BCLP. Client Intelligent

BankBCLP

BANKING BITES – MAY 30 2022

May 30, 2022

SUMMARY

This edition of Banking Bites provides updates on:

1. Privy Council rules against extension of the Quincecare duty
2. No privilege protection for the identity of the person communicating with solicitors
3. Payment Systems Regulator fines NatWest Group £1.82m for overcharging interchange fees on credit cards
4. EU member states reach deal to bolster cybersecurity rules
5. Financial Conduct Authority commits to removing unused regulatory permissions
6. Lessons Learned: Knowing your customer processes remains key FCA focus for challenger banks
7. The Wolfsberg Group releases FAQ guidance on negative news screening
8. FCA encourages reporting on sanction evasions or control issues

1. PRIVY COUNCIL RULES AGAINST EXTENSION OF THE QUINCECARE DUTY

Does a bank owe a duty of care to a person who is the beneficial owner of funds held in the account of a customer of the bank and who has been defrauded by that customer? This decision seeks to answer that question. It was a judgment by the Privy Council in proceedings that had originally been brought in the Isle of Man. However, it is nevertheless interesting and potentially persuasive. The Privy Council answered the question in the negative, rejecting the fund's argument that such a duty of care was already established in law on the basis of a case called *Quincecare*. The appellate court disagreed – there was nothing in case law which supported the argument that the duty extended beyond that owed to a bank's customers and there would potentially be "radical implications" if it were to be accepted by the courts that such a duty extended to a beneficiary who sits behind the

bank account customer. The judgment is another example of how, in light of recent case law, parties are continuing to try and expand the scope of the a bank's duty to spot, stop and compensate fraud on or by its customers.

Please contact Andrew Tuson if you have any questions.

2. NO PRIVILEGE PROTECTION FOR THE IDENTITY OF THE PERSON COMMUNICATING WITH SOLICITORS

In a recent judgment, the UK's High Court has considered whether the identity of those authorised to give instructions to solicitors on behalf of a corporate is itself subject to litigation privilege under English law. The judgment confirms that, in some cases, the question of who gives instructions to the lawyer may trespass into an answer to the question of the content of those instructions. It is important to consider who is the client for the purposes of legal professional privilege and the judgment highlights some of the sensitivities around the roles of individuals in the client group. Where there is a risk that disclosure of the identity of the specific individual involved might lead to disclosure of the nature of the communications or advice given, further care must be taken to protect the privilege in the communications.

Please contact Oran Gelb with any queries.

3. PAYMENT SYSTEMS REGULATOR (PSR) FINES BANKING GROUP £1.82M FOR OVERCHARGING INTERCHANGE FEES ON CREDIT CARDS

Four banks have been issued with fines totalling £1.82m for overcharging interchange fees on cards. The initial investigation was launched four years ago, after the UK's PSR found issues during routine monitoring. The four banks were found to have incorrectly treated a number of cards as being commercial cards when they should have been treated as consumer cards. This meant that fees charged by these banks were not capped and were set at too high a level. As a result, this led to merchants' banks (and, ultimately, merchants) being overcharged. While the banks eventually closed the consumer card accounts and reimbursed the excess fees they had received, the PSR concluded that the banks should have acted more swiftly to comply with the interchange fee regulation. For those with exposure to its remit, the decision serves as a useful reminder of the importance of keeping abreast of the latest PSR guidance in order to ensure compliance, particularly in light of regular PSR monitoring.

Please contact Polly James if you would like more information on this.

4. EU MEMBER STATES REACH DEAL TO BOLSTER CYBERSECURITY RULES

On 13 May, the EU Parliament and member states came to a tentative agreement on new cybersecurity rules and information systems. The new NIS 2 Directive will require medium-sized and large entities from sectors that are critical to the economy and society (including banks and energy

services) to take certain cybersecurity risk management measures. According to the Commission, the directive is intended to increase information-sharing and cooperation on cyber crisis management on the national and EU level, while imposing additional cybersecurity requirements on companies and tackling security vulnerabilities in the supply chain.

NIS 2 will also impose a minimum list of basic security elements that companies would have to implement; create more precise requirements for the process and timeline for reporting cyber incidents; and require individual companies to address cybersecurity risks in the supply chain and supplier relationships. Member states, in conjunction with the Commission and the EU Agency for Cybersecurity, would also be empowered to carry out coordinated risk assessments of critical supply chains, and national data protection authorities would be handed enhanced powers, including the ability to impose administrative fines of up to €10 million or 2% of a company's total global revenue, whichever is higher.

5. FINANCIAL CONDUCT AUTHORITY (FCA) COMMITS TO REMOVING UNUSED REGULATORY PERMISSIONS

The UK's financial services regulator, the FCA, has issued a press release warning that it intends to use new powers to more swiftly cancel or change what regulated activities firms are permitted to carry out. The new powers are set out in Policy Statement PS22/5 and allow the FCA under Schedule 6A FSMA 2000, to cancel or vary a firm's Part 4A permission. The FCA will now be able to cancel a permission, or change it, 28 days after the first warning if the firm has not taken appropriate action. The hope is that this will strengthen consumer protection by reducing the risk of consumers misunderstanding or being misled about their exposure to financial risk and how much consumer protection they have. The press release is a reminder that FCA regulated firms should regularly review their permissions, ensure they are correct, and they are acting in accordance with them. If certain permissions are not needed or used, firms should seek to cancel them promptly.

Please contact Polly James or Joanna Munro should you wish to discuss.

6. LESSONS LEARNED: KNOWING YOUR CUSTOMER PROCESSES REMAINS KEY FOCUS FOR CHALLENGER BANKS

Our recent experience of working with challenger banks suggests that the UK's financial services regulator is strongly focused on ensuring that effective KYC processes are being implemented. In particular, the FCA has referred to customer video selfies being useful in enabling banks to flag human trafficking concerns to the relevant authorities. The FCA has also made clear that no matter how good a transaction monitoring system is, firms must still comply with the relevant customer due diligence requirements. There is also an expectation for challenger banks that any enhanced due diligence measures should be contained in a written document, as opposed to being stored as code.

Please contact Siân Cowan if you have any questions.

7. THE WOLFSBERG GROUP RELEASES FAQ GUIDANCE ON NEGATIVE NEWS SCREENING

The Wolfsberg Group has released FAQ guidance to assist financial institutions in creating a negative news screening framework in support of financial crime risk management. Implementing an effective negative news screening framework can help financial institutions to understand who they are doing business with and the risks to which they are exposed. While there is no universally accepted definition of what constitutes negative news, it can be broadly defined as information available in the public domain which financial institutions would consider relevant to the management of financial crime risk. As well as helping financial institutions to better understand who they are doing business with, negative news screening can also add value in the followings ways:

- reveal involvement in criminal activity which may determine the need for additional due diligence and/or targeted reviews of past transactional activity;
- provide additional context to support an investigation into potentially suspicious activity; and
- help to identify potential risks with respect to a customer's source of wealth and/or source of funds narrative.

Please contact Oran Gelb for further information.

8. FCA ENCOURAGES REPORTING ON SANCTION EVASIONS OR CONTROL ISSUES

The UK's FCA has issued a press release encouraging reporting about sanctions evasion or control issues where they relate to firms on the Financial Services Register, other FCA registers, or companies with UK listed securities. The main areas of focus for the FCA are broad and cover:

- any suggestion that firms have poor sanctions controls;
- suspected breaches of the sanctions regime;
- actual breaches on the sanctions regime; and/or
- any method which is being used by firms or individuals to breach the sanctions regime.

When reporting to the FCA on these issues, it is important that firms comply with any statutory legal disclosure, reporting and data protection requirements they may have and consider carefully whether any other relevant supervisor authority or professional body should also be made aware of the potential disclosure.

Please contact Joseph Ninan if you would like to discuss this further.

RELATED PRACTICE AREAS

- Fintech
- Financial Regulation Compliance & Investigations
- White Collar
- Business & Commercial Disputes
