BOS Banking Ombudsman Scheme

Quick Guide

Privacy and confidentiality

7 August 2017

Banks have a legal duty to protect the confidentiality of existing and former customers. Banks also have obligations under the Privacy Act 1993. The Act has 12 privacy principles about personal information. In the banking context, these govern:

- banks' collection and storage of customer information
- customers' rights to access and correct information about themselves
- the disclosure of personal information.

We can consider complaints about breaches of privacy and duty of confidence. Sometimes we refer a privacy complaint to the Office of the Privacy Commissioner if we consider it would be better dealt with by that office. An example would be if a customer sought compensation that exceeded our limit.

Concepts similar, but not the same

A duty of confidence and the legal obligation to protect privacy are similar, but not the same. The former applies to information about individuals and businesses, the latter to information about individuals only (and that includes bank staff). If a complaint requires us to look into the behaviour of a staff member, we can ask the bank to tell us what systems or process changes it has put in place to correct a problem, but we cannot seek information about any disciplinary or other action the bank may have taken against that individual.

Disclosing confidential information

There are four broad situations in which a bank can lawfully disclose confidential information:

When the law compels it to: Banks sometimes have to give evidence about a customer's affairs in court. Banks can also be required to give information to the Inland Revenue Department (under the Tax Administration Act 1994), to the Ministry of Social Development (under the Social Security Act 1964) and to a company liquidator (under the Companies Act 1993). Banks are also required to report suspicious transactions to Police (under the Financial Transactions Reporting Act 1996 and Anti-Money Laundering and Countering Financing of Terrorism Act 2009).

When it has a public duty to: This applies when there is a danger to the state or when the wider public needs protection against crime. A bank needs to balance the public interest with respecting a customer's right to privacy when it considers providing information about that person to a third party.

When a bank must disclose information to protect its interests: This applies when a bank takes legal action against a customer (such as to recover a debt), or defends an action from a customer and needs to provide information about the customer's affairs.

When a customer agrees: A bank can disclose customer information if the customer agrees. A bank must ensure the information is correct and within the scope of the customer's consent. A customer may, for example, agree to the bank's disclosure of information about one account only. If the bank releases information about other accounts, it has breached its duty of confidence.

When a bank breaches confidentiality or privacy

If we consider a complaint about breach of confidence or privacy to be valid (whether accidental or deliberate), we assess whether this has resulted in a direct financial loss to the customer and, if so, award compensation. We also look at whether the customer has suffered distress, embarrassment or inconvenience. We must be satisfied any distress, embarrassment or inconvenience warrants a compensation payment. Sometimes customers submit substantial claims for minor frustration or inconvenience. We are unlikely to award compensation for minor mistakes that have little or no harmful effects.

Case 1: Employee's viewing ruled a breach

Mrs K's former husband was in a relationship with a woman who worked at Mrs K's bank. Mrs K asked the bank if the woman was viewing her banking details. It confirmed the employee had done so some months earlier.

The bank undertook disciplinary action against the woman, but could not disclose what steps it had taken, because this would have breached the employee's privacy. The bank offered Mrs K $550 in recognition of the stress caused by the breach. Mrs K considered the offer was too low because she had had recent fears for her safety.

We consulted the Privacy Commissioner about Mrs K's case. We considered the bank's offer was reasonable. The breach had happened some months earlier, before Mrs K had moved house. The compensation would have been greater if the breach had compromised Mrs K's safety. Mrs K accepted the offer.

Case 2: Misdirected mail led to compensation offer

Mrs J's bank accidentally sent her savings account statements to her previous address. Mrs J's friend lived there and opened them. Mrs J was embarrassed because she had recently told her friend she did not have enough money to give him a loan, but the statements showed otherwise. Mrs J

contacted us seeking financial compensation from the bank for damage to the relationship with her friend.

We explained that it was her friend who had acted inappropriately by opening and reading her mail. The Postal Services Act 1998 makes it an offence to wilfully, and without reasonable excuse, open mail addressed to someone else.

The bank offered Mrs J $500 compensation in recognition of stress and inconvenience caused by its failure to send the statements to the correct address. We told Mrs J the offer was reasonable and she should accept it. She did.

Case 3: Scope of medical notes too wide

Mrs C bought a life insurance policy with death and terminal illness benefits through her bank. Eight years later, she was diagnosed with a serious illness and lodged a terminal illness benefit claim. The bank asked Mrs C to authorise the release of her medical information. She agreed. The bank asked her doctors for full medical records going back two years. After assessing Mrs C's records, the bank declined her claim, saying she had a serious, but not terminal, illness.

Mrs C complained about the bank's collection of two years of medical records, saying she thought it would collect information only about the diagnosed condition. She did not believe the bank needed the other medical information to assess her claim, and thought it had collected more personal information than was necessary. She felt embarrassed and humiliated.

The bank said its standard practice was to seek information covering a certain period of time. It needed to understand pre-diagnosis events to help assess a claim.

We considered Mrs C's complaint in light of a review in 2009 by the Office of the Privacy Commissioner into insurers' collection of medical notes. Its report noted the tension between insurers' legitimate need for detailed medical information to make claims decisions and an individual's right to privacy.

We looked at whether Mrs C had authorised the collection of full medical notes for two years, and whether that collection was necessary to make a decision on her claim.

We were not satisfied Mrs C had authorised the collection of full medical notes. In our view, a claimant would reasonably infer from the bank's authority form that the bank would collect only information relevant to the condition in question. The bank accepted our finding, and undertook to review the information it requested of health insurance claimants.

We were also not satisfied it was necessary to collect full medical records to evaluate Mrs C's claim. Certainly, the period leading up to a diagnosis can contain medical information of relevance to an insurer, but we considered the bank could have obtained this by requesting pre-diagnosis investigations and symptoms notes. The bank did not accept our findings and did not give its reasons.

We accepted Mrs C had been shocked and upset at discovering the scope of the bank's information collection and recommended compensation of $850. Both parties accepted this recommendation.