Presentation for the

APPG on Personal Banking and Fairer Financial Services

Symposium on 25th January 2021

Potential Solutions to the challenge of Authorised Push Payment Fraud

by

Richard Emery - 4Keys International

for

Transparency Task Force Ltd

4KEYS INTERNATIONAL

30 Farley Copse, BRACKNELL, Berkshire, RG42 1PF, UK

Tel: 01344 484 235 Richard@4Keys.co.uk

Mbl: 0777 165 6638 www.4Keys.co.uk

Contents

~ ~

Table of Abbreviations

The following abbreviations are used in this presentation:

APPG	All Party Parliamentary Group
APPF	Authorised Push Payment Fraud (see para: 2.2)
APPScam	Authorised Push Payment Scam (see para: 2.2)
CoP	Confirmation of Payee
CRM	Contingent Reimbursement Model (CRM Code of Practice)
FCA	Financial Conduct Authority
FOS	Financial Ombudsman Service
FPS	Faster Payment System
LSB	Lending Standard Board
NPO	Norwich Pharmacal Order (see para: 7.5)
PSP	Payment Service Provider (a Bank / referred to as a 'Firm' in CRM)
PSR	Payment Systems Regulator
PSR2017	Payment Services Regulations 2017
(D)SAR	(Data) Subject Access Request
	(*A 'SAR' is a Suspicious Activity Report*)
TTF	Transparency Task Force

1 INTRODUCTION

1.1 About the Transparency Task Force (TTF)

1.1.1 TTF's mission is to promote ongoing reform of the financial sector, so that it serves society better. Our vision is to build a large, influential and highly respected international institution that helps to ensure consumers are treated fairly by the financial sector. The primary beneficiaries of our work will be consumers; but the sector itself will also benefit through improved market conduct and increased trust in the services it provides.

1.1.2 Much of our focus is on rebuilding trustworthiness and confidence in financial services through a framework for finance reform which we describe as a "whole system solution for a whole-system problem". (http://www.transparencytaskforce.org)

1.2 About the Author

1.2.1 Richard Emery is an Independent Forensic Fraud Investigator, with an extensive background serving as an Expert Witness in both Civil and Criminal matters covering Retail Theft & Fraud, Credit/Debit Card Fraud and On-line Bank Fraud. He now focuses on assisting individuals, small businesses and charities (hereinafter: individuals) who have been the victims of bank fraud to challenge the banks and take complaints to the Financial Ombudsman Service. (https://www.4keys.co.uk)

1.2.2 He also challenges the Regulators and FOS on their approach to the various Regulations and Codes of Practice.

1.2.3 He is an Ambassador for TTF, supporting their work with the APPG on Personal Banking and Fairer Financial Services as a member of its Secretariat Committee.

1.3 About this presentation

1.3.1 This presentation focusses on five primary topics:

- What is APPF?
- CRM Code of Practice
- Confirmation of Payee
- Historic Reimbursement
- Delaying Faster Payments

1.3.2 It also introduces a number of other topics that the APPG may wish to consider.

- Bank Identification
- Account Opening
- Active Account Monitoring
- Disclosure of Beneficiary Details
- Complaints About Beneficiary Banks
- Repatriation of Stolen Money
- Regional Economic Crime Teams

2 INTRODUCTION TO APPF

2.1 What is APPF?

2.1.1 When the bank's customer (aka: the Payer):

- Is deceived into authorising a payment to the wrong person, or
- They pay the intended Payee, but that person turns out to be a fraudster or scammer.

2.2 A Fraud or a Scam?

2.2.1 Some banks seek to differentiate between 'a fraud' and 'a scam'. Two sides of the same coin:

- The 'scam' can be seen as the presentation of false information to draw in the victim
- The 'fraud' can be seen as the misappropriation of the money when the payment is authorised.

2.3 The Scale of APPF

2.3.1 The figures that have been reported by UK Finance for APP Fraud show that it has almost doubled between 2017 and 2019. There are no published figures before 2017.

- 2017 £236m
- 2018 £354m
- 2019 £455m

2.4 The Impact of APPF

- There were an estimated 300,000 cases in the six years 2014-19
- The total value of their losses was c.£1.3bn
- The average loss over £4,000
- Applying the Pareto (80/20) principle
- The top 45,000 cases (i.e.15%) had losses averaging c.£22,000
- The cases on my desk average over £50,000

2.5 Types of APPF

2.5.1 UK Finance categorise APPF into eight 'scam types':

- Purchase Scams
- Investment
- Romance
- Advance Fee
- Invoice
- CEO
- Impersonation - Police/Bank
- Impersonation - Other

3 CONTINGENT REIMBURSEMENT MODEL CODE OF PRACTICE

3.1 What is CRM?

A voluntary Code of Practice developed by the PSR and the banks

Sending bank / receiving bank / customer

- Increased protections against APPF
- Full reimbursement for victims - conditional
- Introduced on 28th May 2019

Barclays, HSBC, Lloyds, Metro, NatWest/RBS, Nationwide, Santander and Starling. Co-operative Bank (Dec 2019).

3.2 Disappointing Performance

Low levels of reimbursement

- First 7 months - possibly due to issues of education and/or understanding?
- January-June 2020 - only 37.5% by value

3.3 Limited Transparency

PSR Conference in March 2020

- Reimbursement by cases and by value
- 2 out of 8 banks declined 96% of cases
- 2 out of 8 banks declined 94% and 87% by value

But which banks are they?

3.4 Why No Reimbursement?

The banks are not disclosing their reasons for not reimbursing victims of APPF

"You didn't conduct sufficient checks before making the payment"

- Customer behavior will not be changed
- Frauds will not be prevented
- Banks cannot be held to account

3.5 'Effective Warnings'

An 'Effective Warning' should result in an 'Appropriate Action'

- They should be based on the scam risk of the specific payment type
- They should create a clear understanding of the consequences of the action
- "Understandable, Clear, Impactful, Timely and Specific"
- In every situation of contact with the customer, not just online.

Banks are not disclosing the exact wording or the circumstances

3.6 "A reasonable basis for believing that:"

- Paying the person they expected to pay
- Genuine goods or services, and/or
- Person or business was legitimate

FOS update to PSR conference in March 2020: "Some firms are inappropriately declining reimbursement on the basis that the consumer did not have a reasonable basis for believing the transaction or recipient was genuine".

3.7 Alignment with FOS limits

Unhelpful difference between CRM and FOS limits

- The CRM limit is a "Micro-enterprise"
- The FOS limit is a "Small Business"

CRM reference is to a European Directive from 6th May 2003

3.8 Reimbursement Process

- The CRM Code is unclear - "receive 100%" or "advance 100%"
- What happens when one of the banks is a "Non-code firm"?
- Who pays in 'no-blame' scenarios?
- The actual reimbursement process is inconsistent

3.9 POTENTIAL SOLUTIONS

- Mandatory - all PSPs
- Update and clarify the CRM Code
- Review 'Effective Warnings'
- Review 'Reasonable Basis'
- Align limits to a UK standard
- Clear reimbursement process

3.10 POTENTIAL ACTIONS - GENERAL

- Work towards making CRM mandatory (by end 2021?)
- Full transparency of statistics for every PSP
- Seek improved compliance with the CRM Code

3.11 POTENTIAL ACTIONS WITH LSB

- Support CRM Code update
- Review (and standardise?) Effective Warnings
- Clarify 'Reasonable Basis' criteria
- Resolve funding of 'no-blame' cases
- Update limits for Small Businesses

4 CONFIRMATION OF PAYEE (COP)

4.1 What is CoP?

Allows the Payer to confirm the actual name on the Payee account:

- Payment to someone like a builder for genuine work done
- Solicitor's email for house purchase intercepted and replaced
- An investment for a genuine company goes to a fraudster's account
- A person told by their bank to move their money to a new 'safe' account

4.2 How Does It Work?

New Payee is setup, or first payment is being made

- Only if Payer's and Payee's bank have CoP
- Response with one of three messages (or service not available)
- Perfect Match
- Close Match
- NO Match - "a clear negative CoP result"

4.3 Why Hasn't It Worked?

- Not 100% coverage
- Inadequate customer education
- Delayed implementation was conditional
- Ineffective and inconsistent messages
- Lack of visual impact - 'press here'
- No facility for 'Known As'
- The role of PSR and Pay.UK

4.4 POTENTIAL SOLUTIONS

- Mandatory - all PSPs - all beneficiaries
- PSR to prescribe words and visual impact
- Additional confirmation warning
- Add 'Known As'
- Effective customer education program

4.5 POTENTIAL ACTIONS

- Work towards 100% of PSPs (by end 2021?)
- Work towards consistent messaging
- Review reimbursement if CoP not available
- Transparent enquiry into delayed implementation compliance
- Full transparency of statistics for every PSP

5 HISTORIC REIMBURSEMENT SCHEME (HRS)

5.1 The Need for Historic Reimbursement

UK Finance record APPF losses of:

- 2017 £236m
- 2018 £354m
- 2019 £455m

Estimated losses for 2014-2019 is £1.3bn.

Top 45,000 victims (15%) lost £1.0bn (77%) an average of over £22,000

5.2 What About CRM?

The banks and PSR were very clear that CRM was about the future, not the past.

But the banks' past failures must not be swept under the carpet.

5.3 Response to Treasury Committee Report 2019

SILENCE!

The Government, the PSR, the FCA and Pay.UK all made no comment.

5.4 Banks and Regulators Knew The Risk

- 2008 - Faster Payment System - no names
- Unverifiable sort codes and account numbers
- 2012/13 - Tidal Energy Ltd v Bank of Scotland

- 2014 - Was "obvious risk" discussed?

5.5 Grossly Negligent

- Red Sea Tankers Ltd v Papachristidis (The "Ardent")
- Winnetka Trading Corp v Julius Baer International Ltd & Anor

- Gross Negligence ….. indifference to an obvious risk

5.6 POTENTIAL SOLUTIONS

- PSR to mandate that the banks must do this

5.7 POTENTIAL ACTIONS

- Ask the banks why they have not done this
- Publish the banks' reasons for not doing it

6 DELAYING FASTER PAYMENTS

6.1 Why Delay Faster Payments?

- 'Instant' payments are very useful
  but
- Faster payments = faster fraud

Particular risk for certain types of APPF (and unauthorised transactions).

6.2 What Is Proposed?

To delay the first high value payment until 24 hours after a new Payee is created.

- High value? £500 / £1,000? User choice?
- Opt-in or opt-out?
- Planned over-ride - 72 hours notice
- Emergency over-ride - secure verification

6.3 Why 24 hours?

- Allows the customer time to think
- Allows the bank time to check

6.4 "Not allowed under the Regulations"

- Nobody has shown that it is not allowed
- PSR 2017 and FPS rules imply 'end of next day'
- It is a Customer Instruction

6.5 "It will be inconvenient"

When was the last time that you made a payment of more than £500 to someone you had never paid before and did not have their payment details at least 24 hours before they needed the payment?

6.6 POTENTIAL SOLUTIONS

- Review the value of doing it since CoP
- Make it available as a customer option
- Promote the benefits

6.7 POTENTIAL ACTIONS

- Ask the banks why they have not done this
- Publish the banks' reasons for not doing it

7 OTHER TOPICS

There are a number of other matters that I believe would either reduce the risk of APPF or benefit victims in recovering from such fraud. These are outlined below.

7.1 Bank Identification

- Why it is that I have to prove who I am, but the bank makes no effort to prove who they are?
- Impersonation of the police or the bank is serious
- 23% (by value) of personal APPF in 2019
- Amongst the most emotionally stressful

7.2 Account Opening

- CRM Code: "Firms must take reasonable steps to prevent accounts being opened for criminal purposes."
- Companies House: 221,020 new incorporations in July-Sept 2020 (+30.2%)

7.3 Active Account Monitoring

- Monitor against individual 'Account Profiles'
- Inbound as well as Outbound
- Freeze individual transactions

7.4 Disclosure of Beneficiary Account Details

- PSR 2017 regulation 90(4) "….. provide to the payer all available relevant information in order for the payer to claim repayment of the funds."
- Paragraphs 5(3)(a-c) of Part 1 of Schedule 2 of the DPA 2018 … "is necessary for the purpose of, or in connection with, legal proceedings ….."

- FCA, PSR, ICO and FOS

7.5 Norwich Pharmacal Order (NPO).

- Forces the bank to disclose information
- An NPO can cost as much as £5,000
- The banks resist them because of what they might show

7.6 Complaints About Beneficiary Banks

The scope of the FOS needs to be extended to allow them greater rights of investigation into the receiving bank.

7.7 Repatriation of Stolen Money

- Money 'frozen' by the receiving bank can be returned
- The process can be infuriatingly slow
- The process is unclear

7.8 Regional Economic Crime Teams (1)

City of London Police DCPCU - great success

- 20/21 budget capped £2.66m
- Estimated savings in 2018 of £94.5m
- Savings from reduced fraud activity of £600m since 2002

7.9 Regional Economic Crime Teams (2)

Regional Police forces

- Need skilled, dedicated Officers
- Supported by civilian staff
- Funded by the banks

8 APPENDIX A - THE BANKS HAVE BEEN GROSSLY NEGLIGENT

8.1.1 Figures published by UK Finance record APPF losses of £455.8m (i.e. £1.25m/day) in 2019. The headline figures for 2018 and 2017 were £354m and £236m. It is, in my view, reasonable to extrapolate that the total value of APPF losses between 1st January 2014 and 31st December 2019 is in the order of £1.3bn. A modest sum when we consider the financial impact of C-19, but a very significant sum for the individuals who have lost life-changing sums of money.

8.1.2 The question that I am asking is: Have the banks done all that they reasonably could have done to prevent, or at least mitigate, these losses; or have they been 'Grossly Negligent'?

8.2 The Risks of Faster Payment System (FPS) and CHAPS

8.2.1 Prior to the introduction of FPS we used cheques, and cheques relied on the Payee name.

8.2.2 When FPS was launched on 27 May 2008 it was based on the use of the Sort Code and Account Number (the Unique Identifier) to route the payment to the Payee's account. FPS made no reference to, or use of, the Account Name that the Payer had used to identify the intended Payee.

8.2.3 CHAPS, which is designed for making high value payments, requires the Customer to provide a correct name for the intended recipient of the payment that matches the Account Name associated with the Unique Identifier (i.e. the Sort Code and Account Number), but the system does not validate it.

8.2.4 In my view a thorough and detailed analysis of the risks associated with the introduction of '*instant payments based solely on an unverifiable sort code and account number*' should have resulted in the development of appropriate security protocols. There were obvious risks.

8.2.5 Even if those risks were not properly identified at the time, then they should have been identified and responded to as they became increasingly obvious in the following years.

8.3 Tidal Energy Ltd v Bank of Scotland

8.3.1 Even if the risk of fraud from the use of unverifiable sort codes and account numbers was not obvious in 2008, it became obvious in 2012 and 2013 with the case of Tidal Energy Ltd v Bank of Scotland (EWHC 2780). In January 2012 Tidal Energy attempted to make a payment of £217,781 but it went to the 'wrong' account. The court ruled that Bank of Scotland did not have to reimburse Tidal Energy because it was not banking practice to check the Payee name.

8.3.2 The fact that it was not banking practice at that time to check the Payee name does not, in my view, mean that the banks could remain indifferent to what was now an obvious risk.

8.4 Camerata Property Inc v Credit Suisse Securities (Europe)

8.4.1 In this case, together with those of Red Sea Tankers Ltd v Papachristidis (The "Ardent") and Winnetka Trading Corp v Julius Baer International Ltd & Anor, one of the issues that the judges had to consider was that of potential 'Gross Negligence'.

8.4.2 The specific point that I focus on is the statement made by Mance J that: "the concept of Gross Negligence seems to me capable of embracing ….. indifference to an obvious risk".

8.5 The Banks have been Grossly Negligent

8.5.1 Based on the principal that "indifference to an obvious risk" may constitute Gross Negligence, and that the Banks have been aware of the risk since at least 2013, they must, in my view, have been Grossly Negligent since the start of 2014, in that they have, amongst other things, failed to develop and deliver systems to allow Account Holders to confirm the account name on the Payee's account.

9 APPENDIX B - TYPES AND VALUES OF APPF

9.1 UK Finance :: Fraud - The Facts 2020

9.1.1 The following information is taken from UK Finance "Fraud - The Facts 2020". The figures are for 2019 and are divided into "personal" and "non personal". The "% inc" is the increase since 2018:

	Personal		Non-Personal		Total	
	2019	% Inc	2019	% Inc	Total	% Inc
Volume	114,731	47%	7,706	20%	122,437	45%
Value	£ 317.1m	39%	£ 138.7m	10%	£ 455.8m	29%
Average	£2,763.86		£17,998.96		£3,722.73	

9.1.2 The values below each description are for 'personal' cases and show:

- The Number of Cases and the Percentage of all Cases
- The Value (in £m) and the Percentage of the Total Value of all Cases
- The Average Loss of each Case

9.2 Purchase Scams

9.2.1 In a purchase scam, the victim pays in advance for goods or services that are never received. These scams usually involve the victim using an online platform such as an auction website or social media. Common scams include a criminal posing as the seller of a car or a technology product, such as a phone or computer, which they advertise at a low price to attract buyers.

Cases 71,574 62% Value £51.1m 16% Aveg Loss £714

9.3 Investment

9.3.1 In an investment scam, a criminal convinces their victim to move their money to a fictitious fund or to pay for a fake investment. The criminal will usually promise a high return in order to entice their victim into making the transfer. These scams include investment in items such as gold, property, carbon credits, cryptocurrencies, land banks and wine.

Cases 6,679 6% Value £89.5m 28% Aveg Loss £13,400

9.4 Romance

9.4.1 In a romance scam, the victim is persuaded to make a payment to a person they have met, often online through social media or dating websites, and with whom they believe they are in a relationship. Once they have established their victim's trust, the criminal will then claim to be experiencing a problem, such as an issue with a visa, health issues or flight tickets and ask for money to help.

Cases 2,137 2% Value £18.0m 6% Aveg Loss £8,423

9.5 Advanced Fee

9.5.1 In an advance fee scam, a criminal convinces their victim to pay a fee which they claim would result in the release of a much larger payment or high value goods. These scams include claims from the criminals that the victim has won an overseas lottery, that gold or jewellery is being held at customs or that an inheritance is due. The fraudster tells the victims that a fee must be paid to release the funds or goods. However, when the payment is made, the promised goods or money never materialises.

Cases	10,508	9%	Value	£16.0m	5%	Aveg Loss	£1,523

9.6 Invoice

9.6.1 In an invoice or mandate scam, the victim attempts to pay an invoice to a legitimate payee, but the criminal intervenes to convince the victim to redirect the payment to an account they control. It includes criminals targeting consumers posing as conveyancing solicitors, builders and other tradespeople, or targeting businesses posing as a supplier, and claiming that the bank account details have changed. This type of fraud often involves the criminal either intercepting emails or compromising an email account.

Cases	4,732	4%	Value	£31.7m	10%	Aveg Loss	£6,699

9.7 CEO

9.7.1 CEO fraud is where the scammer manages to impersonate the CEO or other high ranking official of the victim's organisation to convince the victim to make an urgent payment to the scammer's account. This type of fraud mostly affects businesses.

Cases	80	0%	Value	£1.2m	0%	Aveg Loss	£15,000

9.8 Impersonation - Police/Bank

9.8.1 In this scam, the criminal contacts the victim purporting to be from either the police or the victim's bank and convinces the victim to make a payment to an account they control.

Cases	10,835	9%	Value	£73.5m	23%	Aveg Loss	£6,784

9.9 Impersonation - Other

9.9.1 In this scam, a criminal claims to represent an organisation such as a utility company, communications service provider or government department. Common scams include claims that the victim must settle a fictitious fine, pay overdue tax or return an erroneous refund. Sometimes the criminal requests remote access to the victim's computer as part of the scam, claiming that they need to help 'fix' a problem.

Cases	8,186	7%	Value	£36.2m	11%	Aveg Loss	£4,422