Chapter 2 The banker-customer relationship

2.1 Introduction

Page 21

They were succeeded by the 2011 Lending Code,[1] which itself was replaced in July 2016 by the Standards of Lending Practice (personal customers), and March 2017 by the Standards of Lending Practice (business customers).[2]

2.4 Duties of the bank in the banker-customer relationship

2.4.4 Confidentiality

2.4.4.2 Alternative sources of the duty

Page 40

Most recently the *Lending Code* was replaced by the *Standards of Lending Practice* in July 2016, which itself was updated most recently in April 2021. These standards fail to explicitly refer to the requirement of banks to treat personal information as private and confidential, instead only mentioning that *'Firms will maintain the security of customers' data.'*[3]

Page 41

While the UK was still part of the EU when the GDPR came into force, the uncertainty in light of Brexit led the UK Department of Digital, Culture, Media and Sport to publish a Statement of Intent on 7 August 2017 in which it outlined the policy and objectives behind a new Data Protection Bill which would enshrine the EU standards in the UK.[4] This Bill was introduced in Parliament on 13 September 2017 and the new Data Protection Act 2018 received Royal assent on 23rd May 2018. The

---

[1] Revised most recently in September 2015, https://www.lendingstandardsboard.org.uk/wp-content/uploads/2016/06/The-Lending-Code-Mar-2011-revised-2015-1.pdf

[2] The standards for personal customers were revised most recently in April 2021 and are available at https://www.lendingstandardsboard.org.uk/wp-content/uploads/2021/04/The-Standards-of-Lending-Practice-for-personal-customers-April-2021.pdf The standards for business customers were revised most recently in August 2020 (and contain temporary provisions relating directly to Covid) and are available at https://www.lendingstandardsboard.org.uk/wp-content/uploads/2020/08/Standards-of-Lending-Practice-for-business-customers-August-2020-Covid-update.pdf

[3] The April 2021 publication relates to the voluntary standards for personal customers, available at https://www.lendingstandardsboard.org.uk/wp-content/uploads/2021/04/The-Standards-of-Lending-Practice-for-personal-customers-April-2021.pdf The same phrase is contained in the August 2020 standards for business customers, available at https://www.lendingstandardsboard.org.uk/wp-content/uploads/2017/03/standards-of-lending-practice-business.pdf

[4] Department for Digital, Culture, Media and Sport, *A New Data Protection Bill: Our Planned Reforms Statement of Intent* (7 August 2017) at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/635900/2017-08-07_DP_Bill_-_Statement_of_Intent.pdf

Act was initially read in conjunction with the EU GDPR, but on 1st January 2021, when the UK formally exited the EU, the Act was amended, and the UK GDPR came into force.[5] Some of the key developments are as follows:

- The definition of 'personal data' contained in the UK Data Protection Act 1998 has been broadened to reflect the growth and development of technology in recent decades. For example, personal data now encompasses IP addresses and internet cookies.[6]
- A number of data subject rights have been introduced and enhanced including; the right to be notified by the controller or processor of a data breach[7]; the right to obtain confirmation from the data controller with respect to whether data concerning them is being processed, where and for what purpose (responses must be given within a month, generally without charge, and with additional information, such as data retention periods)[8]; the right to request, and in some cases require, companies to delete their personal data (this could include, for example, the right to request that media platforms delete all of someone's posts.[9]
- Higher financial penalties can now be imposed up to £17.5 million or 4% of a company's global turnover (whichever is higher).[10]

2.4.4.3 Qualifications to the duty

Duty to the public

Page 45

A more recent example is *Saab v Dangate Consulting Ltd.*[11] Here, the High Court held that the defendants, who had been employed by the owners of a bank to conduct an independent internal review of the bank following allegations of money laundering, had breached their duty of confidentiality to the bank when they disclosed material to the regulators and law enforcement agencies. In their defence, the defendants argued that they had found evidence of criminal dealings

[5] See The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019.

[6] Data Protection Act 2018 s3(2) and (3). An IP address is a unique string of numbers separated by full stops that identifies a device using the internet. An internet cookie is a small piece of data that is generated by a website and saved by your web browser, the purpose of which is to remember information about you.

[7] Ibid, s68.

[8] Ibid, s45.

[9] Ibid, s47-8.

[10] Ibid, s157. Previously the Information Commissioner could only impose fines up to £500,000, see Information Commissioner's Office *Data Protection Act 1998: Information Commissioner's guidance about the issue of monetary penalties prepared and issued under section 55C (1) of the Data Protection Act 1998* (December 2015) at https://ico.org.uk/media/for-organisations/documents/1043720/ico-guidance-on-monetary-penalties.pdf

[11] [2019] EWHC 1558 (Comm).

and therefore, not only were they compelled by law to disclose, but it was also in the public interest that they do so. Regarding the latter defence, they argued that the nature and seriousness of the criminal conduct found represented a threat, not only to the banking system itself, but to the safety and welfare of the general public, and therefore disclosure was justified. The High Court emphasised that a balancing exercise was required, 'weighing the public interest in maintaining confidence against a countervailing public interest favouring disclosure.'[12] On the facts, it was held that the conclusions of criminality reached by the defendants in their investigations were 'premature and speculative' and were therefore not sufficiently credible to found a public interest disclosure defence.[13]

Customer's Consent

Page 47

<START> Box 2.2. At a Glance: The Duty of Confidentiality

The duty of confidentiality is an implied term in the banker customer relationship as demonstrated in the leading case of Tournier.

- In terms of scope, the duty of non-disclosure extends to any information obtained by the bank regardless of its source; information remains confidential after the account is closed.
- There are other sources that serve to bolster the duty including The Standards of Lending Practice, 2020 and 2021; the Human Rights Act 1998; and the Data Protection Act 2018 and UK GDPR.
- There are four qualifications to the duty of confidentiality namely; compulsion by law; duty to the public; interests of the bank; and customer's consent.

<END>

2.4.5 Duty of care and other regulatory duties

2.4.5.1 Contract

Page 49

The question of whether a bank has breached its *Quincecare* duty of care has been litigated in two recent cases. In *Singularis v Daiwa*[14] the Supreme Court held unanimously that the defendant bank owed a duty, as per the *Quincecare* decision, not to execute an order if it had been put on enquiry that it was an attempt to misappropriate funds of the customer, and that the Bank had breached this duty. The claimant company was owned by Mr Al Sanea and was established to manage his personal assets. Mr Al Sanea also owned a substantial business group, the Saad group. In June and July 2009, the bank executed several payment requests totalling $204 million from the claimant company's client account at the bank, to Saad group companies. These payment instructions were authorised without further enquiry by the bank, despite the fact that the bank was aware of the dire financial straits of Mr Al Sanea and the Saad group, and other suspicious circumstances.[15] When the

[12] At paragraph 134.

[13] At paragraph 163.

[14] [2019] UKSC 50

[15] See paragraph 11.

company later went into liquidation, the liquidators sought repayment of the $204 million from the bank, claiming they had breached their *Quincecare* duty.

At first instance, the court found in favour of the company but awarded a 25% reduction for the contributory negligence of Mr Al Sanea. The Court of Appeal dismissed the bank's appeal and so the bank appealed to the Supreme Court. It was held that it was incontrovertible that there had been a clear breach of Daiwa's *Quincecare* duty to Singularis.[16] The issue for the Supreme Court was whether the fraud of Mr Al Sanea could be attributed to the company, thereby defeating the claim by the company on the grounds of illegality, lack of causation, or a countervailing claim in deceit against the company. On the facts, it was held that none of these defences were made out and that Mr Al Sanea's fraud could not be attributed to the company. The bank was therefore liable. This is an important decision in which the *Quincecare* duty is given Supreme Court approval. It demonstrates that a bank will face difficulty defending itself against a claim where a customer is known to be in serious financial difficulty.

More recently, the High Court has ruled that a banks *Quincecare* duty does not extend to situations where the customer is a victim of authorised push payment (APP) fraud (see Box 2.3). *In Philipp v Barclays Bank*[17] the claimant, Mrs Philipp, was deceived by fraudsters into making two international payments from her bank account in the belief that her money would be safe and that she was assisting an investigation by the Financial Conduct Authority and the National Crime Agency. As a result of this APP fraud, she lost £700,000. Mrs Philipp brought an action against the bank, arguing that they were liable to reimburse her for her losses because they had breached their *Quincecare* duty by not asking questions or investigating the recipient of the money. Judge Russen stated:[18]

> 'The Quincecare duty is a common law duty which rests upon the more general concept of a bank adhering to standards of honest and reasonable conduct in being alive to suspected fraud…I do not accept that the Quincecare duty can properly be used to impose a higher (or more specific) set of standards which dictate that, in certain defined circumstances, the bank is obliged to question the customer's instructions. It is a duty of care framed by concepts of knowledge (actual or constructive) rather than further negligence in failing to follow the rules of some code. If a bank is to be held to the standards of something equivalent to a code for intervention – for present purposes, in the case of suspected APP fraud - then it needs to know its terms. There was no such code in March 2018[19] and the observation of May LJ in Lipkin Gorman is a clear indication that judges in later cases should not proceed as if a set of detailed rules had been laid down.
>
> In my judgment, the observations of Lady Hale in Singularis about the purpose of the duty…have no resonance where the cause of the customer's loss is her own desire to make the payments to their intended recipients. The Supreme Court said nothing about a bank protecting an individual customer (and her monies) from her own intentional decision. If the Quincecare duty was to be supported by matters going beyond the honest and reasonable conduct of the ordinary prudent banker then in my judgment it would have to be by

[16] At paragraph 12.

[17] [2021] EWHC 10

[18] At paragraph 160-1.

[19] Such a Code was introduced in May 2019 but this was more than a year after these payments were made and in any event, as highlighted by the High Court, the code does not extend to international payments.

> reference to some form of industry-recognised rules from which a bank could identify the particular circumstances in which it should not act (or act immediately) upon its customer's genuine instructions.'

Judge Russon accordingly concluded that it 'would not be fair, just or reasonable' to impose liability on the bank and to do so would amount to an 'unprincipled and impermissible extension of the Quincecare duty.'[20]

<START> Box 2.3. Banking in Practice: Authorised Push Payment Fraud

'Push payments' occur when a customer instructs their bank to send funds to another person's account, typically via the CHAPS, Bacs, or Faster Payments settlement systems (see Chapter 3.4.3). An authorised push payment (APP) is one where the customer has consented to the payment being made. An APP scam occurs when someone is tricked into making a payment to a fraudster. According to the Payment Systems Regulator, APP scam losses for the first half of 2020 alone totalled £208 million.[21] There are eight main types of APP scam:[22]

1. Purchase scam: The victim pays in advance for goods or a service that they never receive.

2. Investment scam: A fraudster convinces the victim to move their money to a fictitious fund or to make a fake investment.

3. Romance scam: The victim is persuaded to make a payment to a fraudster they have met, normally online via social media or a dating app, and with whom they believe they are in a relationship.

4. Advance fee scam: A fraudster convinces the victim to pay a fee which they claim will unlock a much larger payment, or some high value goods.

5. Invoice and mandate scam: The victim attempts to pay an invoice to a legitimate payee, but the fraudster intervenes and convinces the victim to redirect the payment to an account they control.

6. CEO fraud: A fraudster impersonates a CEO or other high-ranking official of the victim's organisation and convinces the victim to make a payment to an account they control.

7. Police/bank staff impersonation: A fraudster contacts the victim purporting to be from the police or the victim's bank and convinces the victim to make a payment to an account they control.

8. Other impersonation: A fraudster claims to be from an organisation such as a utility company, communications service provider or government department and convinces the victim to make a payment to an account they control.

[20] At paragraph 184.

[21] Payment Systems Regulator, 'Authorised push payment (APP) scams: Call for views' (Feb 2021) CP21/3 available at https://www.psr.org.uk/media/5yvpidyc/psr_cp21-3_app_scams_call_for_views_feb-2021.pdf

[22] Ibid.

In contrast to victims of unauthorised transactions, such as where a victim's account is hacked, under existing arrangements victims of APP fraud have no statutory protection.[23]

<END>

2.4.5 Duty of care and other regulatory duties

2.4.5.3 Regulatory duties

Page 53

In February 2021, the FCA provided further guidance on what firms need to do to comply with their obligations under the Principles to ensure, in particular, that they treat vulnerable customers fairly.[24] The FCA have made it clear that protecting vulnerable customers is a key focus, and it has increased in significance in light of the ongoing Covid-19 pandemic.

[23] Note that the industry launched a voluntary code, the 'contingent reimbursement model (CRM) code' on 28th May 2019 which set new standards for the prevention of APP scams and provided guidance on how victims should be treated and reimbursed. An overarching principle of the CRM Code is that customers should be reimbursed where they have acted appropriately. The Payment Systems Regulator has been measuring outcomes, and in February 2021 concluded that the Code has not gone far enough to significantly reduce APP scam losses. Accordingly, the PSR has invited views on three new measures that could help prevent APP scams and protect victims. See 'Authorised push payment (APP) scams: Call for views' ibid.

[24] Financial Conduct Authority, *'FG21/1 Guidance for firm on the fair treatment of vulnerable customers'* (February 2021) available at https://www.fca.org.uk/publication/finalised-guidance/fg21-1.pdf