Case study: Banking / Credit

FRAUDULENT ACTIVITY WENT UNCHECKED LEADING TO REIMBURSEMENT

Themes: Payment card fraud, customer responsibility for care and control of card and PIN, internal fraud controls, failure to mitigate loss

Mr B claimed to be the victim of a fraud in Hong Kong when a bank card he used exclusively to make payments on a UK mortgage was stolen. Mr B did not realise the card had been stolen as it was always kept in a safe in his residence along with the PIN code provided by the bank. The card, and the safe it was stored in, were rarely checked due to their limited purpose. The unique circumstances which led to the thief gaining access to Mr B's home safe, while very interesting and illustrative of the risks of being administered with debilitating drugs in public drinking establishments, were determined by the CIFO case handler as not relevant to the question of responsibility for the losses incurred given the specific circumstances of this complaint.

Immediately following the theft of the card and PIN, there were a series of unusual transactions, including purchases from high-end fashion and beauty establishments, and withdrawals of cash over the course of a month, however Mr B was only made aware of the situation after a total of 73 suspicious transactions had already occurred, totalling £34,015.60.

The bank refused to release Mr B of responsibility for the losses on the basis that Mr B had breached the terms and conditions of his account by storing the PIN code with the card and not destroying the record of the PIN. Mr B complained to CIFO.

CIFO reviewed the bank's internal fraud control records and discovered that the bank was alerted by its own internal fraud control systems to various of these fraudulent transactions 22 times during the period when the transactions took place. Two of those fraud alerts were triggered on the first day the transactions commenced after the theft of the card and PIN. However, the bank took no action. When the bank did finally contact Mr B, it was due to insufficient funds in his account to cover the transactions, not the fraud alerts that had been raised repeatedly by the bank's own internal fraud control systems due to the unusual transaction activity on the account.

Conclusion

Regarding the breach of the terms and conditions of his account, Mr B did clearly breach them through having the PIN number written down in the same location as the card. This was not in dispute. However, Mr B did appear to be the victim of a genuine fraud and the bank failed to either block his card or notify him of the suspicious transactions, which did not fit the normal profile of transactions on his account. The CIFO case handler concluded that the lack of action in response to the internal fraud alerts on the first day the fraudulent transactions started was a serious failure by the bank. Had the bank acted on its own internal fraud alerts, it could have prevented most of the fraud losses.

CIFO decided to partly uphold the complaint and have the bank release Mr B from liability for all amounts lost to the fraudulent transactions after the first day when the two internal fraud alerts were generated and not acted upon. Both parties accepted this decision and the file was closed.