APP Fraud: The Long Road to Reimbursement

Authorised Push Payment ("**APP**") fraud scams have been an ever-growing threat to the safety of both personal and business banking customers in recent years. These scams come in various forms and range in levels of sophistication. The two most common formats appear to be email intercept scams in which emails are hacked and legitimate invoices/requests for money are replaced with a fraudster's bank account details or where victims are contacted by a fraudster posing as a legitimate payee or bank employee, who then convinces them to transfer money from their own bank account to one controlled by the fraudster. The most sophisticated scams groom customers by calling to inform them that there has been an attempted fraud on their account and that their funds are at risk if they are not transferred to account which is actually controlled by a fraudster. In these instances, the fraudsters often persuade customers that they are part of the bank's fraud team or the FCA and that they must follow their instructions to protect their money.

The amounts of money lost to APP vary, however, they are often life-altering for personal banking customers and can have a severe impact on the operating capabilities for businesses. Further, the prevalence of APP scams and the amounts being lost overall to them has been rising dramatically in recent years, with a total of £354 being lost in 2018, £456 million in 2019, £479 million in 2020 and £355 million lost in the first half of 2021 alone (up 71% for the same period in 2020). Much of this appears to be a result of the global coronavirus pandemic as more and more transactions occur electronically and individuals less accustomed to online banking are forced to embrace that as the norm.

In reaction to this growing threat, the Lending Standards Board ("**LSB**") introduced the Contingent Reimbursement Model ("**CRM**") code on 28 May 2019 to provide greater protection to both personal and business banking customers from APP scams. The CRM code is voluntary and sets out the manner in which signatory banks should attempt to prevent, investigate and respond to APP scams and the customers who have fallen victim to them.

In this article, Dan Dodman and Ruhi Sethi-Smith will summarise the CRM code, its application to victims of APP fraud and the reasons often cited by banks for refusing to reimburse victims. For those who are refused reimbursement from their bank, we will examine the current legal position in relation to seeking recovery of losses flowing from APP fraud and the potential changes to the law as a result of the case of *Philipp v Barclays Bank UK Plc*[1].

1. The CRM Code

There are currently nine UK banks which have signed up to the CRM code, those being: Barclays Bank, the Co-Operative Bank, Lloyds Banking Group, Metro Bank, Nationwide Building Society, NatWest (including Royal Bank of Scotland and Ulster Bank), Santander, and Starling Bank.

CRM Code Standards for Firms

[1] [2021] EWHC 10 (Comm)

The CRM code imposes a set of standards on each signatory bank specifically in relation to APP scams, which if not met, will require those banks to reimburse their customers for some or all of the amount they have lost. These requirements are specified under rule SF of the CRM Code, which states:

"These provisions set out the standards that firms should meet. If firms failed to meet these standards, they may be responsible for meeting the cost of reimbursing, in accordance with R1, a customer who has fallen victim to an APP scam."

These standards are heightened where the customer in question is considered vulnerable, as a result of the personal circumstances of that customer (i.e. their age or health), their capacity to protect themselves, and the impact and nature of the scam itself.

Additionally, the standards in the CRM Code are split between the banks which send customer money and the banks which receive it, and it requires that both the sender and receiver of customer money have in place systems which can detect, prevent and respond to suspected or confirmed APP scams.

CRM Code Standards for Sending Banks

Under the CRM Code, the requirement for sending banks to have in place systems which can detect, prevent and respond to APP scams are outlined under rules SF1 (1), (2), (5) & (6).

1. Detect – SF1(1)

    - Sending banks should be able to identify customer payments which run a high risk of being associated with APP scams.
    - They can do so by analysing customer transactional data and behavioural analytics, and by training their employees to readily identify such transactions.

2. Prevent – SF1(2)

    - Sending banks should take reasonable steps to provide their customers with effective warnings throughout the process of making a transfer to a potential fraudster in an APP scam.
    - This means that fraud warnings should be present throughout the payment process, including when a customer is setting up a new payee, amending an existing payee and immediately before they authorise a payment from their account.
    - While the CRM Code does not currently require the implementation of Confirmation of Payee (**"CoP"**) systems, it is strongly suggested that such systems are put in place and they have left a placeholder in the code where such a date for mandatory implementation can be inserted.

3. Respond – SF1(5) & (6)

    - Under rule SF1(5), where a bank has sufficient concern that a customer authorised payment may be an APP scam, they are expected to intervene and take appropriate action to delay that payment while they get in touch with both the customer and receiving bank to confirm its authenticity.
    - Under rule SF1(6), where a customer reports that they have been subject to an APP scam, the sending bank is obligated to notify the receiving bank within the specified time frames.

CRM Code Standards for Receiving Banks

Similar to the above, banks receiving funds are also expected to have in place systems which can prevent, detect and respond to suspected or confirmed APP scams. These are outlined under rules SF2 (1), (3), (4) & (5).

1. Prevent – SF2(1)

    - Receiving banks must take reasonable steps to prevent their accounts from being used to facilitate fraud and other criminal activities.
    - To comply with this direction, banks are advised to use shared intelligence sources and industry fraud databases. These can be used to screen or identify accounts which are highly likely to be set up and used by criminals.

4. Detect – SF2(3)

    - Receiving banks are expected to take reasonable steps to detect accounts which are likely to have been used to receive APP scam funds.
    - Similarly to sending banks, receiving banks are expected to make use of transactional data, customer analytics and enhanced staff training to achieve this.

5. Respond – SF2(4) & (5)

    - When a receiving bank is notified of concerns regarding a possible APP scam, they are expected to act in accordance with the best practice standards developed by the UK Finance trade association.
    - Conversely, where an APP scam has been identified, the receiving bank must take reasonable steps to freeze and repatriate the funds to the sending bank.

The CRM Code and reimbursing APP victims

In addition to the standards outlined above, the CRM Code also provides rules on how banks should treat victims who have actually been defrauded.

As a starting point, under rule R1, the CRM Code notes that one of its fundamental principles is that:

"Subject to rule R2, when a customer has been a victim of APP fraud banks should reimburse them"

While, generally, this is good news for victims of APP fraud, it does not mean that customers are automatically entitled to a refund in any and all circumstances. The key here is the qualification that this rule is subject to the terms of R2.

Under rule R2, it states that:

"A firm may choose not to reimburse a customer if it can establish any of the following matters in (a) to (e)"

Therefore, a bank can decide not to refund a customer if they can show that the matters listed in (a) – (e) had any impact on preventing the APP scam. The factors covered under (a) – (e) include:

1. The customer ignoring the fraud warnings provided by the bank;

2. The customer authorising the APP transfer despite receiving a CoP notification;

3. The customer authorised the APP transfer in circumstances where it was not reasonable to believe that the payment being made was legitimate;

4. The customer was a business or charity which did not follow their own internal payment approval procedures; and

5. The customer was grossly negligent.

The above factors are intended to act as guidelines only for banks and each case will turn on its individual facts. Banks are required to carry out their own investigations into each APP fraud, and based on their findings, they can then make a decision on whether or not to reimburse a customer based on who they believe to be most at fault. Regardless of their decision, under rule R3, banks are required to provide a response within 15 business days or 35 business days in exceptional circumstances.

2. Reasons for refusing to reimburse victims

In general, the CRM Code provides a single, well laid out set of standards which signatory banks are required to meet. In theory, this should provide customers with both a greater level of protection from APP scams and certainty on whether they will be refunded.

However, while the reimbursement rates have improved somewhat, with the average reimbursement rate rising from 20% to around 45% in the 13 months after the CRM Code was introduced[2], in the majority of cases banks are refusing to reimburse their customers.

The data provided by the LSB in their 2021 review of the impact of the CRM Code highlights that the main reasons used by banks to refuse reimbursement are:

1. The customer is solely liable;
2. The sending bank is liable;
3. The receiving bank is liable;
4. There is no blame; and
5. The blame is shared (between the two or more of the sending bank, the receiving bank and the customer).

In our experience, by far the most common reason given by banks when refusing to reimburse clients is that of contributory negligence i.e. that they believe the customer is either fully or partially liable for their own misfortune in falling for the APP scam. These findings seem to be on trend with what the banks are reporting, as the data provided to the LSB in their review of the CRM Code, also states that between May 2019 (when the code was introduced) and July 2020, banks ruled that 77% of fraud victims were partially or fully to blame for their losses[3].

[2] LSB, Review of the Contingent Reimbursement Model Code for Authorised Push Payment Scams, January 2021, pg. 20

[3] LSB, Review of the Contingent Reimbursement Model Code for Authorised Push Payment Scams, Data Analysis, January 2021, pg. 17

Inconsistent Application

In addition to the banks' proclivity to blame their customers for money lost to APP scams, they are also highly inconsistent in how they apply the CRM Code. It seems that the decision to reimburse customers varies dramatically depending on the type of APP scam involved, the size of the bank itself and, perhaps most alarmingly, the amount lost by the customer.

For example, when reimbursement decisions are compared by APP fraud type, the data provided by the LSB indicates that in instances of CEO fraud (where a fraudster poses as a company CEO) and invoice and direct debit fraud, shared blame between the bank and the customer is a very common decision and accounts for 30% and 29% respectively of the decisions. This is far in excess of the other fraud types, which typically see shared blame decisions in the region of around 15% or less. Similarly, when dealing with banking staff or police impersonation APP scams, in 29% of all cases, no blame was assigned to either the banks or the customer. Again, this is far in excess of the other fraud types, where this decision is usually only issued in less than 10% of cases.

In addition to the above, as noted, the bank a customer uses can also have a marked impact on how they are treated if they are a victim of an APP scam. As the data provided by the LSB in their review of the CRM code clearly indicates that smaller banks (by CRM case totals) are much more likely to provide a no blame decision (52% of cases), while medium banks are more likely to assign blame to the customer (63% of cases). The larger banks do tend to provide a more balanced spread of decisions, however, they also lean further towards assigning blame to their customers (60% of cases)[4].

The above issues, coupled with the fact that the data provided by the LSB on the signatory banks is anonymous, means that customers still face a great deal of uncertainty in how the CRM Code is applied and whether or not they will be reimbursed.

3. Current Legal Position

Given the potential difficulties in obtaining reimbursement under the CRM Code outlined above, it is important to consider whether there are any legal avenues for recovery of the losses flowing from APP fraud from the bank which authorised and facilitated the payments to the fraudster.

The question of whether a banker might owe a duty to its customer to protect that customer against fraud, even if that fraud was committed by someone who had authority to act on behalf of the company, was first considered in the case of *Barclays Bank plc v Quincecare Ltd*[5]. The case concerned the misappropriation of the majority of a £400,000 loan by the chairman of Quincecare. Steyn J appreciated the delicate balancing act between executing a customer's payment orders promptly and guarding against the facilitation of fraud and struck that balance by formulating the duty in his judgment as follows: *"a banker must refrain from executing an order if and for as 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 of the company."* He confirmed that the standard of that duty was that of an ordinary prudent banker. This duty has since been referred to as the Quincecare duty.

[4] LSB, Review of the Contingent Reimbursement Model Code for Authorised Push Payment Scams, Data Analysis, January 2021, pg. 24

[5] [1992] 4 All E.R. 363, though the judgment was actually issued in 1988.

The first time that an English court held that the Quincecare duty had been breached was in the case of *Singularis Holdings Ltd (In Liquidation) v Daiwa Capital Markets Europe Ltd*[6]. This was essentially a case of CEO fraud whereby Mr Al Sanea, the Chairman and sole shareholder of Singularis instructed Daiwa to transfer US$204m to two other entities controlled by him in spite of knowledge that Mr Al Sanea's assets had been frozen and that he and Singularis were insolvent. It is noteworthy that Daiwa were able to persuade the Supreme Court to uphold the finding that Singularis's claim should be reduced by 25% for contributory negligence. The case of *Federal Republic of Nigeria v J.P. Morgan Chase Bank NA*[7] followed the decision in *Singularis* and the Court of Appeal held that the core of the Quincecare duty was an obligation on the Bank to refrain from making a payment where it had reasonable grounds for believing that the payment was part of a fraudulent scheme. Essentially, the Quincecare duty usually required a bank to do more than merely refuse to comply with a payment instruction but rather to take steps to resolve its concerns regarding a particular transaction.

An example of the most sophisticated APP fraud scams carried out on personal rather than corporate customers is the case of *Philipp v Barclays Bank Plc*. In this case, Dr and Mrs Philipp were persuaded by very sophisticated fraudsters to transfer the sum of £700,000 to a bank account in the United Arab Emirates. They were persuaded that they were assisting an investigation by the Financial Conduct Authority and the National Crime Agency. The grooming began with a telephone call from a fraudster claiming to be from HSBC's fraud department to Dr Philipp telling him that his account was not safe. Dr Philipp had another account with HSBC and therefore had no reason to doubt the provenance of this call. What followed was the exertion of coercive control over Dr and Mrs Philipp which left Dr Philipp feeling like he was *'being squeezed in a very unpleasant vice, not knowing who to trust'*.

HHJ Russen held that the Quincecare duty ought not to be extended to such situations (i.e. applied to individual customers) and instead "should be confined to cases where the suspicion which has been raised (or objectively ought to have been raised) is one of attempted misappropriation of the customer's funds by an agent of the customer"[8]. Therefore, as Mrs Philipp was acting on her own account and could not misappropriate her own funds, the Quincecare duty does not apply. HHJ Russen also held that Barclays Bank Plc was not required to play "amateur detective" and that Barclays Bank Plc had no reason to doubt the instructions given by Mrs Philipp and could not have been expected to know that she was being controlled by a fraudster. Given the high bar for obtaining strike out and/or summary judgment it is surprising that HHJ Russen decided to do this on a summary basis without hearing any evidence from either party.

The case of *Hamblin v World First Ltd*[9] involved a successful claim by Mr and Mrs Hamblin against World First Ltd as they had allowed fraudsters to withdraw their funds on the basis that a constructive trust had arisen in respect of the funds transferred.

As it stands, there have to be very particular circumstances before a bank is held to have been put on enquiry and therefore subject to the Quincecare duty i.e. corporate customers whose agent has authorised a payment and where there is a constructive trust and there are reasonable grounds for believing that the payment is a fraud on the customer.

---

[6] [2019] UKSC 50

[7] [2019] EWCA Civ 1641

[8] See para 156 of the judgment

[9] [2020] EWHC 2383

4. The Court of Appeal hearing in *Philipp v Barclays Bank Plc*

Dr and Mrs Philipp appealed the decision by HHJ Russen and that appeal was heard earlier this year. The grounds of the appeal are that (1) HHJ Russen erred in concluding on a summary basis that there was no duty owed to Dr and Mrs Philipp by Barclays Bank Plc and (2) HHJ Russen erred in concluding that the claim had no realistic prospect of success.

The arguments put forward in support of the appeal included the following:

- HHJ Russen was wrongly persuaded that the bank owed no duty to take reasonable steps to protect its customers from APP fraud;
- HHJ Russen was wrongly persuaded that the duties of the bank as a payment service provider was solely a question of law and decided this question on case law uninformed as to the industry practice;
- HHJ Russen was wrongly persuaded to look at historic case law;
- HHJ Russen was wrongly persuaded to look solely at historic case law;
- HHJ Russen was wrongly persuaded to ignore evidence regarding banking industry practice at the time;
- HHJ Russen wrongly rejected this evidence on the basis that it went to standards and not duty whereas the Appellants say that it went to both and was relevant;
- HHJ Russen was wrongly persuaded that there was no real prospect of the Dr and Mrs Philipp showing that there were relevant standards of banking practice regarding APP fraud in 2018
- HHJ Russen was wrongly persuaded to treat the Quincecare duty in as a 'solitary island' rather than a sub set of the case law in this area

During the submissions for the appellants, Lord Justice Birss commented if one was to take HHJ Russen's reasoning in his judgment to its logical conclusion you would end up in a strange situation whereby 'the duty only really exists in relation to corporate customers and individual customers, who are the very people who most of the relevant legislation and guidance is designed to protect, would be left out in the cold.

The Consumer Association, Which?, intervened and the following points were made on its behalf:

- The Quincecare duty is an aspect or sub-set of the general duty that a bank owes to its customer to exercise reasonable care and skill
- It would be illogical and unprincipled to limit the Quincecare duty to cases where a corporate customer is defrauded by its agent
- The requirements of the Quincecare duty is calibrated by ordinary banking practice and does not seek to impose onerous obligations upon banks in relation to APP fraud
- The requirements of ordinary banking practice have developed over time and were not fully taken into account by HHJ Russen
- Even if the application of the Quincecare duty to individual customers involves an extension, it would be fair, just & reasonable to extend it to individual customers who are the victims of APP fraud.

The overarching backdrop to the appeal is that customers are simply seeking to require banks to take reasonable steps to protect them from the effects of APP fraud where there are clear warning signs or 'red flags' as they are best placed to do this.

Perhaps unsurprisingly, Barclays Bank Plc maintained that HHJ Russen's reasoning was impeccable and that the sole issue in the case was whether the bank was under the duty alleged by the claimants. It was argued

that the standards of care or standards of the banking industry at the time are completely immaterial and that this case was well suited to being dealt with summarily.

Judgment in the case was handed down on 14 March 2022 and the appeal was unanimously allowed. Having been persuaded by Counsel for the Appellant and Counsel for the Intervener, it was held that it was *'at least possible in principle that a relevant duty of care could arise in the case of a customer instructing their bank to make a payment when that customer is the victim of APP fraud'* (as set out in paragraph 78 of the judgment). In essence, the *Quincecare* duty could in theory apply to victims of APP fraud and be put 'on inquiry' in the same way as they are in relation to companies. The second conclusion was that '*the right occasion on which to decide whether such a duty in fact arises in this case is at trial.'*

It will be interesting to see how the case is decided at trial and in particular the circumstances in which a bank would be put *'on inquiry'* when dealing with victims of APP fraud and the level of any contributory negligence on the part of the customer(s).

Daniel Dodman

Dan is a partner at Goodman Derrick LLP where he heads up the Dispute Resolution team and the civil fraud practice. He acts on high value disputes, freezing injunctions and tracing claims. Dan also has a particular interest in consumer frauds and Push Payment scams where he regularly acts for individuals who have lost sums that they are unable to recover through other means.

Ruhi Sethi-Smith

Ruhi Sethi-Smith is a barrister at Forum Chambers specialising in banking and financial services law and commercial disputes. Ruhi regularly receives instructions on APP fraud claims where individuals have been the victims of sophisticated scams.