Ms Meg Hillier MP  
Chair, Committee of Public Accounts  
House of Commons  
London SW1A 0AA

Dear Meg,

NAO REPORT INTO ONLINE FRAUD

I wanted to thank the Public Accounts Committee for the opportunity to participate in your hearing on 18th October into the National Audit Office (NAO) report into Online Fraud. The industry takes the issue of fraud, including online fraud, extremely seriously and values the work that the NAO has done in this space.

I thought it would be helpful to follow up on some of the points and themes we discussed, and to provide further evidence that your Committee may find helpful. I would be grateful if this letter could be treated with sensitivity in terms of how it is referenced in any final report. As you will see from the below, banks carry legal risk regarding some of the actions they have chosen to take, such as returning the proceeds of fraud to victims, to deliver better public outcomes. Whilst that is the right thing to do, we have been careful with regards to how we describe these areas publicly to prevent fraudsters exploiting legal vulnerabilities.

Engagement with the Inquiry

The Committee asked why my banking members had not submitted evidence. Whilst we did not submit written evidence to the Committee, I do wish to clarify that the industry, through some of the precursor organisations of UK Finance, had been engaging with the NAO directly on their report ahead of publication and subsequently to follow up on key recommendations. However, on reflection, whilst the precursor organisations believed that was what the NAO required, I accept it would have been more helpful if we had provided more detailed written evidence. I hope the below goes some way to addressing that.

Transparency & Reporting

The Committee rightly raised the importance of transparency and clear data in understanding the total scale of the problem and queried whether banks could publish their individual fraud statistics. There was a view that this could encourage a ‘race to the top’ in terms of safety and security. As we stated in the hearing, we do not believe that it would be right for organisations to publish their individual fraud statistics.

Primarily this is because this information could be exploited by fraudsters. It is also because publishing individual figures would not reflect the fact that fraud, including online fraud, can occur from vulnerabilities or choices in other sectors, such as a retailer choosing not to use two-step verification for a card payment or where there has
been a data breach. There would need to be a more holistic way of capturing this kind of granularity to ensure that figures were accurately reflected.

By way of context it is important to note that the UK is by far one of the most transparent countries in terms of the amount of information on fraud that is shared between banks, law enforcement and with the public. UK Finance collates and publishes half yearly industry statistics from our members on fraud losses from unauthorised payments. These industry statistics are subject to stringent checks monthly and are published in the form of a press release. As part of our commitment to the Payment Services Regulator in response to the Which Super-Complaint the industry has also agreed to publish half yearly data for authorised push payment fraud to ensure we can provide greater clarity on the scale and typologies of this type of fraud. This data was published for the first time this week and I enclose a copy of our figures for the Committee’s information. We believe aggregate statistics support a better understanding of the volume, cost and impact of fraud and help underpin a stronger private and public-sector focus to drive activity. Banks also use this data to help measure and benchmark the effectiveness of their fraud controls.

The latest industry statistics for the first half of 2017 show that financial fraud losses fell by 8% year-on-year with banks now stopping more than two thirds of potential financial fraud (67%).

As you will understand, the nature of fraud prevention means that transparency will sometimes be in tension with effective operational activity. We are not complacent about safety and security and the UK banking sector works closely with law enforcement and regulators to identify and address vulnerabilities and spread good practice.

Information Sharing and Legislative Reform

The Committee also asked whether our banking members share information with other bodies to support wider anti-fraud work. Information sharing is at the heart of stopping fraud so the sector shares a wide range of fraud information across industry, government and law enforcement agencies.

On behalf of the UK payments industry and retail banking sector, UK Finance provides confirmed fraud intelligence on a weekly basis to the National Fraud Intelligence Bureau (NFIB) via our Fraud Intelligence Sharing System (FISS). We also support information sharing between members through weekly intelligence calls and other fora, and members will share cases directly with UK and international law enforcement as needed. Members also share fraud information with many other cross-industry bodies, such as CIFAS, National SIRA, National Hunter and other bodies facilitating cross-border intelligence sharing.

In the past 12 months, the industry shared intelligence on over 87,000 fraud offences with the NFIB or directly with law enforcement, and UK Finance circulated nearly 400 fraud alerts to industry covering over 500,000 accounts potentially at risk of fraud. During the same period, nearly 900 separate fraud incidents were discussed on intelligence calls and we received over 50 information requests from law enforcement.

The Committee asked if we should report every instance of fraud. In answering this question, I think it is helpful to distinguish crime reporting from intelligence sharing with law enforcement. In terms of crime reporting, we have worked with the Office for National Statistics for many years by providing them with our fraud statistics for all unauthorised fraud. In terms of intelligence sharing, banks share intelligence on all confirmed fraud cases through the NFIB. We continue to work with City of London Police on how to improve these intelligence sharing arrangements, including changes they are making to the NFIB and early discussions on the ‘555’ fraud reporting concept.

As well as information, we facilitate sharing good practice across the industry and government, including through the Joint Fraud Taskforce (JFT), the fraud prevention work of UK Finance and our Dedicated Card and Payment Crime Unit (DCPCU). I updated you on the Banking Protocol as one example of how we have developed and are sharing good practice on identifying vulnerability and the risk of fraud across the industry and national police forces. There are other examples, such as where one bank is seeking to prevent money reaching accounts believed to be money mule accounts which we are seeking to support roll out of, even though, as below, banks carry an amount of legal risk in adopting such an approach. Whilst there are many good initiatives and systems in place we recognise the need to do more. We believe a refreshed JFT, in line with NAO recommendations, will be more effective at sharing best practice and helping the industry make progress in addressing all types of fraud.

However, we also believe there is a need for a stronger legislative framework required for a transformative approach to information and intelligence sharing. We have proposed to the Government a new power to allow...
banks to more widely share information between themselves and with law enforcement for the prevention and detection of economic crime. In the fraud space, this would better help identify potential victims and prevent fraud, as well as more effectively help trace stolen funds if fraud does happen. We also believe it could be used to provide safe harbour to companies who have suffered a data breach to share details of their customers with banks to help prevent fraud.

We understand that the need to ensure the right balance on data protection and look forward to continuing to discuss this with Government. In the immediate term, our focus is on the Data Protection Bill and implementation of the General Data Protection Regulation (GDPR). We believe that this requires derogations to GDPR like that of section 29/3 of the current Data Protection Act (DPA) as well as better information sharing gateways.

**Take Five**

I would like to take this opportunity to correct the figure of £3.8 million headline spend for the second phase of the Take Five campaign that I gave in the hearing. The correct figure is £3.02 million headline spend, of which £2.52 million is contributed by UK Finance members and £500,000 is contributed by the Government. This does not include member contributions to supplementary awareness raising initiatives, such as the £125,000 the industry has committed to running a campaign on money mules.

The Committee also raised questions about the effectiveness of the Take Five campaign. As I explained, Take Five is a public awareness campaign that aims to provide simple advice to consumers and businesses on how to protect themselves from fraud and scams.

The latest phase of the campaign focuses on fraud risks from unsolicited requests for personal information, encouraging customers to pause and reflect carefully before deciding. Building on the first phase of Take Five, investment in the campaign has been trebled and includes a range of above the line advertising (Video on Demand, radio, digital). The campaign launched four weeks ago so it is not possible yet to evaluate the impact, but we are working with the Home Office to evaluate the impact of this campaign on awareness and behaviour. We would be happy to share future updates on the evaluation in due course with the Committee.

**Anti-Fraud Technology**

In response to questions from the Committee around the use of anti-fraud technology to protect customers, I wish to reinforce that banks are spending millions of pounds in advanced fraud protection systems, and use technology extensively to tackle online fraud.

This includes sophisticated monitoring technology such as biometric profiling and procedures to verify the customer and the devices that they use to make payments. For example, procedures to flag lost or stolen payment cards, fraudulent device IDs and IP addresses, and geolocation services to check for locations unusual to the customer. Card based transactions are also protected by separate authorisation processes that make use of highly sophisticated transaction risk scoring processes, and are evolving to utilise the latest artificial intelligence and machine learning technology. The customer will not always be aware of this technology as it is often used in the background such as when logging in to online banking or at each stage of the online transaction process.

However, whilst these measures help prevent 67% of attempted fraud, there is no single technological solution to online fraud soon that would have the equivalent impact of chip and PIN. That is partly because of the volume of transactions - over 18.6 billion per year – and partly because the online shopping and payment infrastructure is complicated, with different parts of the system having to decide what steps they wish to adopt. Retailers and online merchants may, for example, choose not to rely upon two step verification.

Dynamic CVCs have been suggested as a solution, but there are limitations even here. This type of technology remains vulnerable to the dynamic CVC card being physically lost or stolen and subsequently misused by criminals. In addition, the second step authentication control can be circumvented by criminals tricking customers into divulging the dynamic CVC code, as is the case with current dynamic/multi-factor authentication solutions.

More widely, the industry is also still waiting to see what requirements will flow on stronger customer authentication under the implementation of the Second Payment Services Directive (PSD2) and the associated EBA RTS (European Banking Authority Regulatory Technical Standard). The guidelines are already delayed,
which is frustrating as the industry has a desire to understand what is expected to ensure that further investment in security can meet regulatory requirements.

We have also urged a more strategic approach to this issue. We believe there is a need for the Government to lead work through the JFT for banks, retailers, internet service providers (ISPs), telecommunications operators (on whom the banks rely on to communicate with their customers) and regulators to decide on the most appropriate multi-layered approach.

Repatriation of funds

There was rightly a lot of questioning over why our banking members are not returning more money to victims, including unlocking the estimated £130 million of funds held in banks is frozen and believed to be connected to crime. By way of context it is important to note banks already routinely refund fraud where the payment was unauthorised, which includes online fraud.

On returning stolen funds to victims of fraud where the victim has authorised the payment after being scammed, the simple fact is that banks have no easy legal vehicle to do so unless instructed to do so by law enforcement or the courts. At present once the funds move to the alleged scammer, the customer no longer has legal title to them as that legal title belongs to the account holder. Equally, as you are aware, must frauds have no law enforcement investigation, so law enforcement cannot even confirm to the bank if fraud has occurred or not, as they have to assess to a criminal standard. Consequently, it is left to banks to decide if an incident of fraud has taken place or if this is contractual dispute and to decide how to treat the monies.

Banks do, where the funds can be traced, return funds to victims. However, they do so at their own legal risk to deliver better outcomes for victims. In the same way, even where banks seek to prevent funds hitting suspected money mule accounts in the first place, this is arguably a breach of a customer mandate to transfer money to that account. You will appreciate why we are careful how we discuss these issues in public as we do not wish to encourage fraudsters to seek legal redress against banks for breaching the customer mandate.

Turning to the £130 million, this figure is an estimate, of the amount of funds we believe may have been built up over time across the industry after being frozen by banks as the funds are considered to be connected to criminality as opposed simply fraud. At present there is no mechanism for, banks to easily unlock this money, to either refund to victims of fraud or indeed to pay it to the Government without a judicial instruction.

That is why the UK banking industry is working with Government and law enforcement on a more effective approach that helps return more money to victims as part of the implementation of new powers in Criminal Finances Act (CFA) which helps make it easier for law enforcement to freeze and seize the proceeds of crime including fraud. We are in discussions with the National Crime Agency (NCA) and the Home Office on this issue.

However, this alone will not resolve the problem. In addition to the CFA we believe wider reform is needed to make significant progress on repatriation of funds. Under the current legal system even where funds are restrained, banks may not know if these funds are connected to fraud, or even who the original victim is. The funds may have passed through many other accounts and banks, both in the UK and overseas before ending up in an account that a bank suspects of being a money mule account. There may be multiple victims, with case law to be applied over who gets priority and what share (such as Clayton's Principle of first in, first out). It is not always appropriate for banks to decide on the distribution of frozen funds if they came from multiple victims so this can be another hurdle to quick repatriation.

Ultimately, even if all these issues can be resolved, as above, there is still no easy legal vehicle for returning monies to victims where law enforcement or the courts have not confirmed that fraud has happened and instructed the banks to do so. That is why we are working with the JFT to deliver a legal framework which supports effective financial crime prevention and disruption, including a more effective approach for identifying and repatriating funds held by our members to victims. This is long term work and will require legislative and regulatory changes to support it, however we firmly believe this is the right approach to take.
Reducing the drivers of fraud

I also thought it may be helpful to summarise some of the areas, as referenced above where the industry has suggested legislative or regulatory changes to better prevent and detect fraudsters, and to refund victims where it happens. We believe that more needs to be done to reduce the drivers of fraud. These changes include:

- The legislative framework for banks to share information more easily to prevent and detect fraud, as well as the ability to share information more swiftly because the speed at which information can move does not mirror the speed of monies.

- The ability for banks to slow down payments where there is concern and be protected when doing so in good faith as the current legislative requirement is within one working day, and the regulatory expectations is within 2 hours, soon to be 15 minutes. Clearly given there are over 18.6 billion transactions per year, it is not possible to easily spot possible fraud without being able to calibrate payments accordingly.

- The legislative ability for banks to return monies to victims or to law enforcement and be protected when doing so in good faith. It is incoherent that banks face legal risk for seeking to do the right thing, or have to monitor accounts where they would prefer not to hold the monies as there is no easy way to unlock them.

- The regulators and law enforcement to provide guidance to banks on thresholds for deciding if fraud has happened, and subsequent decisions that flow from that with regards to sharing information and holding and moving monies. Again, it is a strange situation where banks have having to use civil powers to make in essence what is a criminal assessment.

As well as new legislation, there is also a need to ensure that we do not inadvertently row back from the powers banks already use to prevent and detect all types of economic crime. As part of that there is a need to ensure that the Data Protection Bill, which seeks to implement the General Data Protection Regulation (GDPR) explicitly provides the protections allowed under GDPR for banks to use automated decision making for public good outcomes. For example, the use of automated decision-making is vital in monitoring transactions to detect and block fraud, resulting in £6 out of every £10 of fraud stopped by banks.

The protection of personal data is important, and these systems of course need to be carefully monitored, and customers need to have a right to query decisions and have them reconsidered. However, the legal framework also needs to ensure that data can be used in defined circumstance to achieve legitimate business and public policy outcomes. For financial services, as well as preventing fraud, this also involves systems and procedures to allow personal data to be used when necessary to ensure responsible lending (preventing over-indebtedness), detecting and preventing money laundering, tax evasion, terrorist financing, human trafficking and other crime, and managing liquidity and capital risk appropriately to preserve financial stability.

We have fed back these concerns to the Government and would welcome the support of the Committee on this issue.

I hope the additional information I have provided to the Committee serves to be a useful addition to your inquiry and I would be happy to provide further information on any of the areas above if that would be helpful.

I have also copied this letter to Brian Dilley, the Permanent Secretary of the Home Office and the Commissioner of the City of London Police.

Yours sincerely,

Stephen Jones
Chief Executive