionate approach and timeframe for further CoP implementation.

Subtle differences which might not be immediately obvious to many people, such as using 'soliciters' rather than 'solicitors', could represent a fruitful way for fraudsters to disguise fraudulent accounts as legitimate accounts, and therefore small inaccuracies should be flagged for consumers' own protection. We recommend that spelling mistakes are flagged within the new Confirmation of Payee System. (Paragraph 43)

The government recognises that flagging spelling inconsistencies as part of the new CoP system could in some instances prevent APP scams.

The CoP rules contain minimum standards with regard to spelling-checks. As CoP is introduced, banks are coordinating together to ensure that the flagging of inconsistencies is implemented consistently.

Delaying payments

Fraudsters rely on the speed of the payment system to move money into a series of different accounts before a customer or a customer's bank are aware that a fraud has taken place. The speed of transactions make it difficult for banks to trace stolen money once a fraud has occurred. Very few first-time payments need to be received instantaneously. Very large payments will often be scheduled days in advance. Therefore, high-speed payments on first time payments could be made redundant with only a limited impact on consumers. (Paragraph 49)

We recommend a mandatory 24-hour delay on all initial or first-time payments, during which time a consumer about to be defrauded could remove themselves from the high-pressure environment in which they are being manipulated. All future payments to that same account could flow at normal speed to minimise inconvenience to customers. If a situation arose whereby an initial payment was needed instantly, a customer could ring their bank and additional checks could be carried out for the funds to be released. (Paragraph 50)

Payments by Faster Payments deliver a range of benefits for individuals and businesses, allowing them to make time-sensitive payments whenever needed and providing them with more flexibility to manage their money. At the same time, as the Committee notes in its report, slowing down the process for initial payments could be a means of helping to prevent APP scams.

The report notes that banks have the ability to delay payments by Faster Payments in cases where fraud is suspected, and that in some cases they providers customers with the option of delaying payments. It is important to consider the costs and benefits of mandating a 24-hour delay for payments in terms of combatting fraud, especially as banks start to implement CoP.

Money mules

Financial firms who allow members of the public to open bank accounts should provide information about what a money mule is, and the penalties for being convicted, at the point of opening. This should take the form of an easy to read factsheet, rather than being buried in the small print of terms and conditions. (Paragraph 56)

Where groups of people most susceptible to being persuaded to become money mules are identified, targeted campaigns should be undertaken. For example, banks should fund work with universities, youth organisations, community centres, schools, Further Educational institutions and sixth form colleges to provide students with information, both when they join and at graduation. Targeted campaigns where other emerging trends are identified should also be undertaken. (Paragraph 57)

The government agrees with the Committee that financial firms should voluntarily provide members of the public who open bank accounts with clear warnings about the danger of acting as a money mule, including the penalties for being convicted. However, it is worth noting that this will not have a retrospective effect on the adult population that already have a bank account, thereby limiting outreach to existing customers. Given the increasing prominence of digital and in-app banking a wide range of nudges, beyond a factsheet, should also be considered by firms.

Though funding any information campaign activity would be a commercial decision for banks, HMT encourages industry to consider how they can best increase consumer awareness of the issue. The provision of this information should build upon, and complement, the financial sector's existing initiatives aimed at stopping people from becoming the victims of crime or facilitating criminality. These initiatives include the "Don't Be Fooled" campaign, a partnership between UK Finance and Cifas, fully funded by the banking sector, which aims to deter students from becoming money mules. The campaign educates students about how criminals operate and why they are a target. It also intends to communicate the serious consequences of becoming a money mule.

Freezing bank accounts

We recommend that the FCA should set a challenging timeframe in which an account must be frozen when evidence has been received by a bank that it is receiving money fraudulently. We understand the argument made by the FCA that a timeframe may encourage financial firms to work towards the prescribed timeframe, rather than as quickly as possible, but without a deadline, some accounts are remaining open for weeks allowing further fraud to occur unnecessarily. (Paragraph 58)

The FCA will address this recommendation in their response.

Third parties

When third parties are responsible for data breaches which lead to associated fraud, they should be responsible for the associated costs. The government should consider making third parties liable for associated costs to financial services firms and encourage the Information Commission to take this account when fining firms under the General Data Protection Regulations. (Paragraph 68)

There are a number of tools available to the ICO to ensure compliance with General Data Protection Regulations (GDPR) principles on data security.[1] These include regulatory guidance, non-criminal enforcement, audit and monetary penalty notices. There are also criminal offences available to prosecute people who knowingly or recklessly obtain data without the consent of the data controller.[2]

The ICO takes a risk-based and proportionate approach to regulatory action against organisations and individuals that have breached data protection rules. That means organisations and individuals suspected of repeated or wilful misconduct or serious failures are likely to be subject to more serious sanctions than those who cooperate fully with ICO investigations and make genuine efforts to address risky processing activities.

The General Data Protection Regulation has only been in force for just over 18 months, but the ICO has shown a willingness to impose increasingly large fines in the most serious cases. Details of regulatory action taken, including against online services, is available on the ICO's website.[3]

1 Article 5(1)(f) of the GDPR requires organisations to process personal data "in a manner that ensures appropriate security … including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures"

2 Section 170 of the Data Protection Act 2018

3 https://ico.org.uk/action-weve-taken/enforcement/?facet_type=&facet_date=&date_from=&date_to=

The factors that ICO take into account when imposing fines are set out in their Regulatory Action Policy[4] and include things like the scale, the extent of any exposure to financial harm, and nature of the offending and any steps the data controller has taken to mitigate harm to data subjects.

The Information Commissioner has the power to serve a monetary penalty notice on a data controller of up to 4% of global turnover for the most serious and harmful contraventions. Sums recovered by the Information Commissioner by monetary penalties are payable into the Consolidated Fund.

De-risking

In the first instance banks should be as transparent as possible on de-risking to allow all individuals and firms the best possible chance of keeping their financial services. This may include providing greater information about why services have been withdrawn. There are examples of good practice on this and the FCA should ensure its rules allow for that to happen. (Paragraph 76)

The FCA has at times appeared unable to act to prevent de-risking from happening. The improved data gathering from the Financial Crime Report should assist it in its efforts The FCA and Financial Ombudsman Service should ensure that all instances of de-risking where a customer cannot come to resolution with their bank are fully investigated and banking services returned as quickly as possible wherever possible and appropriate. We would expect to see timely and appropriate action taken where instances of blanket de-risking are apparent. (Paragraph 77)

To combat economic crime, it is essential that Anti Money Laundering (AML)/Counter Terrorist Financing (CTF) supervisors and regulated firms take into account the specific ML and TF risks faced by their sectors and businesses. Where banks deem customers to be a high risk of money laundering, they are required to take appropriate and proportionate measures to address this risk in a proportionate manner. This may include choosing to no longer offer banking services.

While the decision to maintain or accept a banking relationship with a customer is a commercial one, the FCA has been clear that wholesale de-risking is not typically representative of effective money laundering risk management. Banks should not deal generically with whole categories of customers or potential customers and should recognise and appreciate the risks associated with different business relationships.

Where individuals or businesses are de-banked, it is important that they understand why they have been de-banked, and the FCA is working with financial institutions to help improve communications, including through a set of principles on how de-banking decisions should be made. Following the implementation of the Payment Services Regulations (2017), banks seeking to withdraw account services from payment services providers must submit an application to the FCA and PSR, who will assess these against criteria of being proportionate, objective and non-discriminatory. The government is further working to ensure de-risking does not create issues in the remittances sector by taking forward recommendations of the G20 taskforce on remittances, and working with stakeholders to ensure this can be done in a way that allows legitimate risks to be countered by financial institutions.

4 https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf

Artificial Intelligence

Banks should only use Artificial Intelligence if they have a high degree of assurance that its use will not result in bias. Regulators have a role to play to ensure it is used responsibility and does not pose indiscriminate risks to sections of society. (Paragraph 78)

The government is committed to supporting innovation in tackling economic crime. It has recently established a senior-level economic crime Innovation Working Group. This will provide a forum for government and private sector partners to explore how to promote innovation and RegTech solutions to improve the effectiveness of private sector preventive measures, while ensuring such new technology is used sensibly and with appropriate safeguards.

The UK's regulators have also taken a world leading approach to fostering innovation. The FCA's AML Techsprints in 2018 and 2019 brought together firms, regulators and law enforcement agencies to investigate how new technologies can be used to more effectively combat money laundering and financial crime responsibly.[5] The FCA has also recently made clear its interest in seeing innovation in machine learning, more specifically federated learning and travelling algorithms, alongside innovation which makes finance work for everyone. Its Sandbox will allow firms to test that technology in an environment where the regulator can pose questions around access and inclusion. The FCA has further partnered with the Alan Turing Institute to explore the transparency of AI in the financial sector and the practical challenges it presents, such as unconscious bias.[6] Meanwhile, the ICO, together with The Alan Turing institute, has published draft guidance on explaining decisions made with AI.[7] The guidance suggests practical steps to ensure AI systems are designed and used in a way that is accountable, transparent, considerate of the context and reflective of the impact on individuals and society. The guidance also covers the implications of the General Data Protection Regulation, such as the requirement to complete a Data Protection Impact Assessment, and the Equality Act 2010, such as ensuring that decisions made with AI do not have a worse impact on individuals with protected characteristics.

3. Investigating fraud as crime

The announcement of a national fraud strategy is long overdue. It followed the damning criticism of Her Majesty's Inspectorate of Constabulary and Fire and Rescue Services' report. It must now be a priority for police forces to make the strategy work. One of the actions from the Economic Crime Plan 2019–22 is that the police response to fraud is improved. The government should provide us with an update on this action within six-months of publication of this report. (Paragraph 89)

The government will provide the Committee with an update on the implementation of the HMICFRS' recommendations and other measures being taken to improve the police response to fraud within six months of the Treasury Committee's report publication, as requested.

5 https://www.fca.org.uk/events/techsprints/2019-global-aml-and-financial-crime-techsprint
6 https://www.fca.org.uk/news/speeches/future-regulation-ai-consumer-good
7 https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-and-the-turing-consultation-on-explaining-ai-decisions-guidance/

The police response

Complex fraud cases have not always been effectively 'tasked' or referred upwards. At times they are just moved from pillar to post. This is unacceptable for the victims of potentially devastating crimes. It is therefore welcome that this is both a focus of the police, and its inspectorate. (Paragraph 96)

Improvements to tasking will hopefully relieve some pressure on local forces. However, some cases will remain at the local level. The government must review how it provides support to individual police forces which consider they have complex frauds they could successfully investigate, where resources may otherwise prevent those cases progressing. (Paragraph 97)

The police response to fraud, including the provision of government support to police forces investigating complex frauds is being reviewed as part of the Serious and Organised Crime (SOC) Review, led by Sir Craig Mackey QPM.

The SOC Review will consider the powers, capabilities, governance and funding required to tackle serious and organised crime threats, including fraud, across law enforcement and the justice system in England and Wales. The findings and recommendations of the review will be presented to the Minister for Security in Spring 2020.

Reporting

We are pleased to hear that in the main, reports of economic crime from financial institutions to the police are happening in a timely manner so the police can start an investigation promptly. However, we are concerned that banks do not always appear to be reporting instances to the police where, for example, the bank has reimbursed the victim. Given the high-speed nature of the financial system, any delay in reporting to the police could prevent recovery of funds and allow fraudsters to profit at a victim's expense. (Paragraph 100)

The government should require all frauds to be reported regardless of their size, and whether or not a financial institution has reimbursed a consumer. (Paragraph 100)

The government recognises the importance of ensuring the timely reporting of fraud to law enforcement agencies in order to facilitate investigation and recovery of funds. As the national lead force for fraud, the City of London Police encourages all organisations to report fraud to the police, providing them with access to web-based applications that facilitate reporting. However, the government will consider the committee's recommendation that all frauds be reported regardless of their size, and whether or not a financial institution has reimbursed a customer.

It is not currently always clear to consumers whether a fraud should be reported to an individual consumer's bank, the police or to Action Fraud, nor is it always clear what each entity would do with the information provided. The process for reporting an economic crime needs to be clarified. We welcome the plans to issue guidance to Action Fraud and chief constables to ensure consumers reporting a crime are clearly told both how reported instances of fraud will be used, and also how they won't be used, when they report a crime. (Paragraph 105)

The serious criticism of Action Fraud in the 'Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services' report and in the media need to be addressed. In its response to this report the government should set out what it has done to address this issue. (Paragraph 106)

The government has been overseeing a programme of activities to improve Action Fraud in response to the HMICFRS report findings and issues highlighted in the media.

In May this year, City of London Police appointed an additional Detective Chief Superintendent to deliver service improvements in the National Fraud Intelligence Bureau. This includes implementation of new processes for triaging and developing serious and organised fraud, and to oversee delivery of HMICFRS recommendations. New performance indicators have been agreed as part of Home Office and City of London Corporation accountability measures.

As a result of consultation with forces, Action Fraud victim lists highlight vulnerability and are now disseminated to forces on a weekly rather than monthly basis. Crime dissemination documentation has been redesigned to make it easier to interpret and action. Force demand and performance information has moved from bi-annual reports to monthly dashboards. Monthly and annual threat assessments have been improved to provide a more comprehensive intelligence picture and overview of national protect activity.

Guidance has been issued to forces to improve practices across a number of areas including fraud reporting and calls for service, victim communication and investigation policies.

City of London Police has been working with the National Economic Crime Centre and National Crime Agency to embed fraud within national strategic tasking and a voluntary tasking for fraud was agreed by chief constables in November 2019.

City of London Police has made clear it will not tolerate the poor behaviour by staff in the call centre exposed in The Times newspaper earlier this year. The individuals involved have been dismissed. This was swift and decisive action. An improvement plan was developed in August 2019 with 81 actions based upon an initial review by Concentrix and IBM. Actions cover recruitment, training, culture and process. Over half of the actions have been completed.

An independent review of Action Fraud and the National Fraud Intelligence Bureau by Sir Craig Mackey has been commissioned by the City of London Corporation to identify where further improvements can be made in the service. The Home Office will work with the City of London Corporation to ensure recommendations of the review are implemented effectively.

3. Consumer rights and responsibilities

The Contingent Reimbursement Model Code

We welcome the Contingent Reimbursement Model Code—a framework for financial institutions to use to determine when reimbursement should be provided to victims of APP Fraud—as a way to protect consumers. We remain unpersuaded that the Code

should be voluntary and strongly urge any relevant parties who have not yet signed up to the Code to do so. As the first year review of the Code approaches, the Code should now be made compulsory through legislation. (Paragraph 114)

In 2015, the government set up the Payment Systems Regulator (PSR) with a statutory objective to, among other things, ensure that payment systems are operated in a way that takes account of users' needs. Since 2016, the PSR has been driving forward work to make sure consumers are better protected against APP scams.

The PSR established a steering group of financial institutions and consumer representatives to develop a voluntary code of good practice to help protect consumers against these kinds of scam. At the end of February 2019, the steering group published the Contingent Reimbursement Model Code for Authorised Push Payments (the Code), which sets out the agreed principles for greater protection of consumers and the circumstances in which they will be reimbursed, making a significant step in delivering improved protections for consumers. The Code became effective on 28 May 2019 and customers of those payment service providers that are signatories are protected under the Code from this date.

The Code is still in its infancy and the government believes it should be given time to embed and take full effect before its effectiveness can properly be assessed. The Lending Standards Board (LSB), which is responsible for the Code, has committed to a first annual review of its operation in Summer 2020 and will shortly publish more information about its planned approach, including its intention to consult widely with consumer representatives and the industry. The LSB is also well-advanced with its own thematic review of the provisions of the Code governing the reimbursement of consumers, which will be completed in early 2020. The government looks forward to reviewing these findings when they become available.

At the launch of the Code, an interim funding arrangement for compensating victims was established by several launch signatories to provide reimbursements from implementation until a new long-term funding arrangement could be implemented by the end of 2019.

Industry and the regulators continue to explore options for a sustainable long-term solution for reimbursing 'no blame' victims, and the Code signatories who provided the initial funding have agreed to extend the funding deadline until March 2020, allowing these discussions to continue.

These discussions should be given time and space to continue so that a mutually agreeable 'no blame' solution can be arrived at and implemented. We look forward to seeing how these discussions unfold.

We accept that keeping the Practitioner Guide private avoids it becoming a guide to committing fraud. However, the current consumer guidance is so high level, it does not give consumers a clear sense of what is expected of them. Without sight of how the Code should work in practice, consumers may be left unable to effectively challenge their bank. This could lead to an increased number of cases being referred to the Financial Ombudsman Service and a delay in any potential reimbursement. We recommend that a more detailed consumers' guide is produced, which includes practical examples. (Paragraph 124)

The FCA will address this recommendation in their response.

Reimbursement

We welcome the FCA's recent rule changes requiring financial firms receiving payments to ensure that they are not inadvertently assisting economic crime. However, we are concerned by the lack of power financial institutions have to recover money sitting in bank accounts once it has been reported as stolen. Given the development of MITS technology, the government should review the current legislation around recovery of stolen funds to ensure that victims can be reimbursed as quickly as possible, whilst protecting legitimate transactions. (Paragraph 129)

In the Economic Crime Plan the government, working with UK Finance, has committed to develop a framework to repatriate funds to victims of fraud by December 2021. This framework will seek to better utilise new technology to track and trace fraudulent transactions, such as the Mule Insights Tactical Solution (MITS). This will include reviewing current legislation around the recovery and repatriation to victims of stolen funds, and, if necessary, make recommendations for appropriate changes.

Gross Negligence

The existing Payment Services Regulations do not define what actions by a customer would be deemed as 'gross negligence'. As a result, each individual firm can set its own bar of what customer behaviour it would deem to be grossly negligent. This could lead to a lack of consistency between how customers with the same circumstances are treated. We recommend that an accepted definition for gross negligence should be agreed by the regulators. The regulators should require financial firms to produce an easy to read lists of 'dos and don'ts' for customers, to show how the individual financial firms would define proper account usage in the majority of circumstances. Such lists would allow for variations between firms. (Paragraph 139)

The FCA will address this recommendation in their response.

Financial firms must ensure that vulnerability is a key factor in determining if a consumer was grossly negligent. The FCA should ensure that the outputs from their recent consultation on the Guidance for Firms on the Fair Treatment of Vulnerable Customers covers any finding of gross negligence. (Paragraph 140)

If firms do find individual consumers to have been grossly negligent, we recommend their customer responses quote the legislation the firms are relying upon to refuse making a reimbursement, alongside an explanation of how this conclusion was reached. Although it may cause distress, we believe that using the phrase 'grossly negligent' would provide a very clear explanation to the consumer why their claim is being refused, and on what grounds. (Paragraph 141)

The FCA will address this recommendation in their response.

Education

Education has an important role to play in the wider fight against economic crime. There is always merit in equipping consumers with skills to give them the confidence and knowledge to pause and think about whether or not the situation they have found themselves in could be a fraud. (Paragraph 148)

We recommend that financial firms should undertake targeted education campaigns where trends have been identified and when new scams appear. These should include information at the point of opening an account about the consequences of being a money mule and information regarding emerging frauds so that consumers can stay vigilant. (Paragraph 149)

The government agrees with the Committee's recommendation that financial firms should voluntarily undertake targeted education campaigns where trends have been identified and when new scams appear, and that these should include the provision of information on opening an account.

The messaging should complement the existing "Take Five – to stop fraud" campaign, which is run jointly by Government and UK Finance. It is designed to equip individuals and small businesses most vulnerable to fraud with the confidence to challenge criminal approaches.

It is important that financial education is not a 'one time' exercise. We recommend that reminders are sent out to consumers in different formats and at different times. This should include online marketing and social media to target messages to younger consumers. This will ensure that firms are not only meeting their obligations of the Contingent Reimbursement Model Code, but also will help prevent fraudsters from succeeding in the first place. (Paragraph 150)

The government agrees that financial institutions should consider sending reminders to consumers in different formats and at different times to help them protect themselves against fraud.

The "Take Five" campaign encourages individuals and small businesses most vulnerable to fraud to challenge criminal approaches. Similarly, the "Don't Be Fooled" campaign, a partnership between UK Finance and Cifas, aims to deter students from becoming money mules, by educating them on the threat and the serious consequences of doing so.

Appendix 2: Payment Systems Regulator Response

Dear Chair

Payment Systems Regulator response to the Treasury Select Committee report on the consumer view of economic crime

Firstly, I would like to congratulate you on your re-election as Chair of the Treasury Select Committee.

The Payment Systems Regulator (PSR) welcomes the Treasury Select Committee's (TSC) report on the consumer view of economic crime. The report is a valuable contribution to the issue. We would like to take this opportunity to respond to the recommendations in the report that relate to the PSR's work, as detailed below.

Confirmation of Payee

TSC recommendation (6): Confirmation of Payee should be introduced as a matter of urgency. Every delay leaves more people vulnerable to falling victim to economic crime. If the implementation date of March 2020 begins to look in doubt, regulators should consider introducing sanctions, such as fines, to firms who have not met the deadline. (Paragraph 41)

PSR response: Confirmation of Payee (CoP) is an important way to fight financial crime, and to protect people from the devastating impact that Authorised Push Payments (APP) scams can have. We have been taking steps so that it is delivered as soon as possible and in a way that protects customers.

On 1 August 2019, we gave Specific Direction 10 to members of the UK's six largest banking groups to implement CoP fully by 31 March 2020. We set out that we expect industry to implement this system to protect people, as we were concerned it was not acting quickly enough.

We are actively engaging with the directed payment system providers (PSPs), to ensure that they have effective implementation plans in place to meet the deadline. The directed PSPs have successfully passed the first major milestone towards CoP, and can all now respond to requests from other PSPs to provide account name information. The next step is to implement the full capability for customers.

We will continue to monitor both the progress and compliance by the PSPs. If, following the 31 March 2020 deadline, we identify that directed PSPs may be failing to comply with our requirements, we have powers under the Financial Services (Banking Reform) Act 2013 to investigate and, where we find a compliance failure, to impose a remedy—including the power to impose a financial penalty. Our approach to deciding whether to take action, and the appropriate form, will involve us considering all of the circumstances of the possible compliance failure and the factors set out in our Administrative Priority Framework.

TSC recommendation (7): The Payment Systems Regulator should ensure that all relevant firms can implement Confirmation of Payee by the end of 2020. (Paragraph 42)

PSR response: For CoP to be effective and achieve the potential benefits for banks and their customers, it needs to be implemented in a timely and coordinated manner and be widely available. People making electronic payments should be familiar with seeing CoP as part of their payment experience and benefit from the protections it offers.

This means that the system itself must have common rules and standards to make sure both the sending and receiving banks can match the data to ensure the payee is sending money to the intended recipient. This could not happen without those common rules and standards, which have been developed by Pay.UK to cover PSPs that operate accounts with their own unique addressable sort code. We directed members of the UK's six largest banking groups, which are involved in the vast majority of FPS and CHAPS transactions, to deliver CoP by 31 March 2020. We gave smaller PSPs the benefit of more flexibility as to when to introduce the CoP service.

However, following ongoing engagement with the whole sector, we know that smaller PSPs want to give their customers the same level of protection as larger firms. There is a strong incentive to implement CoP as soon as they can, there are a number of institutions outside our direction, that are progressing their plans and are looking to deliver CoP in 2020.

For some smaller PSPs which operate accounts without their own unique addressable sort code, Pay.UK is developing the necessary rules and standards to enable them to implement CoP, and we expect these to be ready by the end of 2020.

TSC recommendation (8): We recommend that spelling mistakes are flagged within the new Confirmation of Payee system. (Paragraph 43)

PSR response: The systems to implement CoP make sure that names of recipients are checked before payments are sent. It will work by checking the name and account details entered by the payer match those on the account they are sending money to. If these do not match, or only give a partial match, CoP will alert the customer of this; this will act as a warning for them to check with their payee before proceeding with the payment.

Importantly, if the sending bank allows a transaction that matched to pass through the system, which then turns out to be a fraudulent payment, the sending bank will bear responsibility as they did not have sufficient checks in place.

Delaying Faster Payments

TSC recommendation (10): We recommend a mandatory 24-hour delay on all initial or first-time payments, during which time a consumer about to be defrauded could remove themselves from the high-pressure environment in which they are being manipulated. All future payments to that same account could flow at normal speed to minimise inconvenience to customers. If a situation arose whereby an initial payment was needed instantly, a customer could ring their bank and additional checks could be carried out for the funds to be released. (Paragraph 50)

PSR response: The speed of Faster Payments has brought a lot of benefits to consumers and businesses—allowing people to manage their money in real time with certainty. The UK is a global leader in providing payments that are made quickly and safely. Preventing fraud continues to be an important part of this. Our approach to tackling APP fraud has been to press PSPs to meet standards for protecting customers, via the Contingent Reimbursement Model Code (CRMC) and, in so doing, to provide a strong commercial incentive on banks to take appropriate actions to prevent APP scams.

There are already systems in place that can slow down payments to allow for additional checks to take place if PSPs believe there is fraudulent activity. This provides the flexibility to mitigate fraud without losing the benefits of instant payments.

Contingent Reimbursement Model

TSC recommendation (26): We welcome the Contingent Reimbursement Model Code framework for financial institutions to use to determine when reimbursement should be provided to victims of APP fraud as a way to protect consumers. We remain unpersuaded that the Code should be voluntary and strongly urge any relevant parties who have not yet signed up to the Code to do so. As the first-year review of the Code approaches, the Code should now be made compulsory through legislation. (Paragraph 114)

PSR response: The Code, which came into force with effect from 28 May 2019, was designed to give people the confidence that, if they had done nothing wrong, they would be reimbursed. The signatories to the Code have been considering reimbursement claims from victims since this date and have committed to reimbursing victims of APP scams in line with the obligations set out in the Code.

Given how new the Code is we do not yet have a full picture of how effective it is—and it is critical that any arrangements for protecting customers and reimbursing victims are effective—whether they are voluntary or mandatory.

Reflecting this, we are engaging closely with the Lending Standards Board (LSB) which is the governing body for the Code, as it carries out its first thematic review of the Code in January this year. This will look at making sure that signatory firms are interpreting the Code consistently and correctly, where victims of APP scams were not to blame. They have indicated that a full report of this initial review will be published shortly. We will also engage with them when it undertakes a full annual review of the Code in the summer of 2020, as well as engaging with the Financial Ombudsman Service on the outcomes consumers are experiencing under the Code.

The Code was not designed to be static; but rather act as a package of protections that evolve over time as consumer (and criminal) behaviours change, and the industry continues to develop. Experience of using the Code will no-doubt identify areas that can be improved. One key area of improvement—as your recommendation also notes—is to widen membership to protect more consumers.

More broadly, we are mindful that this is a fast-moving area, and that if we are not satisfied that the Code has had the impact it was designed to achieve, we will explore alternative approaches. This would involve considering the potential to legislate.

TSC recommendations (35 & 36): We recommend that financial firms should undertake targeted education campaigns where trends have been identified and when new scams appear. These should include information at the point of opening an account about the consequences of being a money mule and information regarding emerging frauds so that consumers can stay vigilant. It is important that financial education is not a 'one time' exercise. We recommend that reminders are sent out to consumers in different formats and at different times. This should include online marketing and social media to target messages to younger consumers. This will ensure that firms are not only meeting their obligations of the Contingent Reimbursement Model Code, but also will help prevent fraudsters from succeeding in the first place.

> *PSR response:* As well as making sure that victims of APP scams are reimbursed if they have done nothing wrong, the CRM Code also includes requirements that PSPs should take reasonable steps to raise awareness and educate customers about APP scams and the risk of fraudsters using their accounts as 'mule accounts'. As part of their first annual review in the summer 2020, the LSB will review how banks have implemented the Code.
>
> Collective initiatives to raise consumer awareness have been led by UK Finance, such as the "Take Five" campaign. To inform future activity, it is important that firms learn and understand which of their approaches work and have the most impact in improving consumer awareness. We would therefore expect to see firms taking steps to assess the outcomes of their actions to raise awareness and educate customers and review their activities in light of this.

Making sure that people are protected from the devastating impact of APP scams continues to be a key priority for the PSR. We will continue to make sure that the UK's payments systems operate in a way that benefits everyone and, importantly, that people can be confident their money is protected.

I am aware that both the Treasury and the FCA are also responding to the recommendations, and I trust this update helps provide a full outline of the work we are doing.

Yours sincerely

Chris Hemsley

Managing Director

Appendix 3: Financial Conduct Authority response

Treasury Select Committee's report on Economic Crime: Consumer View

I wanted to respond to the Committee's report on economic crime: consumer view, which I read with great interest. The report makes a number of recommendations touching on the FCA's work and I wanted to set out the FCA's role in protecting consumers from fraud and scams, before sharing our thoughts on the recommendations below.

Protecting consumers is at the heart of everything that we do as a regulator. The FCA, as the conduct regulator and money laundering supervisor for the financial sector, has a keen interest in frauds against consumers or businesses using the financial system.

Some frauds are perpetrated against consumers by firms carrying on regulated activities without FCA authorisation. The FCA has powers under the Financial Services and Markets Act 2000 (FSMA) to investigate and prosecute those carrying on such unauthorised business. In appropriate cases, the FCA may also add fraud charges.

We focus on using our powers to actively pursue those carrying out unauthorised business whilst also undertaking a broader range of consumer education initiatives designed to prevent consumers from being susceptible to scams. We do this by actively warning them about both specific scams and the general risks of falling victim to scams and frauds. Our ScamSmart campaign aims to give at risk consumers the information, knowledge and tools to stop them falling victim to investment and pension fraud. We use TV, print, radio and digital advertising, as well as press activity and partner communications to build awareness of the risks of investment and pension fraud and give consumers tips on how to spot the techniques used by fraudsters.

The FCA also often find examples of schemes outside our remit, where we have no power to investigate or take enforcement action. The FCA is not funded or structured to be a general fraud investigation or prosecution agency and has a limited fraud remit with no general statutory powers to investigate or prosecute fraud.

The FCA is however a committed partner in the National Economic Crime Centre (NECC) where we work closely and in a coordinated manner with law enforcement agencies, government departments, regulatory bodies and the private sector to support the Government's Economic Crime Plan and ensure cases are addressed by the best placed investigation or prosecution agency.

We also work with other bodies within the financial regulatory framework such as the Payment Systems Regulator (PSR) and the Financial Ombudsman Service (the Ombudsman) to maximise tools to tackle fraud and we work with the financial sector to ensure authorised firms' systems and controls are resilient against fraudsters.

As such, we welcome the Committee's recommendations on how regulators, Government, law enforcement and industry can work together to help protect consumers.

Data on economic crime

In order to ensure a clear picture of the scale and types of economic crime facing consumers, the FCA should publish data on economic crime within six months. It should evolve its data collection practices to ensure they allow for emerging trends, while still enabling year-on-year comparisons. (Paragraph 15)

The FCA has started to receive fraud data from banks and other payment service providers under new fraud reporting requirements (introduced in January 2018). The data are broken down into volumes and values by fraud type. We will publish some of these data on an aggregated basis to enable year-on-year comparisons.

Freezing accounts

The FCA should work with financial institutions to ensure consistency across the sector. We recommend that the FCA uses its powers to set a timeframe in which an account must be frozen when evidence has been received by a bank that it is receiving money fraudulently. (Paragraph 28)

We recommend that the FCA should set a challenging timeframe in which an account must be frozen when evidence has been received by a bank that it is receiving money fraudulently. We understand the argument made by the FCA that a timeframe may encourage financial firms to work towards the prescribed timeframe, rather than as quickly as possible, but without a deadline, some accounts are remaining open for weeks allowing further fraud to occur unnecessarily. (Paragraph 58)

We agree that there needs to be consistency across the sector. To attempt to resolve inconsistent approaches taken by firms for the trigger of suspicion, that would lead to a suspicious activity report being sent to the National Crime Agency, the Law Commission consulted last year on whether guidance ought to be issued on Part 7 of the Proceeds of Crime Act 2002 (POCA), including in relation to suspicion.

Among other things, in the response to that consultation the Law Commission recommended a single, definitive statutory source of guidance on the money laundering regime in Part 7 of the POCA, and an amendment to POCA to impose an obligation on the "Secretary of State" (Home Office) to issue guidance covering the operation of Part 7 of POCA and the threshold for suspicion. As such, we will await the Government's interim response to the Law Commission's report to ensure a consistent approach.

However, if the FCA were to identify outlying firms in this respect, we would seek to understand more about their approach through the course of our supervisory activity.

24-hour delay on first-time payments

We recommend a mandatory 24-hour delay on all initial or first-time payments, during which time a consumer about to be defrauded could remove themselves from the high-pressure environment in which they are being manipulated. All future payments to that same account could flow at normal speed to minimise inconvenience to customers. If a situation arose whereby an initial payment was needed instantly, a customer could ring their bank and additional checks could be carried out for the funds to be released. (Paragraph 50)

The FCA proposes that regulators and industry consider the costs and benefits of mandatory delays versus voluntary "opt-in" delays in combatting Authorised Push Payment fraud (APP fraud). However, we also propose that HM Treasury should take part in assessing the costs and benefits of each option, since it is likely that the Payment Services Regulations 2017 would need to be amended if delays were to be made mandatory.

Therefore, we agree that we should consider the benefit of a mandatory delay of up to 24 hours following the implementation of Confirmation of Payee, taking into account whether the introduction of Confirmation of Payee reduces or removes the benefit of a mandatory delay.

Derisking

The FCA and Financial Ombudsman Service should ensure that all instances of de-risking where a customer cannot come to resolution with their bank are fully investigated and banking services returned as quickly as possible wherever possible and appropriate. We would expect to see timely and appropriate action taken where instances of blanket de-risking are apparent. (Paragraph 77)

The FCA agrees that transparency is vital in banks' communications with consumers when considering whether to close an account.

Under the Payment Services Regulations, banks must grant certain types of payment service providers (which could include money transfer businesses, for example) access to payment account services on a proportionate, objective and non-discriminatory basis. Banks must also notify the FCA, providing duly motivated reasons, where such access is refused or withdrawn.

We would expect these reasons to relate specifically to the individual circumstances of the provider. In addition, the Financial Ombudsman Service investigates cases where consumers' or businesses' accounts are closed and decides whether the customer has been treated fairly, taking into account the relevant law, regulators' rules and guidance, industry codes of practice and good industry practice where relevant.

In all instances of eligible complaints the Ombudsman Service will fully investigate to try and understand what has happened, and ensure that banks have not taken inappropriate or disproportionate measures. The FCA will continue to liaise with UK Finance on trends and guidance to banks.

Contingent Reimbursement Mode Code

We remain unpersuaded that the Code should be voluntary and strongly urge any relevant parties who have not yet signed up to the Code to do so. As the first year review of the Code approaches, the Code should now be made compulsory through legislation. (Paragraph 114)

To ensure we have a sustainable and long-term solution that offers protections to consumers, we agree that the code should be made compulsory or an equally suitable solution is found, depending on the findings of the review.

Gross negligence

We recommend that an accepted definition for gross negligence should be agreed by the regulators. The regulators should require financial firms to produce an easy to read lists of 'dos and don'ts' for customers, to show how the individual financial firms would define proper account usage in the majority of circumstances. Such lists would allow for variations between firms. (Paragraph 139)

The FCA's document "Payment Services and Electronic Money – Our Approach"[8] already provides some guidance on the meaning of gross negligence.

However, as the FCA is planning to consult on the Approach Document this year, we will consult on whether more detailed guidance should be included. We will also work with industry to consider how best practice can be shared, and how decisions of the Financial Ombudsman are reflected in firms' dealings with their customers. This work should also address the Committee's recommendation that consumers be provided with guidance. (Paragraph 124)

The FCA should ensure that the outputs from their recent consultation on the Guidance for Firms on the Fair Treatment of Vulnerable Customers covers any finding of gross negligence. (Paragraph 140)

We are planning to publish a second consultation on the draft guidance in Spring 2020. The guidance makes clear that, in order to pay due regard to the interests of customers and treat them fairly, firms should understand what makes customers vulnerable and their needs and ensure the products and services they provide support the fair treatment of vulnerable customers.

I hope this is helpful.

Andrew Bailey

Chief Executive

8 https://www.fca.org.uk/publication/finalised-guidance/fca-approach-payment-services-electronic-money-2017.pdf