25 June 2018

Dear Meg,

RESPONSE TO THE PUBLIC ACCOUNTS COMMITTEE INQUIRY INTO THE GROWING THREAT FROM ONLINE FRAUD

I am writing to update you on progress made on the recommendations from your inquiry into the growing threat from online fraud, in advance of my appearance before the Committee on 27 June. This letter updates the information provided in the Treasury Minute published on 1 March.

To take each recommendation in turn:

**On improved transparency of fraud prevention measures.** We have been working with members of the Joint Fraud Taskforce to develop a phased approach to improved transparency. This will be in two stages: the first will enable more data to be shared with law enforcement and Government to better set the operation and policy response, whilst stage 2 will publish information on the fraud prevention measures banking, and other sectors, have in place to help consumers make informed decisions about their banking provider.

**Improved data-sharing arrangements between the private sector and law enforcement/government will increase the volume of fraud data shared, which will in turn enable improved analysis of fraud threats, typologies and vulnerabilities.** This will also be facilitated through the establishment of the new National Economic Crime Centre.

Data and information has already commenced and includes:

- more frequent information to law enforcement on emerging trends and threats;
- more frequent and joined-up threat assessments and intelligence sharing;
- production of a joint law enforcement and industry threat assessment on fraud;
- more shared intelligence on attempted fraud which will enrich crime reports; and
- information on fraud prevention data to facilitate sharing of best practice across the private sector.
A targeted approach to share best practice, close vulnerabilities and raise standards across the board will be based on a publicly available assessment of activity undertaken to reduce vulnerabilities. We will explore ways to deliver this, including through a number/star-system approach, akin to hotel rating standards or sector specific wide kite-marks.

We believe this type of scheme would:

- Give consumers an improved view of protections put in place by separate banking providers and providers in other sectors such as retail and telecoms;
- Help raise the bar in terms of preventative measures;
- Drive faster take-up of new fraud prevention technology; and
- Drive faster take up of fraud prevention initiatives e.g. confirmation of payee.

A working group, made up of industry, regulators, and wider Government representatives will consider:

- Cost and resource implications;
- Identification of the suite of activity and outcomes that could constitute minimum through to best practice;
- Development of suitable metrics;
- Consideration of who might award and administer a rating system or kite mark; and
- Potential legal risks (e.g. judicial review challenge)

This group will deliver recommendations by the autumn 2018.

We support the policy aims of increased transparency. At the same time, the financial sector and regulators have significant concerns about the potential unintended consequences that could arise from publishing such data. These are risks which will need exploring and managing.

We will also look to roll out this scheme to other sectors, following implementation by the banks, ensuring that consumers are informed about anti-fraud measures in place more widely.

On utilising technology to stop fraud, and returning more money back to victims, good progress is being made.

Through the Taskforce, Mastercard and UK Finance are working to develop new technology to reduce ‘Card Not Present’ Fraud, particularly that which takes place by telephone or mail order. The most recent figures from UK Finance show that Card Not Present Fraud fell by 5% to £409.4m in 2017, compared to the previous year. However, this remains a priority for the Taskforce.

An initial forecast indicates that planned CNP fraud reduction activity is most likely to produce a reduction in fraud losses in the region of 30 percent by 2019.
The Regulatory Technical Standards (RTS) on Strong Customer Authentication (SCA) has been published in the Official European Journal on 13 March 2018. The RTS will come into force 18 months after this date (14 September 2019). Consumers will benefit from enhanced e-commerce security solutions, introduced in line with this regulatory requirement and we expect to see increased reductions in CNP fraud from September 2019 as a consequence.

Mail and Telephone order (MOTO) security standards are not covered by this regulation and continue to be vulnerable to fraud. By utilising technology, we are focused on closing loopholes fraudsters exploit. We have consulted across the industry on a solution and are now considering the responses to inform the design phase, which will take place over the summer.

The Taskforce is committed to ensuring that victims of fraud have more of their losses returned. We are working with the Payment System Regulator, which is developing a contingent reimbursement scheme to, in certain circumstances, refund victims of Authorised Push Payment Fraud. This is complementary to the Funds Repatriation scheme being developed and tested under the Joint Fraud Taskforce.

On funds repatriation, the first phase of a pilot scheme has demonstrated that the technology exists to enable the banks to trace and freeze funds that have moved through money mule networks or split across different accounts through the money mule process. The second phase, to test hypotheses around retracing the fraudulent movement of funds, so that victims of fraud can be reimbursed, has now begun (23 April). The Department looks forward to receiving the results in July.

The Home Office has also established a legal issues group to consider and clarify what specific legal and regulatory barriers there are to implementing both the funds repatriation scheme and other prevention and response measures intended to benefit victims of Authorised Push Payments scams.

On fraud prevention campaigns, phase two of the Take Five campaign has concluded and planning for phase 3 is now underway. This approach represented a significant shift towards a targeted behaviour change campaign, focusing specifically on increasing the general public’s resilience to financial fraud, through encouraging them to make a confident challenge when faced with impersonation scams on the phone, via email or text.

The campaign’s £3.1 million budget – of which the Department has contributed £500,000 against £2.6 million of funding from the financial sector - has been deployed across a range of communications channels from social media to radio advertising with over 13 million views of the campaign video.

The campaign has also harnessed the influence and credibility of leading parliamentarians, Joint Fraud Taskforce members, key private sector organisations, financial institutions, and other government departments. Phase two culminated in Take Five Week, reaching an estimated 47% of all UK adults through media coverage, and resulting in around 200,000 completions of Take Five’s ‘Too Smart to Be Scammed’ quiz.
Take Five has achieved impressive reach and recall - with almost half of those surveyed in January now recognising some form of Take Five campaign activity. In addition, 23% of consumers surveyed were able to spontaneously recall some form of Take Five campaign activity in January, a similar proportion to those who recalled the Barclays campaign activity on fraud.

Communications has the power to change behaviour and attitudes, increase public understanding and build trust. To deliver fraud prevention effectively, we must recognise that shifting behaviours on some issues, such as fraud, takes considerable time and that a targeted six month campaign is the start of a longer process. That is why the Joint Fraud Taskforce is committed to continuing the support for Take Five.

On measuring the performance of the Joint Fraud Taskforce: following recommendations made by the PAC and National Audit Office, the Home Office has commissioned an independent review of the Taskforce to consider:

- how the Taskforce should strengthen its governance;
- accountability for delivery of Taskforce project; and,
- the resource required from Government, private sector and law enforcement to enable the Taskforce to deliver effectively.

The review ran until the end of May and provided a report and recommendations to the Management Board on 20 June.

The Taskforce is developing a quarterly dashboard which will provide performance data and a RAG rating on each programme of work under the JFT. The format of this programme dashboard will, in part, be informed by the findings of the review. The dashboard will also include up to date figures on fraud from the Crime Survey of England and Wales (CSEW) and Police Recorded Crime Statistics (PRC).

The Department is also drafting a report on the work of the JFT which will cover the governance structure, the fraud threat, Taskforce priorities, and performance. This first report will be published in summer and will be produced annually in future.

On making improvements to the reporting and the collection of fraud data: alongside improvements set out above on public – private information sharing, we will publish evidence of the scale, nature and impact of fraud against individuals and businesses, in the form of an evidence pack created by Home Office Analysis and Insight.

Finally, on improving the law enforcement response to fraud: a thematic inspection of the effectiveness and efficiency of the law enforcement response to fraud, including online fraud, is being carried out by Her Majesty’s Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) this year.
Preliminary inspection fieldwork is underway which will be completed by the end of June. The inspection report will be published in autumn 2018.

The inspection will assess whether:

- law enforcement has a well-designed strategy for tackling fraud;
- organisational structures provide the necessary capacity, capabilities and partnerships at force, regional, national and international levels to tackle fraud; and
- the police service across England and Wales consistently provides a high-quality response to fraud.

The inspection will concentrate on fraud committed against individuals and businesses, considering police forces as well as regional organised crime units and the National Crime Agency.

This is the first inspection of its kind. As well as raising the profile of fraud at local level, it will provide the Department with valuable information that will inform its strategic decisions on how to improve the law enforcement response to fraud.

I hope the Committee finds this update helpful.

Yours sincerely,

Sir Philip Rutnam
Permanent Secretary