



Case study: Loan Application

LOAN APPLICATION RESULTS IN SERIOUS PRIVACY BREACH

Themes: Data privacy breach, inadequate internal controls; exceptional distress and inconvenience award

This complaint related to the completion of a personal loan application which resulted in a data breach by an employee of the loan company.

In March 2018, Miss L applied for a loan from a finance company (FC) and provided the necessary application documentation, which included bank statements. In September 2018, Miss L no longer wished to continue with the loan, and FC closed the file.

In August 2019, Miss L re-applied for the loan from FC and an employee, who was personally acquainted with Miss L, was involved in processing the loan application.

This employee accessed information from the previous loan application made in March 2018. The employee noted a bank statement showing a transaction which was referenced "Aids treatment". Taking this information, the employee contacted Miss L's former boyfriend to ask about his relationship with Miss L and commented on the possibility Miss L may have acquired immunodeficiency syndrome (AIDS). The FC employee also divulged this information to other third parties. It became clear that the bank statement transaction reference had been meant as a joke by the former boyfriend (at that time) of Miss L.

Miss L complained to FC and the local data protection regulator requesting a thorough investigation and compensation due to her inability to work as a result of the extreme stress this situation had caused her.

FC confirmed that as soon as Miss L notified them of the issue, they raised an investigation into the circumstances of the situation. In August 2019, FC reported the data breach to the relevant authority and suspended the offending employee, who resigned the next day. FC believed that the privacy breach and the impact it had on Miss L was not a result of their wrongdoing or a failure of process by them, but rather the rogue actions of the employee. In their final response letter to Miss L, FC confirmed that her complaint had been upheld, but offered no compensation or any explanation as to what had caused the incident.

Miss L brought the complaint to CIFO. CIFO investigated and found that FC should not have retained the bank statements from the original application in March 2018 which held the transaction reference shared by the employee. CIFO also concluded that, although this privacy breach and its implications were clearly due to the employee's outrageous conduct, FC should have had policies and procedures in place to better ensure that information was not retained inappropriately and that such a privacy breach could not occur.

CIFO upheld this complaint and concluded that FC should pay a total of £20,354.60 in compensation to cover Miss L's loss of earnings with 8% simple interest, medical bills with interest, and including a substantial award for an extreme level of distress and inconvenience of £10,000.