THOMSON REUTERS
PRACTICAL LAW™

Banks' duties when executing client instructions: the Quincecare duty

by Ravi Jackson and Devon Airey, 3 Verulam Buildings

Status: **Dated 5 January 2024** | Jurisdiction: **United Kingdom**

This document is published by Practical Law and can be found at: **uk.practicallaw.tr.com/w-029-5158**
Request a free trial and demonstration at: **uk.practicallaw.tr.com/about/freetrial**

This note provides an overview of the *Quincecare* duty and explains how banks can mitigate the risks of acting in breach of the duty when executing client instructions. It is one of a suite of notes on banks' duties aimed at in-house legal counsel working at a bank.

Scope of this note

This note provides an overview of the *Quincecare* duty. It addresses six key questions:

- What is the *Quincecare* duty?
- What is the legal basis for the *Quincecare* duty?
- In what circumstances will the *Quincecare* duty arise?
- When is a bank "put on inquiry"?
- What reasonable steps should banks take to avoid acting in breach of duty?
- What alternative methods of redress are available?

The leading case on the duty is the Supreme Court decision in *Philipp v Barclays Bank UK Plc [2023] UKSC 25*.

The note is part of a suite of notes on banks' duties. The other notes are listed below:

- Practice note, Banks' duties when providing bank references and other information to third parties.
- Practice note, Banks' duties: fiduciary duties owed by banks.
- Practice note, Banks' duties: equitable duties owed by mortgagees when exercising a power of sale.
- Practice note, Banks' duties when providing advice and information.
- Practice note, Liability of banks for advice on regulated financial products.

Overview of the *Quincecare* duty

What is the Quincecare duty?

The *Quincecare* duty (established in *Barclays Bank v Quincecare [1992] 4 All ER 363*) prevents a bank from executing a payment instruction given by an agent of its customer where it has reasonable grounds to believe that the instruction is an attempt by the agent to defraud the customer (see *Philipp at paragraphs 5, 90 and 97*).

If such reasonable grounds exist, the bank is "put on inquiry" and must make inquiries to ascertain whether the instruction was actually authorised by the customer before executing the payment instruction; if the bank executes the payment instruction without making such inquiries: the bank will be acting in breach of duty and the instruction will not bind the customer and the bank will not be entitled to debit the payment to the customer's account (*see Philipp at paragraphs 90 and 97*).

What is the legal basis for the *Quincecare* duty?

The legal basis for the *Quincecare* duty was clarified by the Supreme Court in *Philipp*, which is now the leading case in this area. The key points are as follows:

- In ordinary circumstances, a bank is a debtor (not a trustee or fiduciary) of money deposited by its customer and the principal obligation owed by the bank is to discharge its debt to the customer when called upon to do so (see *Foley v Hill (1848) 2 HL Cas 28; Philipp at paragraph 28*). The bank is obliged to repay to the customer on demand an equivalent

THOMSON REUTERS®

sum to that deposited and, provided the account is in credit, to make payments in accordance with the customer's instruction (*Philipp at paragraphs 3 and 28*). In making such payments, the bank acts as the customer's agent (*see Westminster Bank Ltd v Hilton (1926) 43 TLR 124 at paragraph 126; Philipp at paragraph 28*).

- A bank has a duty to exercise reasonable care and skill in executing a payment instruction. However, critically, this duty only arises where the validity or content of the customer's instruction is unclear or leaves the bank with a choice about how to carry out the instruction (*see Philipp at paragraphs 35 to 36 and 63*).
- The *Quincecare* duty is simply an application of this duty to exercise reasonable care and skill in executing a payment instruction (*see Philipp at paragraph 97*). It arises because if there are reasonable grounds to believe that the agent is attempting to defraud the customer, the agent will lack apparent authority to act on the customer's behalf, rendering the validity of the payment instruction unclear or ambiguous (*see Philipp at paragraphs 90 to 91*).

In what circumstances will the *Quincecare* duty arise?

As noted above, the *Quincecare* duty will arise where an agent of the customer gives a payment instruction to the bank and there are reasonable grounds to believe that the instruction is an attempt by the agent to defraud the customer.

The *Quincecare* duty may apply not only to banks, but also to payment service providers (see *Hamblin v World First Ltd [2020] EWHC 2383 (Comm)*).

Importantly, the *Quincecare* duty will not arise where an unequivocal payment instruction is given by the customer personally or by its agent; even where the payment instruction has been procured by fraud (such as where there has been an authorised push payment (APP) fraud (*see Philipp at paragraph 100*)).

Following the logic of *Philipp*, the *Quincecare* duty (or, put more broadly, a duty to exercise reasonable care and skill in executing a payment instruction) may also arise where a fraudster impersonates the customer and gives a payment instruction to the bank, but there are reasonable circumstances to believe that the instruction is an attempt to defraud the customer, such that the validity of the payment instruction is unclear or ambiguous. There is no decision of the English Courts considering this specific scenario but see *Aegis Resources DMCC v Union Bank of India (DIFC) Branch [2020] DIFC CFI 004* where the Dubai International Financial Centre (DIFC) Court of First Instance upheld a claim for breach of the *Quincecare* duty.

When is a bank "put on inquiry"?

This will turn on the facts of each case. However, some general points emerge from the case law:

- The court will not readily find a bank to be "put on inquiry". Although ultimately a question of fact, the *prima facie* assumption is that "men are honest". Further, the court must have regard to the very limited time banks have to decide how to proceed with a payment instruction, without risking liability for delay (*see Selangor United Rubber Estates Ltd v Cradock (No 3) [1968] 1 WLR 1555 at page 1608; Karak Rubber Co Ltd v Burden (No. 2) [1972] 1 WLR 602 at page 603*).
- The bank is likely to have had "reasonable grounds" to believe a payment instruction was fraudulent where it would have considered there to be "a serious or real possibility, albeit not amounting to a probability", that its customer was being defrauded (*see Lipkin Gorman v Karpnale Limited [1989] 1 WLR 1340 at page 1378A; Singularis Holdings Ltd (In Official Liquidation) v Daiwa Capital Markets Europe Ltd [2017] EWHC 257 (Ch) at paragraphs 166 to 167*).
- The court must look at the question holistically. It should consider not only those factors suggestive of fraud but also factors supporting the genuineness of the transaction (*see Nigeria v JP Morgan Chase Bank NA [2022] EWHC 1447 (Comm) at paragraph 347*).
- The focus must be on notice of the matter that vitiated the payment instruction and not any different or wider potential concern (*see JP Morgan at paragraph 158*). In other words, there must be a "distinction between the fraud which is critical and the many frauds which are not" (*see JP Morgan at paragraph 346*). (For example, even a series of Serious Organised Crime Agency investigations, if unrelated to the fraudulent payment itself, will not put a bank on notice (*see JP Morgan at paragraph 389*)).

There are very few cases where the *Quincecare* duty has been found to have been breached. The principal examples are Singularis (decided by the English Court) and Aegis (decided by the DIFC Court of First Instance). Both cases provide examples of factors that may put a bank on inquiry. These include:

- **Inconsistency between the instruction and the customer's transaction history or business.** Where the instruction is outside the customer's transaction history and is unrelated to the customer's known business, that may provoke reasonable suspicion (*see Aegis at paragraphs 141 to 143 and 154*).
- **Non-compliance with the bank's usual process for verifying instructions.** Where the payment instruction does not conform with the bank's process for verifying instructions, that may also give rise to reasonable suspicion (*see Aegis at paragraph 154*).

- **The magnitude of the transaction compared to the customer's financial circumstances.** Significant differences between the size of the payment and the known financial circumstances of the bank's customer may contribute to a bank being put on inquiry (*see Singularis at paragraphs 193 to 197 and 201*).
- **Suspicious contractual arrangements.** Where the customer produces a previously unmentioned contract to justify a very substantial payment, that may give rise to reasonable suspicion (*see Singularis at paragraph 200*).

What reasonable steps should banks take to avoid acting in breach of duty?

To avoid acting in breach of duty, banks should consider the following steps:

- **Surveillance and monitoring.** Have in place robust systems for monitoring accounts and detecting transactions and instructions which are unusual in the light of the customer's usual course of activity, including in relation to:
  - the identity of the person giving the instruction;
  - the form of the instruction;
  - the size of the payment;
  - the identity of the payee;
  - the fact that the account holder might be insolvent; and
  - the fact that the account holder is a company controlled by a sole director and shareholder.
- **Know your customer (KYC).** To the extent possible, make use of relevant information available from other sources, such as information in the public domain. KYC policies and procedures should hold the sales department accountable for passing this information onto the compliance department. Internal systems should also track this kind of information from external sources.
- **Escalation processes.** Have in place clear, step-by-step protocols for escalating concerns to compliance personnel.
- **Red flags.** Red flag key events in the system so that the information flows through the various functions involved.
- **Investigation.** Have in place a clear procedure for enhanced due diligence and the documenting of investigations.
- **Training.** Train sales teams not to accept at face value, and to interrogate thoroughly, explanations and documents proffered by the account holder.
- **Allocation of responsibilities.** Ensure that the responsibility for making decisions in respect of the matter investigated is allocated, by way of written policies and procedures, to a specific person or group of people.
- **Retaining evidence and documenting decisions:**
  - If the conclusion is reached that there are reasonable grounds to believe that the instruction is an attempt to defraud the account holder, document that conclusion carefully and the reasons for it, and decline to execute the instruction until sufficient evidence is produced to demonstrate that the instruction is legitimate. If at any point a bank considers itself to be "put on inquiry", it should also consider whether it needs to file a suspicious activity report (SAR) under the Proceeds of Crime Act 2002 (POCA). Banks should be careful to avoid committing the tipping-off offence under POCA if they have filed a SAR.
  - If the conclusion is reached that sufficient evidence has been produced to demonstrate that the instruction is legitimate, document that conclusion carefully and the reasons for it, before executing the instruction.
- **Industry standards.** Ensure that the bank's internal policies are in line with, or go further than, industry standards.

What alternative methods of redress are available?

As noted above, importantly, the *Quincecare* duty will not arise where the customer gives an unequivocal instruction to the bank that is procured by an APP fraud. However, there are other (limited) legislative and regulatory means by which victims of APP fraud might obtain redress.

CRM Code

Since 2019, banks can voluntarily opt into the Contingent Reimbursement Model Code of Practice for APP scams developed by the Lending Standards Board (LSB) (LSB: Contingent Reimbursement Model Code of Practice). In doing so, banks commit to reimbursing victims of APP fraud for their losses. Details of the banks that are signed up to the Code are available on the LSB website (LSB: Webpage: Protecting personal and business customers through registration).

Section 72 of FSMA 2023

Section 72 of the Financial Services and Markets Act 2023 (FSMA 2023) provides for a mandatory scheme of reimbursement. Payment services providers must reimburse victims of APP fraud "where the payment order is executed subsequent to fraud or dishonesty".

The Payment Systems Regulator (PSR) has been tasked with implementing the scheme, which will take effect in 2024. In summary:

- Banks and other payment service providers will be expected to reimburse APP fraud victims where the Faster Payments system has been used.
- Liability will be split 50/50 between the paying and receiving banks.
- The victim of APP fraud must be reimbursed within five business days unless the "clock is stopped", such as where the sending payment service provider requires further information to properly investigate the claim.

However, the PSR's proposals currently envisage that international payments will not be a "qualifying case" under section 72 of the FSMA 2023. Accordingly, where fraudulent payments are made outside the UK, there will be no obligation on a payment service provider to reimburse its customer. Further, consumers will not presently have a right of action to enforce the reimbursement of payments by banks. For example, there is no equivalent of section 138D of the Financial Services and Markets Act 2000 (FSMA), which grants a right of action for damages to private individuals. Many victims of APP fraud therefore will fall outside the scope of the mandatory reimbursement scheme.

For information on regulatory initiatives relating to APP fraud, see Practice note, UK payments: regulatory landscape and current initiatives: Authorised push payment (APP) fraud. For information on section 138D of FSMA, see Practice note, Actions for damages under FSMA.