



# DUAL

## CYBER CLAIMS EXAMPLES - SOCIAL ENGINEERING, PHISHING, PHREAKING & CYBER FRAUD

Profile	Background	Outcome
<b>Media</b>	A hacker impersonated a client of the Insured, using an identical email address. The hacker emailed the Insured advising that future payments should be made to a new bank account. When the Insured was due to pay the client, they paid SGD41,000 into the fraudulent account.	Indemnity was granted for the direct financial loss suffered by the Insured.  <b>Payment: SGD41,000.</b>
<b>Not for Profit</b>	The Insured engaged a third party supplier for assistance in marketing their organisation and gathering donor's information; including names, emails and phone numbers. The Insured was advised that the third party supplier's system was breached and data had been lost.	The Insured notified DUAL who appointed a law firm to advise in relation to the Insured's privacy legislation obligations. The Insured did not have to report the incident to the Personal Data Protection Commission based on individual circumstances and the IT data they had available to them. Payment was made in relation to the legal costs.  <b>Payment: SGD5,900.</b>
<b>Accountant</b>	The Insured's director noticed that some documents on their server had been deleted. Further investigations were undertaken and it was discovered a hacker had been accessing the Insured's system for the past 2 months.	The Insured notified DUAL who hired an IT Forensic Consultant to review the Insured's systems. It was discovered 800 client files had been accessed which included private details such as driver's licenses and passport numbers. DUAL appointed a specialist firm to monitor whether any client identities were stolen or sold as well as a law firm to advise on the data breach issues and draft a notification letter to all affected parties. It was determined that the Insured had to report the incident to the Personal Data Protection Commission and the appropriate steps were taken to secure the information they held. Remediation costs were also covered to rectify any issues with the Insured's system.  <b>Payment: SGD90,000.</b>
<b>Hairdresser</b>	The Insured uses a VoIP telephone system. A hacker gained access to the telephone system and made multiple unauthorised calls to a premium number over the course of a month. At the end of the month the Insured received their invoice, which included SGD30,000 of unauthorised calls.	The client was covered for their direct financial loss as a result of the phreaking attack.  <b>Payment: SGD30,000.</b>

Profile	Background	Outcome
<b>Real Estate Agent</b>	The Insured's emails were accessed by a hacker who posed as the Insured and sent multiple emails to the Insured's bank instructing for funds to be transferred into the hackers bank account. When the Insured discovered that 3 unauthorised payments had been made totaling SGD3,000,000 they immediately contacted their bank to freeze the funds. The Insured was able to recover SGD2,800,000 of the unauthorised transactions.	The Insured notified DUAL who appointed Lawyers and an IT Forensic Consultant to assist the Insured in repairing the damage to their system which was caused by the hacker. As the Insured had Social Engineering cover under their policy, they were reimbursed for the direct financial loss of the SGD200,000 unrecovered fraudulent transfers as well as their forensic and legal costs.  <b>Payment: SGD230,000.</b>
<b>Hotel Chain</b>	The Insured hired a contractor to perform works on one of their properties. The Insured received an invoice for SGD13,000 from the contractor. The following week the Insured received an email claiming to be the contractor, stating that their bank details had changed and provided the new details. The Insured subsequently paid the SGD13,000 into the 'new' bank account. A few days later the contractor followed up the Insured for payment for their works at which time it was identified that their emails had been compromised and the Insured had paid a fraudulent account.	The Insured was reimbursed for the direct financial loss suffered as a result of the fraud and additional costs payable under the policy.  <b>Payment: SGD30,000.</b>
<b>Property Developer</b>	Following the sale of 2 properties, the Insured was required to make a payment of SGD400,000 to their property consultant. On the day the payment was due, the Insured received an email from the consultant advising their banking details had changed. The Insured requested that this be sent to them in writing on the consultant's letterhead which they received, including the signature of the director of the consultancy company. The Insured was later chased by the consultant for payment at which time it was discovered that the email and letter had been fraudulent.  The Insured contacted their bank to stop the payment and were informed that the money had already been withdrawn and transferred overseas.	DUAL appointed an IT forensic consultant who identified that the hacker had infiltrated the consultants system and intercepted correspondence between the Insured and the consultancy firm.  The Insured was reimbursed for the outstanding funds (capped at the Social Engineering sub limit of SGD250,000).  <b>Payment: SGD250,000.</b>

*The information contained in this fact sheet is meant as a hypothetical guide only.*

*DUAL Asia does not accept any liability arising out of any reliance on the information in this fact sheet.*