Catastrophic fraud loss lies where it falls? Push payment scams and the bank's duty of care to its customer.

Article Classification: Case study

Purpose: To examine the legal redress available to a UK bank customer who has been the victim of a sophisticated push payment scam which made use of the bank's customer facing payment portal.

Design/Methodology /Approach: A detailed study of the experience of a single UK bank customer in Autumn 2020 who was the victim of a push payment scam. Her circumstances are typical of other customers who have been similarly scammed. Her rights of redress are explored in depth in relation to law and an industry code.

Findings: The industry code provides no reliable means of adjudication and redress. The common law of negligence has not adapted to the technological shift in bank payment methods currently used by customers. The duty of care is inadequate in safeguarding customer interests in relation to payment instructions to banks. Customers are bearing the loss associated with inadequate bank transaction analytics.

Originality/Value: The research casts a unique light on the unbalanced relationship now existing between the bank and its customer in relation to the execution of remote payment instructions**.**

Keywords: Money laundering, Redress, Fraud, Duty of Care, Bank and customer.

Introduction

This article looks at the push payment scam from the point of view of a bank customer and assesses the legal remedies available to compensate her in the UK for loss suffered as a result of this financial crime. Comments are made on the relevance of excellent bank IT systems and controls in preventing push payment scams and money laundering. It argues that the standard of the duty of care and skill of banks in executing payment instructions must now incorporate an assessment of the IT systems provided by the bank to the client to effect remote payment instructions otherwise the duty is rendered worthless. If the bank's transaction monitoring is inadequate, the bank should bear the loss.

Costs saved but wide open to crime.

News articles about push payment scams proliferate and they induce feelings of sympathy and commiseration for the individual victims. In 2020 UK Finance members reported 149,946 incidents of authorised push payment (APP) scams with gross losses of £479 million (UK FInance, 2021) .[OBJ] A customer who uses on line banking has been duped by a convincing telephone fraudster into making large payments into a series of bank accounts under the control of the thief.[OBJ] The victim believes they are acting conscientiously on the advice of the bank to safeguard their funds. Contact has been made and sustained on the phone, ostensibly by the bank itself, and the thief uses careful language, phrases and stories to build up a trusting and friendly relationship. Some hours or days later the customer discovers the theft. As they have organised the payments themselves, using the IT portal provided by

the bank, the victim feels embarrassed, shameful and responsible. She is informed that the bank has made efforts to recover the individual payments, which were numerous, but the efforts have been unsuccessful. The damage has been done and the money lost. The customer is deprived of her life savings, pension lump sum, an inheritance. The proceeds of this crime pass through numerous unidentified bank accounts. Their phone call to the local police is met with advice to refer the matter to the UK's National Fraud and Cybercrime Reporting Centre. This is done but no consequences follow and the indications are that the resources available to this Centre are wholly inadequate to deal with the number of crimes reported to it. (Action Fraud, 2021).

Recouping the loss

A more analytical customer may feel extremely aggrieved. She had entrusted her salary, pension and life's savings to the bank by opening several accounts and been a loyal and diligent customer for many years. The theft was enabled by the bank's own decision to provide access to her current account and savings accounts remotely, through its own portal, and by allowing her direct access to its payment network. She was convinced of the advantages of speed and convenience and the bank has benefited by considerable operating costs savings. Had she continued to bank in the traditional way, her savings would have been secure. Assuming that the bank is trustworthy and technically competent she has acceded to the bank's encouragement to move to online account operation. No phone calls, text messages or e mails were received from the bank querying the long succession of highly atypical lump sum transfers to unrecognised bank accounts. No delays were applied to the transfers whilst enquiries were made by the bank. No warning messages appeared on screen during the course of the transactions. Never before had she transferred £49,490 in sixteen separate transfers within a period of 23 hours and in fact only one transfer of more than three figures has been made in the recent past. One account has had no movement whatsoever in the past 19 months. She has little technical knowledge and entirely trusted the caller masquerading as a bank employee. His phone number matched that appearing on the reverse of the debit card and he was in possession of confidential information which convinced her of his identity.

Statutory obligations on the bank.

The customer may embark on the bank's internal complaints process which it is obliged to have under the terms of its authorisation to operate under the Financial Services and Markets Act 2000 (FCA Handbook DISP 1.3.1R and 1.3.3R). The customer also has the option of contacting the Financial Conduct Authority to notify them that the bank is in breach of its regulatory obligations under the FCA Handbook to maintain IT and account operation systems and controls which effectively combat fraud, financial crime and money laundering. Given that she is a typical customer of that bank in that region of Northern England, she has a good argument that her loss demonstrates the inadequacy of the bank's approach to tackling financial crime, risk management and corporate governance at the highest level in relation to financial crime . Numerous provisions in the FCA Handbook are called into play. PRIN 2.1.2 obliges the bank to conduct its business with skill, care and diligence. PRIN 2.1.3 compels the bank to take reasonable care to organise and control its affairs responsibly and effectively with adequate risk management systems. SYSC expands on these obligations. SYSC 3.2.6A-K mandates the maintenance of business and IT systems which address and control financial crime in the light of its particular client base. SYSC 6.3 requires the firm to establish comprehensive and proportionate systems and controls that enable it to assess, manage and monitor money laundering risk. There is also an obligation to assess

regularly whether these systems are adequate. SYSC 6.3.7 compels appropriate measures being taken to ensure that ML risk is taken into account in day-to-day operations including in relation to taking on new customers, development of new products and changes in its business profile. The firm's money laundering reporting officer must report to the board at least annually on the operation and effectiveness of money laundering control.

She considers the laxity of controls applied to her own bank transfers, which were unprecedented in individual amount, collective amount, destination and frequency and went unchecked, and notes that the bank IT systems in operation in relation to her transfers must in practice be identical to those in place to control money laundering. Part 3 of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (as amended) (the ML Regulations) obligates her bank to carry out customer due diligence measures in relation to any occasional transfer of funds of more than Euros 1,000 (plus additional obligations where a transaction or series of linked transactions exceeds 15,000 Euros.) Customer due diligence obligations in the ML Regulations are onerous and extend to obtaining information on why and how the customer will normally use their bank account including, by implication, the quantum and frequency of typical payment. Regulation 19 obligates her bank to maintain detailed records relating to any unusual pattern of transactions and to ensure that when any new delivery mechanism or new technology is adopted (for instance for providing customers with direct remote access to payment systems) appropriate measures are taken to mitigate the associated money laundering risk. Regulation 28 obliges the bank to assess and, where relevant, obtain information on, the nature and purpose of the business relationship and occasional transactions. The obvious purpose here is control access to payment networks by establishing IT (or manual) controls which ensure that transactions which are unusual for that customer are subject to exception reporting, delay and scrutiny so that financial crime can be stopped in its tracks. Regulation 33 obligates more onerous due diligence measures where there is an unusual pattern of transactions or where the transaction is unusually large.

When the money has left our customer's account as a result of the fraudster's activity it becomes the proceeds of crime in the hands of each individual payee bank. A predicate offence (theft) has been committed and the suite of obligations relating to money laundering control, including the criminal offences in the Proceeds of Crime Act 2002, come into play and bite on all the UK banks and payment system providers to which her money has been passed. In addition, the Second Wire Transfer Regulation (EU) 2015/847 of the European Union and of the Council of 20 May 2015 (retained in the UK by Funds Transfer (EU Exit) Regulations SI 2019/253) obliges banks in the UK to include accurate originator and payee information with each and every wire transfer and these do or should provide a clear evidence trail for any well motivated bank or investigator seeking to recover her savings. The current legal and regulatory obligations on the paying and receiving banks are obviously legion. Our customer assumes that these inform and populate the standard of care and skill that her bank owes her under the Consumer Rights Act 2015.

A personal remedy by the customer against the bank under s137D FSMA 2000 would in practice depend on successful prior FCA enforcement activity against her bank for a breach of the section of the FCA Handbook that caused her loss (or for breach of obligations under the ML Regulations). The average length of enforcement activity by the FCA against an authorised firm in 2020 was almost four years

(where cases went to the Regulatory Decisions Committee) and over ten years (where cases went to the Tribunal) (FCA, 2021). This is an uncertain and lengthy path to travel down for recompense.

The Contingent Reimbursement Model Code

Careful research may reveal the above (Model Code) which presents as a scheme providing a useful means of victim redress. This industry code of practice was introduced on 28 May 2019 as a result of increasing customer loss through push payment scams and after pressure from the UK Payment Services Regulator. It currently has nine signatories which together represent 20 banking brands. The Lending Standards Board now takes responsibility for overseeing the workings of the code and analysing its impact (Lending Standards Board, 2021). The Model Code is expressed to be "subject to applicable law and regulation" rather than determinative of law or of the standard of care applicable to the bank /customer relationship. The professed aim of the Model Code is to ensure that customers who lose money when they were not to blame for the success of the scam are reimbursed. The Model Code contains commitments by signatories and the first of these rule 1, is a commitment to reimburse. This is closely followed by exceptions including ignoring effective warnings (SF1(2)), customer gross negligence, or the lack of a reasonable basis, in the particular circumstances of that scam, for the customer's belief that the payee or payment was genuine and legitimate. The Model Code includes a sophisticated and useful definition of customer vulnerability, acknowledging that vulnerability can shift over time with circumstances, and dictates that vulnerable customers should be reimbursed even when some of the listed exceptions to the reimbursement obligation apply. The Model Code mandates the use of prevention measures, by each bank, such as customer due diligence on account opening, use of industry databases and shared intelligence sources, the application of typologies to identify accounts that are at high risk and implementation of a confirmation of payee system in a manner likely to influence customer behavior. The Model Code is carefully worded and detailed. But it has no teeth whatsoever. No penal, financial or regulatory consequences follow from signatories of the code failing to comply with its terms and no method is ascribed for adjudicating on the various standards set out such as the reasonableness of the customer's approach in all the circumstances or whether the warnings given by the bank were in fact real and effective. In the absence of any compulsory and independent adjudication process it is of very little value to the deprived customer. The relevant bank's decision on liability will prevail. It is not "law" within the generally accepted meaning of that word and provides no reliable means of redress. The Lending Standards Board is an industry body. It is not independent. Its latest analysis (Lending Standards Board 2021) of the implementation of the Model Code by the signatory banks is that there are many serious failings in implementation and that it is not providing customers with the protection and remediation for which it was designed. (Lending Standards Board 2021) . Its terms have now been amended and a letter to Chief Executives of the signatories has been delivered which encourages a shift in practice. In the absence of financial consequences, one would expect little to change.

Assuming that our scammed customer writes to her bank seeking reimbursement under the Model Code and her claim is rejected, she may turn to litigation and sue for damages in the civil courts for breach of her contract for service by reason of negligence in executing her payment request. The bank has failed to comply with the FCA Handbook and the MLA Regulations and the Model Code. On the face of it, reasonable care and skill is lacking.

Bank's duty of care in contract

It is an implied term of the contract between the customer and her bank under s 49 Consumer Rights Act 2015 and case law that it will exercise reasonable care and skill in operating the bank and dealing

with the customer's payment instructions. In *Lipkin Gorman v Karpnale Ltd [1989] 1 WLR 1340* , where the relevant means of payment was a cheque, rather than in the instant case an online payment instruction, Parker LJ defined the relevant test as whether the reasonable and honest banker would have considered there was a real or serious possibility that its customer was being defrauded. If that test was applied and the bank failed it, liability would follow.

That decision was followed in *Barclays Bank v Quincecare Ltd [1992] 4 All ER 363* where it was found that there were no facts which ought to have put the bank on enquiry as to the fraudulent behaviour of its client's chairman of the Board of Directors. Steyn J stated (at page 379) that " a banker must refrain from executing an order if and so long as the banker is put on enquiry in the sense that he has reasonable grounds (although not necessarily proof) for believing that the order is an attempt to misappropriate funds." Both these cases relate to written payment instructions (in the Quincecare case the payment instructions were given verbally on the telephone and then confirmed in writing by letter). The cheque (and other forms of hard copy payment instruction) are now very rarely used.

In 2020 over two thirds of UK adults used online banking and over half used mobile banking (UK Finance UK Payment Markets Summary 2021). These remote banking payment instructions are processed via the Faster Payment Service (FPS) or cleared in house by the banks themselves. In 2020 2,952 million remote banking payments were made and this compares with 422 million such payments in 2010. In contrast the number of cheques used to make payments has continued to decline. In 2020 185 million cheques were used to make payments compared to 1,050 million cheques in 2010. The remote banking payment is 16 times more likely to be used by the customer as the means to effect payment than the cheque.

Nearly every bank in the UK now uses FPS to effect remote transfers of money between current accounts. FPS is operated by Pay.Uk Limited a company limited by guarantee and regulated by the Payment Services Regulator. The customer interfaces with her bank, using the internet portal provided by it, and the bank then interfaces with FPS using protocols, operating procedures and contractual terms governing this relationship. The customer's legal relationship is with her bank.

If the common law develops incrementally in the light of social and commercial practice it will apply in the same manner to the remote payment instruction as to the written payment instruction, regardless of the speed of the transactions and the vast volume processed each day. Alternatively, the technological shift to remote payment methods has ridden the duty of care and the obligation of agent to principal of relevance in all but the most exceptional payment cases. If this is the case, the law has abandoned the customer and assisted the criminal and the bank. No remedy exists. The bank is held harmless, the criminal is undetected and the customer suffers the loss.

The standard of care applicable today in remote payment instruction cases

Instances where payment instructions were delivered remotely by the customer were considered by the Court of Appeal in T*idal Energy Ltd v Bank of Scotland plc* [2014] Bus LRR 1167 and in *Singularis Holdings Ltd v Daiwa Capital Markets Europe Ltd* [2019] Bus LR 3086; [2020] AC 1189. Both these cases concerned corporate clients and much larger payments were in issue.

In Tidal Energy the decision turned upon the terms of the CHAPS payment system and the CHAPs authorisation form and evidence of then standard banking practice which relieved the bank of any

obligation to confirm that the sort code and account number provided by their remitting client matched the intended recipient's name. The sort code and account number provided by the client to the bank were erroneous (and had been provided to the client fraudulently). The outcome of the case was that the bank was held not to have been negligent or in breach of contract in remitting the funds on those particular facts. Of course banking practice has changed significantly since this case and there are now regulatory obligations on banks in the six largest UK banking groups banks to undertake "confirmation of payee" checks when acting on payment instructions and an expectation that this will be extended to all banks in the UK. Regulation has responded to risk.

In Singularis the payment instructions were delivered to Daiwa through SWIFT and were then authorised by individuals at Daiwa. The evidence at first instance shows that Daiwa was aware that it was under some obligation to act with care in authorising payment instructions to third parties by Singularis and to refer any difficult issues to their Legal or Compliance divisions. The evidence established the reason for this extra level of caution as related in paragraphs 74-104 as concerns over the probity and honesty of the company and key individuals running it as well as initial concerns over its financial standing. In this case, the facts show that individual employees of the bank authorised each and every payment instruction. In fact the ultimate outcome of the case, in the Supreme Court, was that in authorising these SWIFT payments Daiwa had failed to appropriately take into account all the issues that the bank was aware of in relation to the company's reputation and probity and thus had acted in breach of its duty of care and skill to Singularis. In that case the eight payments in question totaled US$204.5 million.

In *Singularis* Baroness Hale PSC referred to the potentially conflicting duties on the bank to execute a customer's order promptly and to use reasonable care and skill in acting on the customer's payment instructions. At para 1 she stated "... there would be liability if the bank executed the order knowing it to be dishonestly given , or shut its eyes to the obvious fact of the dishonesty, or acted recklessly in failing to make such inquiries as an honest and reasonable man would make; and the bank should refrain from executing an order if and for so long as it was put on inquiry by having reasonable grounds for believing that the order was an attempt to misappropriate funds." Later in the case, at paragraph 35 of [2020] AC 1189, Baroness Hale suggests that the Quincecare duty is one which only applies to circumstances in which agents for the corporate client (such as a director) have attempted to defraud the company in circumstances where the bank should have been put on notice of wrong doing and raised queries or delayed the payment. The limitation of the Quincecare duty to these circumstances is surprising but it would not be logical or in line with authority to conclude that the Quincecare duty, as so limited, is the only duty of care and skill that applies to the bank in dealing with payment instructions especially as in relation to bank customers that are consumers, we now have s49 Consumer Rights Act 2015. It is inconceivable that this statutory obligation does not apply to the bank's role in executing payment instructions, which is a role at the heart of the relationship. In addition case law establishes that the relationship of principal and agent applies with its attached obligations on the bank as agent.

Having established that the duty exists, to determine the applicable standard we turn to reported case law. The difficulty with the legal analysis in all the reported cases is that it examines the precise actions the bank's employees took in dealing with payment instructions and compares them with those of the hypothetical reasonable and prudent bank employee. (This analysis was undertaken diligently by the court in relation to the actions of Barclays Bank plc in dealing with the payment requests of Mrs Philipp in the case of Philipp v Barclays Bank UK plc [2021] Bus LR 451. This is one of the very few reported cases that relate to an ordinary retail customer and push payment scams. In that case the instructions were

delivered in person and evidence was collected from individual bank employees to determine whether the response was that of a reasonable bank.) In the reported cases the payments at stake are very large. It is not surprising that they were dealt with individually. But does the size of the individual payment change the nature of the legal relationship between a bank and its customer and the attendant obligations? Is it the wealth and resources of the customer that determines the standard of care? One hopes not.

For ordinary retail customers using remote payment methods, it is a series of customer key strokes that moves money from one bank account to another, enabled by the customer's use of the bank's portal. It is not a process on which human decision making by any bank employee bears. It is automatic and almost instantaneous unless the bank's anti money laundering and fraud detection IT systems have been programmed to suspend or flag it based on the exception reporting protocols at the relevant bank. The bank's payment systems communicate almost instantaneously with FPS unless prevented from so doing so by the bank's own IT systems. In these circumstances the duty of care and skill must still exist, because, normatively, in its absence the bank could negligently operate its portal and payment systems to the detriment of the customer without liability and, positively, because the Consumer Rights Act 2015 s49 and the law of agency so provide.

Whether a bank would be breaching the standard of care if its IT systems applied no transaction monitoring or other fraud checks or customer identity verification whatsover is a matter that has yet to come before the court. In the Phillip's case, the instructions were delivered in person not remotely and so the issue was not in point (although Phillip's legal team made a brave attempt to introduce it by way of expert evidence to argue that industry standard transaction analytics would have stopped and delayed the payments in issue). Additionally, in the Phillip's case the customer repeatedly concealed relevant information from the bank and the police and breached the terms of her contract with the bank by providing detailed security information to the fraudster and allowing him to covertly listen to phone conversations between herself and the bank and herself and the police. A finding that the customer's actions, and not those of the bank, had caused the loss is unsurprising on these very particular facts and is markedly different from those applying to the standard push payment scam using remote payment facilities provided by the bank where a lack of customer due diligence and transaction monitoring causes the payments to pass unchecked.

Whether the bank's own IT systems have been established and programmed with care and skill in the light of the bank's detailed knowledge of its customer base and transaction pattern is a matter on which a judicial assessment could be made. It is a justiciable issue, if a complex one. Evidence could be collected on industry practice from the UK's regulator the FCA, the Joint Money Laundering Steering Group and FATF. Expert knowledge on artificial intelligence and fraud detection could be assembled and views held in the balance by the court on whether the IT systems applied to the payment instructions were those of the reasonable bank at that particular time. Reference could be made to the regulatory standards demanded by SYSC in relation to customer due diligence and transaction monitoring and to the application of these standards by the FCA in its recent supervision and enforcement activity. The statutory obligations on the bank under the Money Laundering Regulations and Second Wire Transfer Regulation could be examined and applied to determine how lax or diligent this bank had been on this occasion in the face of this unusual payment request. The content of the contingent push payment model code would be relevant in assessing what is now expected of the well run prudent bank in terms of a real and effective warning. Given that no bank can exist lawfully in the UK that is not bound by the

regulatory and civil law described above, it would be astounding if compliance with these standards was not an issue in any adjudication of the standard reached by the bank in executing a payment instruction.

Conclusions

Unfortunately there is little litigation against banks by consumers in relation to the operation of their bank accounts and our culture inclines customers towards complaints rather than enforcement of legal rights. In the circumstances which prompted this article, the fee to commence action in the County Court for damages would have been £2474.50. A large sum to find in the context of having lost one's life's savings with an uncertain legal basis for proceedings. (The circumstances prompting this article were in fact dealt with by reimbursement under the Model Code. Anonymized correspondence can be provided on request.) The lack of litigation provides scant opportunity to put flesh on the bones of the standard of care banks owe their customers in relation to reasonable, appropriate and effective transaction monitoring analytics. Remote banking has cut costs for banks. It does in fact raise real risks for consumers and those risks are greater in terms of personal consequences for less wealthy clients than for wealthy clients. The common law must adapt to technological change and compel banks to take care. These obligations are already imposed on them by criminal and regulatory law. It is right that these obligations assist hard up consumers too.

References

Action Fraud (2021), "Annual Assessment of Fraud Crime Trends 2020/21." Available at https://data.actionfraud.police.uk/cms/wp-er/content/uploads/2021/07/2020-21-Annual-Assessment-Fraud-Crime-Trends.pdf (accessed 10 August 2021).

FCA (2021), "FCA Enforcement Data - Annual Report 2020/21 "

FCA Handbook. Available at https://www.handbook.fca.org.uk/

Lending Standards Board (2021), "Lending Standards Board Review of the CRM Code for Authorised Push Payment (APP) scams. 28 January 2021" Available at https://lendingstandardsboard.org.uk/wp-content/uploads/2021/01/LSB-review-of-the-CRM-Code-FINAL-January-2021-.pdf (accessed 6 October 2021)

Lending Standards Board (June 2021) "Follow-up Review of Contingent Reimbursement Model Code for Authorised Push Payment Scams. Approach to Reimbursement of Customers-provision R2(1). Summary Report. June 2021." Available at https://www.lendingstandardsboard.org.uk/wp-content/uploads/2021/06/CRM-Review-R21c-Follow-Up-Summary-Report.pdf (accessed 11 October 2021)

Model Code, "Lending Standards Board: The Contingent Reimbursement Model Code for Push Payment Scams April 2021". Available at https://www.lendingstandardsboard.org.uk/wp-content/uploads/2021/04/CRM-Code-LSB-Final-April-2021.pdf (accessed 6 October 2021)

UK Finance (2021), "Fraud- The Facts 2021 The Definitive Overview of Payment Industry Fraud"

UK Finance (Payments Markets Summary 2021) , " UK Payments Markets Summary 2021, June 2021". Available at https://www.ukfinance.org.uk/sites/default/files/uploads/SUMMARY-UK-Payment-Markets-2021-FINAL.pdf (accessed 6 October 2021)