GAPS IN CYBER RISK COVERAGE

LESSONS FROM PF CHANG'S CHINA BISTRO V FEDERAL INSURANCE CO

A judgment given on 31 May 2016 in the Federal District Court in Arizona illustrates the gaps that can arise between the exposures that a business faces in relation to cyber risks, on the one hand, and the insurance coverage purchased, on the other.

Facts of the case

Federal had issued a CyberSecurity policy to Chang for 12 months from 1 January 2014. On its website, Federal marketed this policy as "a flexible insurance solution designed by cyber risk experts to address the full breadth of risks associated with doing business in today's technology-dependent world" that "covers direct loss, legal liability and consequential loss resulting from cyber security breaches".

Chang, which operated a chain of restaurants, conducted more than six million transactions a year with customers using credit cards.

On 10 June 2014, Chang learned that computer hackers had obtained and posted on the internet approximately 60,000 credit card numbers belonging to its customers. Chang notified Federal of the data breach and subsequently sought an indemnity under the policy for its losses arising from the security compromise.

Federal reimbursed Chang more than US$1.7m under the policy for costs incurred as a result of the data breach. These costs covered a forensic investigation into the breach and also defending proceedings brought by customers whose credit card information had been stolen, as well as proceedings brought by a bank that had issued credit card information which had been stolen.

However, Chang sought to recover in respect of other financial loss that it had suffered. Chang, along with many other merchants, are unable to process credit card transactions themselves. Such merchants have to enter into agreements with third party "servicers", who process the transactions with the banks that issue the credit cards.

Chang entered into a Master Service Agreement ("MSA") with Bank of America Merchant Services ("BAMS"), pursuant to which BAMS would process credit card payments made by Chang's customers.

BAMS performs its processing obligations pursuant to agreements with the credit card associations ("Associations"), like MasterCard and Visa. BAMS' agreement with MasterCard is governed by the MasterCard Rules, these being incorporated into the MSA with Chang.

Under the MasterCard Rules, BAMS is obliged to pay certain fees and assessments ("Assessments") to MasterCard in the event of a data breach. The MSA provided that BAMS could pass through to Chang any fees, fines, penalties and assessments imposed on it by the Associations.

Following the data breach, MasterCard imposed three Assessments on BAMS:

- A fraud recovery assessment of US$1,716,799 for costs associated with fraudulent charges from the security compromise.
- An operational reimbursement assessment of US$163,122 for the cost of notifying cardholders and reissuing and delivering payment cards, new account numbers and security codes; and
- A case management fee of US$50,000, being a flat fee relating to Chang's compliance with payment card industry data security standards.

Whether claims for injury to a third person's records were covered

Chang claimed that it was entitled to be indemnified for the fraud recovery assessment under Insuring Clause A of its CyberSecurity wording. This provided that Federal would pay for "Loss on behalf of an Insured on account of any Claim first made against such Insured … for Injury". "Injury" included "Privacy Injury", which was defined to mean injury sustained by "a person" because of access to that person's "record". "Record" included any private personal information held by the insured or on behalf of the insured by a third party service provider.

Federal's Defence, upheld by the court, was that the relevant "person", in this case BAMS, had not sustained a privacy injury. Only the person whose record was accessed without authorisation suffered a privacy injury. It was not BAMS' records, but the records of the banks that had issued the credit cards, that had been compromised during the data breach. Thus, BAMS had not made a claim against Chang of a type covered under the Insuring Clause.

Whether privacy notification expenses could be recovered

Chang argued additionally that, under Insuring Clause B, Federal had agreed to pay "privacy notification expenses" incurred by an insured resulting from privacy injury. These expenses were the reasonable and necessary costs of notifying persons directly affected by unauthorised access as well as the expense of changing account numbers, other identification numbers and security codes. Chang alleged that the

operational reimbursement assessment referred to above was a privacy notification expense because it related to the cost of reissuing bank cards, account numbers and security codes to Chang's customers.

Using a similar argument to that for Insuring Clause A, Federal contended that the operational recovery assessment was not personally incurred by Chang, but rather was incurred by BAMS. Federal also argued that there was no evidence that the assessment had been used to notify persons directly affected, or to change that person's account number.

On this occasion, the Court agreed with Chang. Although the operational reimbursement fee was originally incurred by BAMS, Chang was liable for it pursuant to its MSA with BAMS. In an earlier case (Samsel), the Supreme Court of Arizona had held that an insured "incurs" an expense when the insured becomes liable for the expense, "even if the expenses in question were paid by or even required by law to be paid by other sources".

In response to Federal's second argument, the Court accepted that MasterCard's Security Rules clearly stated that the fee was used to compensate for the cost of notification and Federal had not demonstrated that the fee had been used for any other purpose.

Exclusion for assumed contractual liability

However, Chang was ultimately unable to recover for these expenses under Insuring Clause B, because of a general policy exclusion that barred coverage for contractual obligations that Chang had assumed from a third party outside the Policy. The Court was unable to find any evidence indicating that Chang would have been liable for the Assessments, absent its agreement with BAMS. The Court held that Chang was a sophisticated party well versed in negotiating contractual terms, such that Chang could have included the coverages for which they contended in the Policy, had they so intended.

The moral

As more information emerges as to the type and nature of expenses that arise in the context of a cyber loss, risk managers will be expected to purchase coverages that reflect their organisation's exposures.

William Sturge
Partner

T: 0203 697 1904
M: 07957 794 557
E: william.sturge@cpblaw.com