Chris Hemsley
Payment Systems Regulator (PSR)
12 Endeavour Square
London E20 1JN
January 10th 2020

On Demand Payment Technologies Ltd (ODPT) response to the Payment Systems Regulator (PSR) CP/10

Dear Chris and the APP Scam Team,

CP/10 is a well thought-out approach with options on how to deal with the on going acceleration of Authorised Push Payments **(APP)** scams against bank account holding customers. It is natural for people to trust banks to look after their money. However scammers themselves require bank accounts to conduct APP scams and regardless how unintentional, scammers are adapt at obtaining bank accounts for themselves.

In the previous implemented policies, PSR focused on mandating 6 bank/PSPs with the largest payment volume (covering 80% of the market) on using Confirmation of Payee **(CoP)**. This worked well but the fraudsters' reaction was to use the non-CoP bank/PSP for their bank accounts. The risk of being APP scammed from non-CoP is now much higher than from a CoP bank/PSP as CoPs must pay Non-CoPs, the payee, for the overall payment system to function. The suggested move to mandate 95% of the bank/PSP to use CoP, while welcomed, would further increase fraud risk for the remaining 5%; namely smaller bank/PSPs.

ODPT recommends PSR to mandate 100% of the market to Direct Connector (DC) bank/PSPs in the Faster Payment Scheme (FPS) to ensure the whole market is safer from APP scams. The 5% of FPS payments is worth £125 billion a year.

There are 37 DC's in the FPS. The rest of the financial services industry uses a DC as agent to make an instant payment, for example in the UK, PayPal using Barclays. The DC would need to ensure their clients follow the regulated rules for CoP and any other mandates by PSR.

ODPT recommends PRS to support and require intelligence sharing as key priorities.
APP scammers are dedicated criminals aimed at stealing people's money instantly from peoples' bank account. The money is then moved to their bank account(s) to hold or to spend. To open up a bank account, all consumers are required to prove who they are and where they live. Consumer transactions on their bank account(s) are recorded and stored for up to 7 years by bank/PSP. The data on APP scams is therefore held by each bank/PSP. By pooling this data PSR and the banks/PSP will have a greater overview of how past APP scams are conducted and the potential track and trace individual or groups of APP scammers.

The UK GDPR and Data Protection Act 2018 already permit parties sharing data with law enforcement agencies for the prevention and detection of crime. What is needed is PSR to take an active role in establishing an Investigation Centre. This will provide banks/PSPs a centralised investigation hub through which each bank/PSP fraud investigator or compliance team can access information about past APP scams and known scammers.

The above will help push banks/PSPs going forward to actively share details on APP scams and/or scammers with each other and the law enforcement. Equally, law enforcement and The Police Foundation need to become a much more active in investigating and prosecuting scammers.

Naturally the pre-scam activities – fake emails, telephone calls, texts, email and ads – also need to be addressed to prevent the consumer from being lured into parting with their money. These pre-scam activities are becoming more sophisticated.

ODPT welcomes the proposed move from a voluntary Reimbursement Model (CRM-Code) of practise to regulatory action.

One of the biggest issues is the inconsistency of banks towards their customers in terms of reimbursement and, more importantly, blame. The level reimbursement, by individual bank, ranges wildly with a group average of 40% of victims being reimbursed. Implicitly the current practice suggests customers are to be blamed for the fraud.

Most people are reluctant to report being scammed fearing loss of self-esteem and other negative emotions. Many in the media believe the reported APP scams are significantly lower than the actual APP scams taking place.

A table of actions by fraud range modelled on UK Finance analysis is an exemplar model. Banks often have a level in which fraud investigations are uneconomical. As the average fraud loss by consumers is £3,400 this amount is often charged off to the client to sort.

- **The current CRM-Code leaves people at the discretion of their own bank/PSP**

The PSR proposal will provide customers with how their PSP is preventing fraud. This in turn will instil PSPs to treat customers with greater empathy and provide a more consistent fraud reimbursement scheme. By PSR mandating how each bank/PSP is performing on their web sites is a great incentive and provides comparative data for the market to understand and compare bank/PSPs.

The PSR has a great opportunity to guide the consumer into a safer environment by tackling the issues around CoP, sharing of intelligence and rebooting the CRM-Model. Only through mandates will the community see an improvement in the reduction of APP scams. Without such actions even a 25% per year increase would mean APP scam in

2023 could be £2 billion with over 500,000 individuals distressed. The actual payment process with the new proposals has the transformative power to make bank account activities much safer and a more global model.

Looking forward to PSR's success and to seeing APP fraud reduced in 2022.

Kind regards

John Bertrand **Douglas Cosbert**

Directors

On Demand Payment Technologies (https://od-pt.com)

N.B. Details, comments on the 18 questions and Appendix are attached

Details

Increasing the group being mandated for Confirmation of Payment (CoP)

The proposed larger group by the PSR is a welcome addition. The issue for the instant payment system to work is all banks must make payments to banks whether or not the whole group is 100% compliant.

The move to legislation is essential to improve the "laissez faire" PSP environment. The initial mandating of CoP (SD10) resulted in fraudsters moving their bank accounts to non-COP banks. The SD10 had 85% of payments and fraud has moved to the 15% of payments not involved. The fraud of that 15% is now 40 per cent for all payments, trebling APP fraud risk for the smaller Bank/PSPs.

Moving to larger group of Bank/PSP to 14 in the UK covering 95 per cent of payments will further accelerate fraudsters move to Bank/PSP to the remaining 5 per cent. That 5 per cent covers £125 billion payments and is growing year to year. At the current growth rate, within 3 years, this will be £250 billion a year.

- ***Fraudsters have an ideal market, as, fully compliant banks have to send money to banks that "lack fraud prevention capabilities"***

To make the whole market 100% compliant, all directly connected participants (DC) of the Faster Payments scheme, currently 37 Bank/PSPs, need to be compliant. The rest of the banking community who use a DC Bank/PSP as agent would be compliant as well as to the regulator through the agent. Faster Payments by both Bank/PSP being a DC or using an Agent DC are now under the same rules.

Support and require intelligence sharing

The biggest missing link is payee bank account information; which is the receiving of (payee) bank's account activities. The payer bank, if doing CoP checks, simply identifies the Account Name, Sort Code and Account Number of the payee bank account. Scammers have a known behaviour pattern such as new sources of payments that are immediately transferred to another bank account and then, often to a third.

- ***A scorecard that included the Bank/PSP receiving APP scam payments, comparison within to the group would be welcome. Fraudsters are trending to use non-CoP bank accounts. This intelligent sharing needs to be visible at the Bank/PSP Board level.***

Extra intelligence **– the scammers and their details are known by the bank/PSP**

Banks keep records on account bank opening details and the transactions usually for at least 7 years. Each bank that has received stolen money, knows where it came from, and

the accounts into which the money was transferred. The issue is historic as banks loathed to admit they had been scammed.

- ***What is needed is an investigation centre that shows the names, addresses and money movements of the scammers involved. This list, like anti money laundering processes, can become a known scammer alert and added to the Know Your Customer procedures when opening a bank account.***
- ***Bank investigators can use this list to identify 'at risk' bank accounts in the scammers names and locations in customer bases***

Making reimbursement mandatory for scam victims
The proposed move from a voluntary Reimbursement Model (CRM-Code) to regulatory action at the earliest opportunity would solve many issues.

One is the inconsistency of banks towards their customers in terms of reimbursement and more importantly who is to blame. Implicitly the majority of customers (60%) are blamed for the fraud as only 40 per cent being reimbursed.

In terms of reimbursement, a good model is the UK Finance on Year 1 CMR-Code results. Suggest adding a fourth amount size band of £50.000 + as this is where life-altering events for consumers are likely to happen.

		Comments
Band 1	Less than £1,000	Instant refunds and similar policies as credit cards Debit and credit cards are seen by consumers as the same
Band 2	£1,000 to £10,000	30 days for a yes/no decision
Band 3	£10,000 to £50,000	Investigations are commercially viable and the client kept informed on progress
Band 4	Above £50,000	Commercially viable and often, for consumers, life changing and so extra sensitive customer service

Average consumer fraud	£ 3,400 - Consumer banking represents 95% fraud
Average corporate fraud	£95,000 - firms +£4 million turnover in Corporate Bank

- ***A clear, simple to understand APP fraud reimbursement experienced and what to expect from the bank/PSP within each category***

Comments on Questions

1. Proposed data metrics
    a. Metric A, B and C look fine with C of growing importance.
        i. Option C is the missing information link: Payee Account
        ii. By expanding information on individual Bank/PSPs receiving scam payments from directed Bank/PSPs and measured individuals vs. group performance is a clearer picture on individual performance

2. Scope of Payments in Measure 1
    a. Would like to see the Bank/PSPs involved as far reaching as possible.
        - ***Suggest any Direct Connectors to FPS be in scope***

3. Scam Bands
    a. Suggest using UK Finance CRM-Code as a format with the addition of a £50,000 + band to show the life threating scams

4. Draft Direction at Annex 3
    a. Fine with suggestions:
        i. Scope should include more banks outside the top 14, ideally all.
        ii. Faster Payments has 37 Direct Connections and they, in turn, offer Faster Payments to over 100 bank/PSPs. The issue: fraudsters using smaller Bank/PSP not fully covered against scams
        iii. Publication timeframes should become faster as the new reporting process becomes established: e.g. year 2 quarterly and then monthly by year 3

5. PSP reporting Measure 1
    a. Given 5 per cent of the faster payments is worth £125 billion per year suggest a re-look at the scope criteria, including Bank/PSPs with consumer bank accounts

6. Timing of Reporting Systems
    a. The issue here is the amount of outstanding system work is needed at each Bank/PSP. By mandating them, the work will be prioritised and completed. Given today's cloud technology, APIs linking into existing systems and standard formats, estimate up to 6 months
        i. Encourage banks to use third parties, even temporary, to bring the reporting required implemented within 3 months

7. Voluntary reporting
    a. Fine to allow voluntary reporting

8. Comparing PSP at Group Level
    a. Comparison at Group Level increases the fight against APP fraud

9. Receiving PSP included in Metric C
    a. Suggest using data scientists to design the table for best/worst and declining/improving for group comparisons

10. Information about receiving PSPs
    a. **Yes, yes and yes** – information on receiving Bank/PSPs knowledge of the customer's payments/banking history is vital to prevent fraud

11. PSP and data on websites
    a. Agree with publishing PSR data predominately on bank/PSP web sites as this will eradicate any opaqueness around preventing scams

12. Reporting periods
    a. OK to start then speed up as fraudsters are working in real time, so monthly should be the goal – similar to Faster Payments

13. Reporting to the PSR
    a. OK to start and then establishing more faster timetables

14. Data quality assurance
    a. Very sound

15. Trialling Measure 1
    a. Good

16. CBA for Measure 1
    a. Fine

17. Improving Intelligence
    a. Well done in identifying how to improve intelligence against fraud. Long over due and will be needed even more in the future as scammers use ever increasing technology capabilities

18. CRM Code under Measure 3
    a. Prefer Option 3B as the voluntary approach to preventing scams has been tried. Scammers are now a billion pound fraudulent business

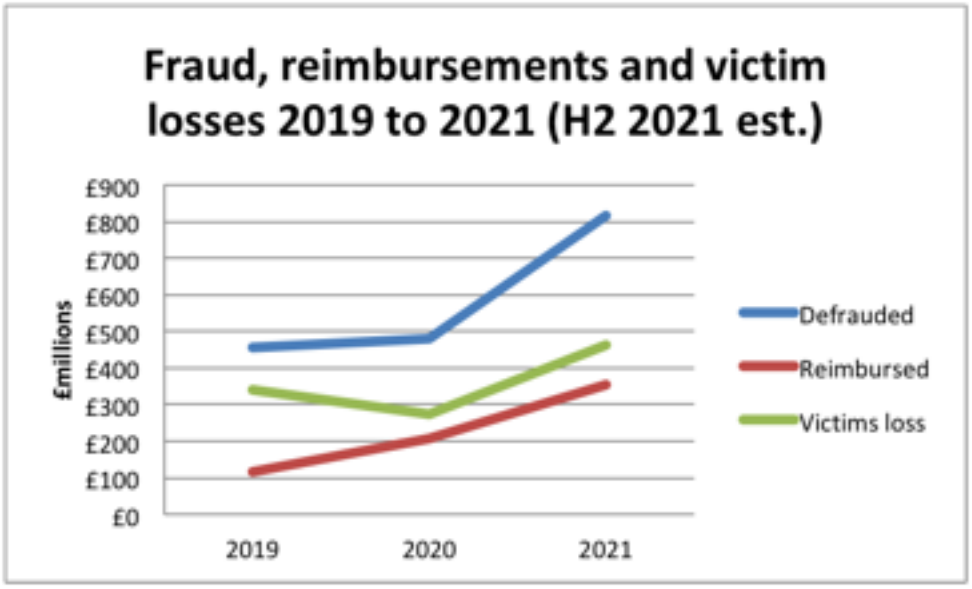
    b. Look at the roles of four parties – Pay.UK, LSB, Financial Ombudsman and the PSR – to see improvements can be made for faster improvements

Appendix

Size of the instant payment market

Over the last two years faster payments value has grown to £2.5 trillion (up 30%) and volume to 3.3 billion messages (up 40%). The average payment is £760.

APP fraud over a similar period increased to an estimated £820 million in 2021 from £460 million in 2019. Reimbursements, since the introduction of the CMR Code, have doubled but customers still lose 60% to the scammers.



Reasons for the increase

Scammers are using the latest in technology and psychology techniques to focus on taking money out of a bank account by moving the victim's money to their own bank account electronically. Information on the payee bank account is critical.

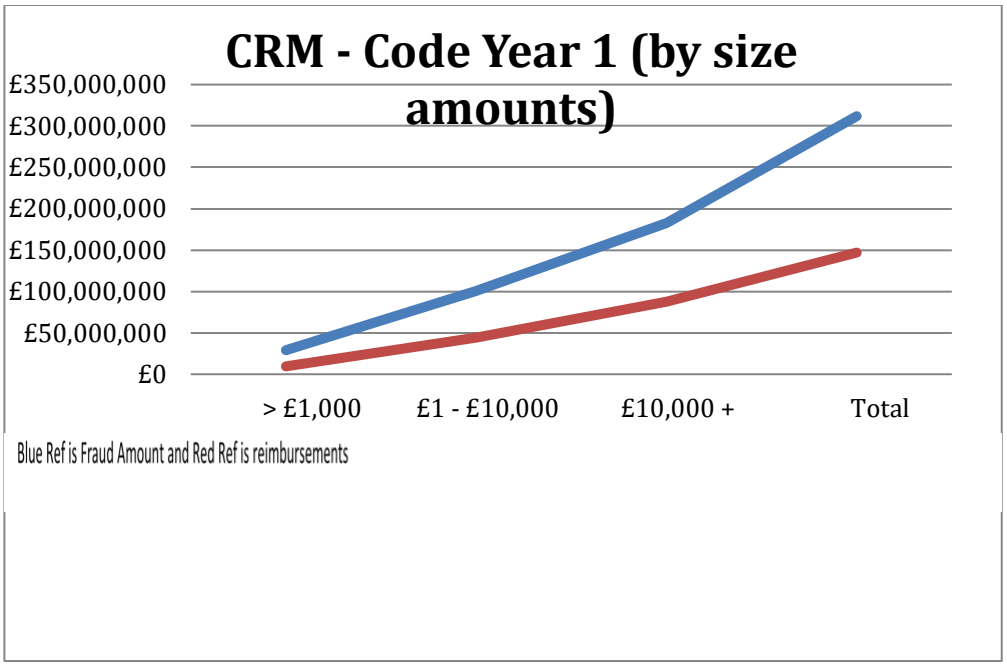
Making reimbursement mandatory for scam victims

The CMR Code since May 2019 has seen a doubling of reimbursement to 40% of the victims scam loses. The six largest banks have been spearheading the voluntary CMR Code and they are mandated to provide CoP. The rest of the financial community, at least 100 institutions, can open bank accounts and offer faster payments to any customers. It is this group, the smaller banks with the least fraud prevention measures – no CoP, no directive on reimbursements – that are ideal for the fraudsters.

Average consumer fraud	£ 3,400 - Consumer banking represents 95% fraud
Average corporate fraud	£95,000 - firms +£4 million turnover in Corporate Bank

- ***Information on the Payee Bank is not disclosed to the Payer Bank***

UK Finance reimbursement results graph:



Average reimbursement	**> £1,000**	**£1 - £10,000**	**£10,000 +**	**Total**
Value	£29,000,000	£100,200,000	£182,600,000	£311,800,000
Reimbursed	£9,500,000	£44,000,000	£87,300,000	£147,000,000

Volume	**>£1,000**	**£1 - £10,000**	**£10,000 plus**	**Total**
Cases	102,645	30,505	5,954	139,304
Payments	128,606	64,836	21,834	215,285

Forecasts

The graph shows actual figures from UK Finance from 2019 through H1 2020. A forecast has been made using an increase of 25% for actual fraud scams and 21% for actual reimbursements. Reimbursements have doubled from 20% to 40% in the first year under the voluntary CRM-Code. Without mandatory activity the increase is forecasted to be 21% to reflect management of the figures in the bank/PSP to be in line with each other and as low as possible. Much of the reimbursement originates from the operation budget and not the line of business. Operational costs are supervised closely often by non-facing customer personal.

	Actual 2019	**Actual 2020**	**HI A H2 F 2021**	**Forecast 2022**	**Forecast 2023**
Fraudsters gain	£455.8	£479.0	£806.5	£1,300.9	£2,098.1
Banks loss	£116.0	£206.8	£333.4	£490.1	£720.3
Victims loss	£340	£272	£473	£811	£1,378

	Actual 2019	Actual 2020	HI A H2 F 2021	Forecast 2022	Forecast 2023
Cases	122,437	149,946	238,869	373,233	583,176
Cumulative		272,383	388,815	612,102	956,409
Av/case	£3,723	£3,194	£3,376	£3,485	£3,598