KEY POINTS

- If there is uncertainty about what a customer's balance is, the quantum of debt owed by the bank to its customer would have to be proven through evidence.
- The Financial Services Compensation Scheme can choose to pay an eligible claimant even if it cannot properly prove the amount owed.
- However, various customer groups would remain at risk.

Spotlight

Authors Raymond Cox QC and Liisa Lahti

Cyber-attacks on banks: the consequences of a loss of access to bank records

In this Spotlight article, the authors speculate on the legal and regulatory consequences of a cyber-attack in which customer credit balances have been misappropriated *and* the bank is no longer able to access computer records including archives of accounts held by it.

In late 2016, cyber-criminals hacked Tesco Bank's online banking computer system and transferred £2.5m from the current accounts of 9,000 customers. The details of the attack are not yet clear. However, on the basis of the media coverage into the incident it is understood that the cyber-criminals were able to hack into Tesco bank's online banking system via an online banking app and were able to transfer sums out of customers' accounts without their knowledge or assistance.

Similarly in 2014 approximately 83 million accounts were compromised by hacking into accounts of JP Morgan. JP Morgan has stated that login information associated with the accounts (such as social security numbers or passwords) was not compromised but names, email and postal addresses, and phone numbers of account holders were obtained by hackers. It is unclear how. Some sources have stated that there may have been phishing (fraudulent emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers).

Other cyber-attacks on financial institutions and especially hospitals have involved ransomware, ie software deployed under a threat to destroy or deny the use of computer systems unless a ransom is paid.[1]

In these circumstances, it does not appear fanciful to suppose that a bank or other financial institution may one day face a situation in which customer credit balances have been misappropriated *and* it is no longer able to access computer records including archives of accounts held by it. This may truly be described as an end of the world, Armageddon scenario for the bank. In this article we speculate on the legal and regulatory consequences of such a loss of funds and bank records. Although the landscape of possible scenarios is very broad, and the survey can only be general, there are some features which stand out, in particular the importance of the bank's terms and conditions providing so far as possible for the consequences of such an attack.

THE STATE OF THE CUSTOMER ACCOUNT

If the bank has no computer record of the state of the bank account at any given time, there is an immediate question, as between the bank customer, as to what is the true amount owing either way.

In reality, the bank will no doubt have back up or archive records at a separate location. However if access to these has been denied the position is rendered even more difficult. The equivalent situation could have arisen before internet banking if there was a flood or fire at the bank that destroyed its hard copy records and any back-ups, although we are not aware of any law reports arising from such a case.

A credit balance on a bank account is a debt owed by the bank to its customer.[2] Therefore if there is uncertainty about what that balance is, the quantum of the debt owed by the bank to its customer would have to be proven through evidence – and the normal rules of evidence would apply. In those circumstances even if a bank may accept that it is required to refund the balance on the customer's account immediately before the attack it may be unable to ascertain what that balance is. If the customer has recent paper records the position is straightforward. The customer can prove how much the bank owes it by reference to those paper statements. However, many customers opt out of paper statements or the latest statement may be a month (or more) out of date.

In most cases of a "pure hack" (where the customer has not divulged sensitive information to the criminal) the bank will be liable to refund the customer the amounts lost. The payment(s) are unauthorised and therefore the bank is liable to refund the customer pursuant to the Payment Services Regulation 2009 (Reg 61) and the common law. The provisions of the PSR would most likely be reflected in the bank's terms and conditions thereby giving rise to a claim in damages for breach of contract as well.

> ... if there is uncertainty about what [the] balance is, the quantum of the debt owed by the bank to its customer would have to be proven through evidence ...

CONSEQUENTIAL LOSS

Further, if the bank's security systems were to blame in that they allowed the attack to occur then the bank might arguably also be liable in negligence, or for breach of duty, to its customers.

The bank owes a duty to provide reasonable skill and care in providing a service pursuant to s 13 Supply of Goods and Services Act 1982. Subject to the precise terms and conditions in place, a customer may also seek to make a claim

in damages for any consequential loss suffered, though there would no doubt be extensive argument about precisely what the bank should have done in order to meet requirements imposed on the bank with regard to its security systems. This is a developing area of the law, and there are not standardised requirements imposed on banks with regard to their security systems. In addition, cyber fraud is a moving target and the risks as well as the responses change and develop over time. It is therefore difficult to impose detailed standard requirements on banks in terms of what security measures they are obliged to have in place at any given time.

unlikely that a customer borrower of the bank could rely on this to avoid paying back a loan to the bank – the clause would be likely to refer to a material adverse change in the customer's ability to repay the bank rather than the other way around. The bank could seek to rely on the MAC though that would prove difficult if the reason why the customer's ability to repay the loan had materially changed was a third party hacking into the bank's systems. Difficult questions would arise about whether the bank was relying on its own wrong.

However, the wiping out of account balance records could trigger a MAC in loans as between banks. If a bank is itself a borrower, and subject to a cyber-attack which empties customer accounts and destroys records, it is not difficult to see that a MAC in the terms on which the victim bank is borrowing funds may be engaged, worsening the financial position of the victim bank.

> … however the wiping out of account balance records could trigger a MAC in loans as between banks.

There is also optional non-mandatory guidance such as:

- the International Organization for Standardization (ISO) compliance standards on a range of areas, including information security and risk management;
- the International Chamber of Commerce (ICC) cybersecurity guide; and
- the Department for Business Innovation and Skills (BIS) published cybersecurity guidance for businesses.

Although general in terms, such guidance may be relevant to the consideration of the duties of banks in operating accounts.

OTHER TRANSACTIONS

In addition to having an impact on individual bank accounts, ignorance of the true state of an account could affect a whole host of other obligations such as borrowing and LTV covenants in loan and security contracts, simply because the parties may not know or be in dispute as to whether or not clauses apply because the state of the account is uncertain.

Further, the wiping out of account balance records could trigger material adverse change (MAC) clauses in loans and other equivalent documents. It seems

COMPENSATION FOR CUSTOMERS

A further issue arises if the bank cannot repay its customers. It is possible for a hacker to have an impact on a large number of customers in one attack. The attack on JP Morgan is an example of such a situation – approximately 83 million accounts were compromised. Indeed, the chairman of the UK's National Cyber Management Centre (NCMC) has warned that a major bank will fail as a result of a cyber-attack in 2017.

Those customers who are "eligible claimants" under the Financial Services Compensation Scheme (FSCS) can claim under the scheme up to a certain amount (at the time of writing this is understood to be £85,000).

However in order to claim under the scheme, the claimant must satisfy the relevant criteria. The bank needs to be "in default" (COMP 6.3.1R) essentially this means that the bank must be "unable or likely to be unable to" satisfy claims". Further, the claimant must be an "eligible claimant" (COMP 4.2.1R). This essentially means individuals, small companies and small charities.

The amount that could be claimed under the FSCS is provided as follows:

> "amount of compensation payable to the claimant in respect of any type of protected claim is the amount of his overall net claim against the [bank]."

This would certainly include the balance on the account immediately before the hack. In calculating the amount,

> "the FSCS may rely, to the extent that it is relevant, on any determination by: (1) a court of competent jurisdiction; (2) a trustee in bankruptcy; (3) a liquidator; (4) any other recognised insolvency practitioner; and on the certification of any net sum due which is made in default proceedings of any exchange or clearing house" (COMP 12.2.6)

"Claim" is defined as "a valid claim made in respect of a civil liability …". Therefore the claimant can claim whatever it can prove was the balance on the account immediately before the hack as well as any recoverable consequential losses, which indicates the usual burdens of proof etc.

Interestingly COMP states that (COMP 12.2.10):

> "(1)The FSCS may pay compensation without fully or at all investigating the eligibility of the claimant and/or the validity and/or amount of the claim notwithstanding any provision in this sourcebook or FEES 6 to the contrary, if in the opinion of the FSCS: (a) the costs of investigating the merits of the claim are reasonably likely to be disproportionate to the likely benefit of such investigation; and (b) (as a result or otherwise) it is reasonably in the interests of participant firms to do so … ."

Therefore the FSCS can choose to pay an eligible claimant even if it cannot properly prove the amount owed. This may become

Biog box

Raymond Cox QC is a barrister specialising in banking and financial services law at Fountain Court Chambers and co-editor of "The Law of Bank Payments". Email: rc@fountaincourt.co.uk

Liisa Lahti is a barrister practising from Quadrant Chambers specialising in banking, financial services and international trade. Email: liisa.lahti@quadrantchambers.com

relevant in the situation set out above, where the bank's records are also tampered with by the hacker. Needless to say, the FSCS is not *obliged* to take this more relaxed approach to evidential matters.

However various customer groups remain at risk, namely:

- individuals and small companies that have lost more than £85,000 and wish to reclaim the rest of the sums; and
- claimants who do not satisfy the requirements of "eligible claimant" under COMP (larger companies and charities for example).

In our view, those claimants would be left to claim against the bank in question in court (or prove in its insolvency). The bank's former customers would end up seeking to enforce against the bank's assets and/or debts (via a third party debt order).

THE REGULATORY POSITION

Under EU regulations due to come into force on 25 May 2018, a bank will have to report incidents where its data security measures have been breached, and will be liable to a fine of up to 2% of global turnover for non-compliance (the General Data Protection Regulation 2016/679).

Under existing regulation, banks are regulated by the Financial Conduct Authority (FCA), and various provisions of the FCA Handbook either directly or indirectly relate to data security and cybersecurity measures. The Principles for Business (PRIN) as well as responsibility standards for senior management and directors (Senior Management Arrangements Systems and Controls (SYSC)) are potentially relevant. For example, SYSC contains provisions about systems and controls (SYSC 3) and risk control (SYSC 7) which are potentially relevant, and the third Principle for Business (PRIN 2.1.1) requires a firm to "take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems."

Breaches of requirements imposed by the FCA can result in fines and enforcement action by the FCA against the bank in question. For example in July 2009, the (then) FSA fined three HSBC firms £3m for data security failings, including not having adequate systems and controls in place to protect their customers' confidential details from being lost or stolen in breach of Principle 3 of the FSA's Principles of Business (PRIN). Among other things, unencrypted customer details had been sent to third parties via post/courier and on two incidents had been lost in the post. Other potentially relevant regulation includes the Data Protection Act 1998. ■

1 Federal Financial Institutions Examination Council Statement on Cyber Attacks Involving Extortion, 3 November 2016 https://www.ffiec.gov/press/pr110315.htm

2 *Foley v Hill* (1848) 2 HL.

Further Reading:

- What can be done to mitigate cyber risk? [2015] 6 JIBFL 353.
- Protecting the bank's position when customers fall hook, (on)line and sinker for vishing frauds [2014] 8 JIBFL 540.
- LexisPSL: Corporate: Keeping corporate and financial information safe from cyber-criminals.