

OCTOBER 2020

Social Engineering Fraud – An update for Marsh NZ Real Estate facility clients

Social engineering fraud has increased in frequency and severity in recent years. Fraudsters have become especially sophisticated in their impersonation of unsuspecting victims and the financial consequences of such crime can be devastating.

What is social engineering?

“Social engineering fraud” (sometimes known as “invoice or payment transfer fraud”) refers to a variety of techniques used by fraudsters to deceive and manipulate victims into the surrender of funds or loss of confidential information.

Over time these techniques have become increasingly sophisticated and can be very difficult to detect; for example cyber-criminals will often intercept communication lines – such as email – over a span of weeks or even months, awaiting the prime opportunity to issue a plausible yet fraudulent payment request.

By piecing together information from various sources, these fraudsters appear convincing and trustworthy as they work to impersonate trusted contacts of the target. The complex nature of these schemes often makes it extremely difficult to identify the fraud before it is too late. Victims range from small businesses to large organisations, across many industries and geographies.

Cyber crime in the wake of COVID-19

It was already apparent that the worldwide cost of cyber-crime was substantial. A 2019 Internet Security Threat Report released by Symantec Corporation¹ revealed that there were:

- **800 million** victims of online crime
- **117 million** of which involved identity theft and
- Just under **40%** rendering financial loss.

Coupled with a global health crisis, online fraud and phishing attempts became increasingly problematic with fraudsters seeking to exploit fears over the coronavirus outbreak.

Towards the start of the pandemic CERT NZ revealed a raft of local examples²; one such scheme involved fraudulent email communication appearing to have come from the World Health Organisation, requesting donation to a false COVID-19 Response Fund.

¹ Source: <https://docs.broadcom.com/docs/istr-24-2019-en>

² Source: <https://www.cert.govt.nz/individuals/alerts/attackers-using-covid-19-themed-scams-updated-alert/>

It is very difficult to determine exactly how a given social engineering claim will play out – these scams have become so varied in their approach, ultimately there is no ‘one size fits all’ insurance policy to cover this type of loss.

Other scams claimed to provide useful, but ultimately malicious information such as infection maps or vital details on testing stations, in an attempt to steal sensitive data from the device used to access this information, including usernames and passwords (also known as “credential harvesting”).

How will my liability insurance protect against social engineering loss?

It is very difficult to determine exactly how a given social engineering claim will play out – these scams have become so varied in their approach, ultimately there is no ‘one size fits all’ insurance policy to cover this type of loss.

Under Marsh’s Real Estate Liability Insurance Facility however (backed by AIG and Lumley) there are two policies in particular which, within the underlying terms and conditions, can indemnify you if a significant cyber-crime loss is suffered. These are the Crime policy (which forms part of AIG’s PrivateEdge Management Liability wording), and the CyberEdge policy which is a separate and optional, but highly recommend policy.

Crime insurance

In many cases, AIG’s Crime policy will be triggered by social engineering loss itself. The policy contains specific insuring clauses for Third Party Crime, Electronic and Computer Crime, and Erroneous Funds Transfer. This is great news for Marsh Real Estate Liability Insurance Facility customers, almost all of whom will have PrivateEdge Management Liability cover in place as it forms part of the default package offering – please contact us if you are unsure as to whether you have included this cover. There are however two very important points to be aware of:

1. WRITTEN VERIFICATION PROCEDURES (IMPORTANT) –

It is a condition under the Crime policy that, if a loss involves your voluntary surrender of funds (whether induced by deception or not), your firm **MUST** have already established a written process for authenticating payment requests.

This verification process should include:

- Call-backs to third parties (i.e. using the telephone number that you have on file) to reconfirm their identity, the account number and payment amount.
- Checking third-party contact details (i.e. email address, phone numbers,) against those that you have on file.
- Sign-off from management when payment amounts exceed a certain dollar figure (i.e. gaining additional authority for larger payments).

As long as your business complies with a pre-established, written verification protocol, then AIG's crime policy can and should respond to social engineering loss – subject always to the terms and conditions of cover.

2. LIMIT OF INDEMNITY (IMPORTANT) – Please be aware that by default, \$150,000 is the maximum amount that AIG and Lumley will pay for Crime loss in any given period of insurance (whether social engineering-related or otherwise), under the Marsh Real Estate insurance facility. If your firm often makes or receives large payments (i.e. greater than \$50,000), please contact your Marsh broker to establish whether this limit is suitable. We can request that this limit be increased, subject to underwriting criteria and an additional premium.

Cyber insurance

Cyber insurance is an optional add-on under Marsh's Real Estate Liability Insurance Facility, but complex Social Engineering claims highlight the importance of holding Cyber insurance in the current climate. Unlike the Crime policy, AIG's CyberEdge product can indemnify you for the added cost of IT Forensic Services, Public Relations Services, Network Interruption Loss, Data Protection Investigation, Claims Preparation and resulting Third Party Liability (among other types of loss) – subject always to the terms and conditions of cover. It is entirely likely that a Social Engineering loss suffered by your firm may also incur some measure of these additional first or third party losses.

Example – Suppose that your office network security was breached, resulting in a malicious third party gaining access to internal communications. The fraudster then poses as a Director of your firm and successfully defrauds one of your clients of payment by way of a false invoice noting a fraudulent bank account. In this scenario, a Cyber insurance policy could prove vital in covering the additional cost of identifying the security issue, containing the breach and restoring your network's security so that further loss can be avoided. If your client then lodged a complaint with the Privacy Commissioner (or some other statutory body), AIG's CyberEdge policy could also extend to cover the cost of defending an allegation and the awarded damages, under the third party liability section.

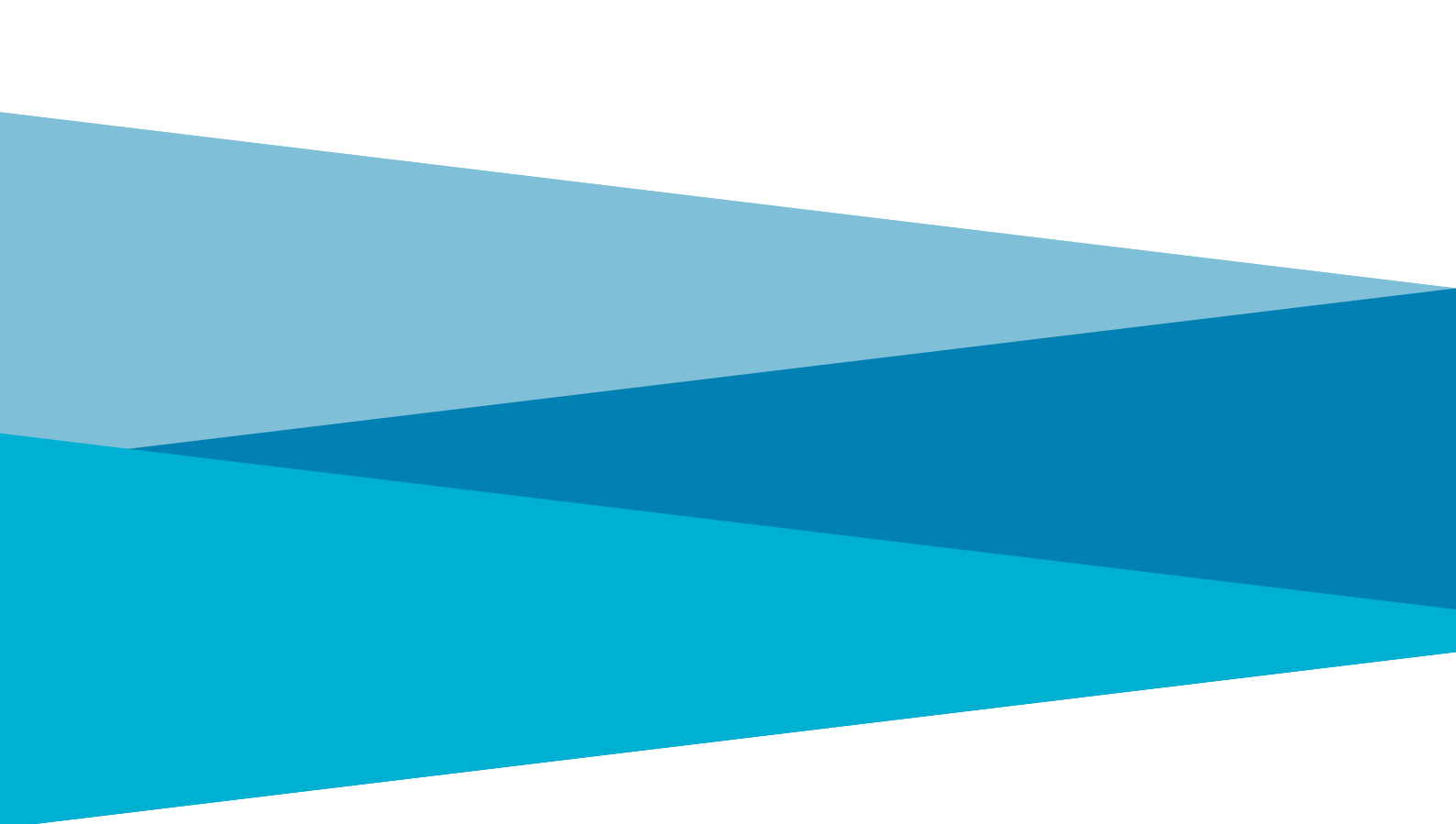
Privacy Act 2020 – For the first time in 27 years, New Zealand's Privacy Act has undergone a significant overhaul, effective from 1 December 2020. Marsh have prepared a separate client briefing in relation to this legislative change, which highlights some of the key changes, how these might affect the way that you do business moving forward, and the added importance of robust Cyber insurance cover. In light of the Privacy Act amendment and considering the significant threat that Social Engineering poses, we strongly recommend contacting your broker to review your Cyber insurance protection needs.

Summary

Irrespective of digital security software or the systems and controls implemented within your business, social engineering fraudsters are extremely persistent and their methods have become very difficult to detect. Prevention and preparation can however play a key role in avoiding social engineering attacks on your business.

Implementing robust Written Verification Procedures will not only help filter out fraud attempts, but can also validate a claim under the Crime section of AIG's PrivateEdge policy (for insured clients under the Marsh Real Estate Liability Insurance Facility). It is important that business principals understand their responsibilities in this area and the scope of protection that their insurance can provide as a safety net for this type of loss. In particular, special attention should be paid to the conditions of cover stipulated within modern Crime and Cyber insurance policies.

Marsh will continue to develop tailored insurance products for the Real Estate industry and select the best coverage available in the market to meet our clients' needs and exposures. We strongly encourage you to discuss Social Engineering fraud with your staff to help raise awareness, and to reach out to us for further advice on how best to manage these emerging exposures.



For more information about Social Engineering Fraud and other solutions from Marsh, visit marsh.com, or contact your Marsh representative.

DAVID HYLAND
Client Executive
Marsh JLT Specialty, Real Estate, New Zealand
+64 (0)21 671 468
david.hyland@marsh.com

About Marsh: [Marsh](#) is the world's leading insurance broker and risk adviser. With over 35,000 colleagues operating in more than 130 countries, Marsh serves commercial and individual clients with data driven risk solutions and advisory services. Marsh is a business of [Marsh & McLennan Companies](#) (NYSE: MMC), the leading global professional services firm in the areas of risk, strategy and people. With annual revenue approaching US\$17 billion and 76,000 colleagues worldwide, MMC helps clients navigate an increasingly dynamic and complex environment through four market-leading businesses: [Marsh](#), [Guy Carpenter](#), [Mercer](#), and [Oliver Wyman](#). Follow Marsh on Twitter [@MarshGlobal](#); [LinkedIn](#); [Facebook](#); and [YouTube](#), or subscribe to [BRINK](#).

Disclaimer: Marsh Ltd arrange this insurance and are not the insurer. The information contained in this publication provides only a general overview of subjects covered, is not intended to be taken as advice regarding any individual situation and should not be relied upon as such. Insureds should consult their insurance and legal advisors regarding specific coverage issues. All insurance coverage is subject to the terms, conditions, and exclusions of the applicable individual policies. Marsh cannot provide any assurance that insurance can be obtained for any particular client or for any particular risk.

Copyright © 2020 Marsh Ltd. All rights reserved. S20-1657