On Demand Payment Technologies – Written evidence (FDF0046)

1. Fraud Landscape

A. Fraud risks are for a) Individuals, b) Government and c) Businesses:

Since 2015, the rise of crypto/digital Fraud has become expediential on a major scale.

Bank Fraud across the three groups are rife. In particular:

- UK Authorised Push Payments Fraud (APP Fraud) exceeded Credit Card Fraud in 2021
- By 2024, (APP Fraud) will exceed burglary in case numbers
- Burglary fell (20%) and APP Fraud increased (70%). Chances of Criminals going to Court have dropped from 1 in 20 cases for Burglary and to 1 in 500 for cyber/fraud

Online Fraudsters are 'invisible' through the use of fake emails, texts, phone calling and phone numbers backed by unchallenged ads and posts on Social Media Platforms**.**

According to the Office for National Statistics there were **5.1 million cases of Fraud** last year. **UK Banks inculpates** customers and less than half of the victims were reimbursed. **Which?** believes (43%) of individuals did not bother to report the crime.

95% of UK Banks do not operate with **Confirmation of Payee (CoP**). CoP verifies the true ownership of the Bank Account. The Netherlands Banking Community utilise CoP and Fraud has gone down 80% since 2017.

In 2014, Digital Policy Alliance showed APP Fraud can be reduced instantly by 70 to 80% and with Mule Networks identified and tracked. Banks detest sharing 'Payee' information with other banks hence little action taken with Faster Payment Fraud while 'Track and Trace' methods developed to counter Mule Networks.

COVID has accelerated the move to the new cyber/digital world by replacing the existing physical world and behaviours virtually overnight.

Technology is plentiful, inexpensive and growing in capacity year on year. Over the last 5 years, storage and data access has increased by a multiple of 10.

Bank Branches, to where the Police and Bank Staff have shown that by working together they can put a stop to Fraud, been reduced 50% since 2015

B. Impact on Future Economic and Technology to Fraud

Without Government action the three stages in committing crypto/digital fraud will continue to **augment** the lack of control in preventing and stopping scams.

1. Fraudsters Persuasion to gain the Victims attention
2. Intimidation and getting the Victim to set up a fake company or personas on their online banking app including coercing/pleading the Victim for access to the app
3. Victims forced into silence, intimidated to make the payment from their (Payer) Bank Account to the Fraudster's (Payee) Bank Account by Faster Payments.

   The payment is sent and delivered in seconds; arrives at the Fraudster's Account and immediately the Fraudsters send the monies to their other UK Bank Accounts.

Fraud is not treated as a crime per se and there is no urgency within banking and Government to change the situation or attitude. Individuals are virtually powerless against the Banks with 'fraud is the client's issue' response. Large businesses and the Financial Service Ombudsman do challenge banks over Fraud attribution.

C. Are the Victims of Fraud treated as a Priority? ~ No ~

In the time before the internet Fraud was a white-collar crime. Banks never admitted to being defrauded. The Police investigated only major Frauds, in excess of hundreds of thousands, and still do. It is not the fault of the Police as Financial Fraud was then focused on The City of London and a niche crime. Now in the cyber/digital world anyone, anywhere, can become a Fraudster at scale.

Fraudsters run scams from anywhere. Fake telephone numbers from any countries to exploit people are used. Investment and Cryptocurrency Fraud openly use international numbers that often cannot accept return calls. Cards, if used, need to be cancelled to stop a fraudulent international payment that same day.

D. Role of International Actors in UK fraud landscape

The UK, having created Faster Payments, are currently being copied in 70 countries should lead on to creating world class Fraud Solutions.

SWIFT, the world's payment society leads in the development of stopping payment fraud. **SWIFT** International Bank Account Numbers **(IBAN) however do not use CoP (Confirmation of Payee).**

The Dutch Banks use CoP and have introduced it to payments going to France and Germany. The UK Government should show best practice by ensuring all Domestic and International Payments verify the true ownership of the Payee Bank Account.

Telephone companies are tracking the use of international calls closely helping prevent fraudsters in Country A operating in Country B.

Cryptocurrency frauds, with regulations, are becoming more controlled but few barriers exist to stop borderless fraud.

2. Actions to Tackle Fraud

E. Current effectiveness for Policing Fraud

The effectiveness of The City of London Police, including Action Fraud and the National Fraud Intelligence Bureau as the lead Police Force for Fraud is minimal. The issue is the level of low value Fraud (less than £5,000) is increasing at alarming rates. The cost of the Police and the Banks to investigate a case is a 'state of play' as the chances of conviction is less than 0.2%.

Cyber fraud is a volume-based business and needs exigencies for technology, including Artificial Intelligence, to identify the Fraudsters, their mode of operandi, close them down instantly and meaningful penalties.

Recommend a single command aimed at cyber/digital Fraud and working closely with the Home Office and the Police.

F. Sufficient Resources

The requirement to properly address the emotional distress of being defrauded demands resources that cover the handling of cases in a sympathetic approach. At present Banks manage the defrauded as 'it's their fault' and traditional Policing as 'is cyber fraud really a crime?' This is unhelpful to those who have to handling their/family fraud circumstances. A much more positive approach is required to tackle the Fraudsters at source.

Currently the belief is, (are) Bank Clients aiding and abetting the scammers? And not, 'it's the Fraudsters' that are using available technology to steal from the innocent?

To be of service to the Payer (client) the Bank/PSP (Payment Service Providers) must reflect their Know Your Customer (KYC) of the owners (Payee) and the time frame as to when the Account was opened initially. This information will enable the Bank to give clearer insight to Fraud risk. If the risk is high and the client goes ahead and is defrauded, the client should not be entitled to reimbursement.

Additional information for online help and real-time action is required to tackle the cyber criminal.

G. Responses to the Private Sector

The private sector provides an uncoordinated approach to cyber crime. Many in the Private Sector do not see cyber fraud and security as a significant or priority incident until it happens to them. Fraud historically has been a one-off encounter and time to react has been in days/weeks not seconds.

One way to get the Private Sector's attention is to set penalties, both financially and reputational that would impact the group and not the individual subsidiary. These incentives help to overcome the silo practises within a company.

To overcome silo practices within Banking and Payment, the demand to share vital data across the industries is imperative. Unbelievably this is not happening today.

All Banks under KYC, Anti Money Laundering (AML), and banking criteria on stored information know who the Fraudsters are and where the monies went. The issue is Banks are reluctant to share Payee information with each other even when cyber/digital Fraud is occurring unrestrained.

H. Data Sharing

The information Commissioner's Office, home of upholding information rights (GDPR), will be the first to explain they condone cyber fraud. It is how and in what form the data is shared that is of concern.

What is needed is a call for third party(s) to analyse the ownership of Fraudsters' Bank Accounts to identify who they are, where they operate, and the level of activity.

Banks to engage in bi-lateral agreements between each other to identify Fraudster activities quickly and permitted to screen against known Fraudsters' Lists.

This will enable Bank Investigators to stop Fraudsters and pass the details to The Home Office/Police in the format necessary to meet the requirements of the law.

I. Role of the Individual

Cyber crime represents a culture shift for the individual. The individual needs to ask for data that certifies the person is legitimate, and should they not be, have the information that can be used to identify and track them down.

This is not easy for anyone as the personas in the crypto world are so life-like. Therefore, all people in the payment chain – individual (Payer), Payer Bank, new persona (Payee), Payee Bank – need to work together in real-time, to identify the level of Fraud risk. The Individual, provided with the probability that the payment is a scam, can authorise it but does so knowing that the liability belongs to them.

Fraudsters take as much money as possible and then move it as fast as possible. Once the Victim has made the payment using Faster Payments, the payment arrives in milliseconds. The Fraudster immediately uses Faster Payments to move the money to their many different Bank Accounts.

Bank/PSP (Payment Service Provider) upon making a Faster Payment to a new Payee is no different to that of any existing Payees; yet the new Payee is unknown to most likely both parties. Before making the payment to the new Payee Bank/PSP need to ensure the client

understands the risk level of fraud and that they will be held liable should it be a scam payment.

Mandate certain data on scammer behaviours to increase/decrease the level of fraud risk. For example, the Payee transaction behaviour on the average time money is spent in the account and any Payer payment exceeding 30% of the balance may possibly reflect a scam payment.

Banks must have the latest technologies and real-time information sourcing to protect their clients from the Fraudsters who are in effect controlling them today.

3. Legislative Remedies

J. Assessment of Fraud Act 2006

The Act came into force effectively on 15 January 2007 the same year Steve Jobs unveiled the iPhone. In 2021, 63 million smartphones sold in the UK of which 7 million were iPhones and iPhone 13, the latest and improved device.

Court convictions are declining over the last few years while Fraud is proliferating suggesting there is a mismatch between the law and crypto crime.

K. Is There Other Existing Remedies?

Yes – Industrial and Government Regulators, e.g., Bank/PSP Regulators:

L. Prosecuting Fraud Cases

Recommend the traditional Court route may not be applicable to the vast majority of Fraud cases given the low level of convictions. Need an approach that is more in line with the growing cyber/digital environment and quick timeframes

M. Sanctions and Penalties

Recommend an effective deterrent given the move from burglary to increasing online assault on the Bank Account market – 70 million accounts.

4. Best Practise

N. Lessons learnt

Telephone companies are stopping fake Sim Cards being used by fraudsters to bypass phone verification and authorisation. The telephone companies and FinTech services are also highlighting 'spoofed' legitimate numbers, numbers that forward the call and where the call is being made geographically. Many of the telephone numbers when called back are not in use and with a pre-recorded message such as 'this number is not in service'.

Many mobile phones allow the blocking/barring of nuisance calls.

Text message scams – fees for parcel delivery, HMRC, VAT, NHS – are starting to be stopped at source. One issue is when asked to 'STOP' text, don't as replying let's the fraudster knows this text is live.

e-mail scams are becoming more sophisticated as spam e-mails have been with us since the early days. Now emails are linked to web sites that look almost like the real thing and minor changes in the return email addresses. Here some of the web site platforms are monitoring the legitimacy along side regulators. For

example, The Advertising Standards Authority in March told 50 cryptocurrencies web sites to review their ads by May 2022.

UK banks and some platforms, for example, Google, do restrict the access to these crypto/digital currencies because of their wide fluctuations in value, chances many are fake, for examples, OneCoin, vulnerable asset storage, e.g. Mt. Gox and the exchanges could be under funding making them a risk in their own right.

In the UK, Cryptocurrencies are held by 2.3 million people [Financial Conduct Authority (FCA)], and along side investment scams, people under 45 are now accountable for 70% of reported frauds.

HMRC is using Confirmation of Payment (CoP). This trend started in The Netherlands as corporates themselves have more to lose in fraud than the average individual (UK Finance shows individuals lost £3,400 against £100,000 for businesses).

The key is early intervention before the scam gathers momentum.

O. One Policy Recommendation

The establishment of a national curricular for the teaching of cyber/digital security for people aged 5 through to 100 that allow everyone to be at least be aware of online fraud to certified qualifications for employment. Employee remuneration is to start at £25,000/year and advancing to £100,000+/year.

As cyber/digital security is in its infancy, teachers need to be trained; curricular created, qualifications from novice to expert agreed (e.g. City of Guilds) and short-term sprint semesters (12 week) starting in 2022.

As all major changes in society – the UK move to decimalisation in 1971 and the Millennium bug in 2000 – needed Government support. The UK and World are moving to a full on cyber/digital world. Everyone needs to be at least aware of what is happening and the opportunities that can be used anywhere.

The UK with cyber/digital security program supported nationally can almost immediately lead the world in this new digital era. Similar to the introduction of the first steam locomotive, UK went on to build railways everywhere for years.

The UK can lead the world in cyber/digital security with the whole country behind it

22 April 2022