PAYMENT REDIRECTION SCAMS AND 'RED FLAG' WARNINGS

Maritime Mutual Risk Bulletin No. 57

April 29, 2022

INTRODUCTION

E-mail payment redirection scams are designed to intercept money transfers to legitimate receiver accounts and divert them into the accounts of criminal scammers. There are several ways – ranging from simple to sophisticated – in which this scam is accomplished. However, the result is invariably the same: money transfers are diverted and stolen. This Risk Bulletin is intended to raise the awareness of MM Members their ship managers and crews of the now global and endemic risk of payment redirection scam theft and the critical need for countermeasure procedures, including 'Red Flag' warnings training and consistent application.

BACKGROUND

The most common method used by fraudsters to intercept and steal money transfers appears to be through a combination of e-mail fraud techniques known as 'spoofing' and 'spear fishing'.

'Spoofing' is defined as the creation of email messages with a forged sender address. The address will often be virtually identical to a genuine address with a difficult to spot deletion or addition of a single letter, number or character.

'Spear fishing' is a specifically targeted form of 'Phishing'. 'Phishing' occurs when an attacker sends a spoofed, fake, or otherwise deceptive message designed to dupe the receiver into transferring funds to a fake account, revealing sensitive information or inserting malicious software into the victim's computer systems. Phishing can also covertly mirror and display to the attacker the site being targeted as well as being able to detect and facilitate the avoidance of security software.

PAYMENT REDIRECTION SCAM METHODOLOGY

Payment redirection scams, also known as business email compromise scams, appear to be one of the most common and financially damaging scams for all businesses worldwide. The basic methodology is that scammers impersonate a business or one of its employees using a 'spoofed' and 'spear phishing' targeted email. The request will usually be that an upcoming payment due be sent to a specified 'updated' or 'new' account, which is in fact a fraudulent account.

Scammers are known to target new or junior employees, as they are less likely to be familiar with their business employer's finance and payment processes.

A variation on the above scam is that attackers can also hack into mail accounts and intercepting business emails that have invoices attached. They then change the invoice bank details (BSB) and account number to that of a fraudulent account before forwarding, under cover of a 'spoofed' address, to the intended recipient.

SCAM LOSS PREVENTION AND RED FLAGS

No precise figures seem to be available but global payment redirection scam losses appear to add up to several USD billions over the past decade. Worse, annual losses from such scams – totalling USD hundreds of millions – reportedly continue to increase.

What can be done to prevent such losses? Computer system security software is of course available, and many Members will have already purchased and installed such software into their

shipboard and shore-based systems. These software system providers often advertise that their software can detect and flag spoofed emails. But is it foolproof?

Unfortunately, security software weaknesses exist. It is therefore always essential to confirm that any security software is kept fully updated to optimise its protection capability. Even then, it is still possible that scammers may have detected and bypassed a security software programme by using anti-security software acquired on the 'darknet'. As such, scam email protection still relies to a large extent on human observation and visual detection of spoofed or otherwise suspicious emails.

The first part of the human observer/detector solution is to develop office and shipboard procedures which include advice on spotting 'lessons learned' scam techniques. 'Red Flag' warnings include but are not limited to those listed below:

- Use of a 'From:' email address which is not a usual customer/service supplier address or, much harder to spot, looks like it has come from a known customer/supplier but has been subtly amended to create a 'spoofed' address, OR;
- Specific reference to 'updated' and/or 'new' payment details and/or provision of bank account details that do not match the account details of customer or service suppliers stored in recipient records, OR;
- Use of expressions of urgency in the cover email or fake emails from the recipient company's own CEO or other high-level executive to encourage bypassing standard procedures to speed transmission of funds, OR;
- Inclusion of telephone contact numbers, email addresses or websites in the email cover note and/or invoice which do not match customer or service supplier contacts details stored in the recipient company's records, OR;
- Spelling mistakes and/or grammatical errors in the cover email and/or attached invoice, OR;
- Use of a poorly scanned company email or invoice heading and/or use of an unfamiliar format or layout, OR;
- Anything else within the content or format of the email or invoice which appears to the recipient to be unusual to a degree that raises concerns that the email and/or invoice is not genuine.

The second part of the solution is 'Red Flag' training and implementation in the workplace, complete with practice rehearsals to ensure that 'Red Flags' are promptly spotted and acted on immediately and defensively. Further, this process becomes an integral part of office and shipboard standard practice.

WHAT TO DO IF 'RED FLAGS' ARE IN FACT SPOTTED?

The principal advice from governmental and banking based anti-scammer organisations around the world is much the same. If you are suspicious of the authenticity of any email and/or invoice, then first check carefully by communicating directly with the sender using email or telephone, but do NOT use the mail, telephone or other contact details, including websites, printed in the suspicious documents. Instead, refer to your own in-house records and databases and use only those contact details.

If a 'Red Flag' is subsequently confirmed as a payment redirection scam then, after first alerting your customer/supplier to the situation, your second call should be to your own bank to advise them that you are 'under attack' and that they should take urgent and appropriate precautions. Your third and fourth calls should be to a recognised internet anti-scamming organisation in your own country and the police to report the details of the scam and assist with hopefully identifying and locating the scammers.

Examples of such organisations and the work being done in Singapore to combat spoofing and phishing scams are provided by the links below. Members and their P&I brokers are encouraged to research and source similar facilities and advice centres in their own countries and incorporate these contact details into their scam loss prevention procedures.

Singapore Cyber Security Agency Website

Singapore introduces potent anti-scam measures, The Register, 16 Feb 2022

Singapore Police Media Website, Let's Fight Scams 2020

CONCLUSION AND TAKEAWAY

The key message of this Risk Bulletin is that MM Members need to understand the serious and increasing dangers of 'Payment Redirection Scams'. Members must therefore be pro-active in

taking measures to create formal money transfer vetting procedures to protect their interests. These procedures need to include 'Red Flag' warning countermeasures which are supported by staff training and drills to ensure full and consistent implementation. To do otherwise is an invitation to being attacked and suffering a potentially large financial loss.

Members should also note that the chance of success in recovering any losses from their own or transferee bank following a payment redirection scam attack is reportedly quite low. Members should therefore discuss this issue directly with their bankers to clearly understand what protections may be available if such losses are in fact suffered. Members may also wish to consider taking out a cyber protection insurance policy with a specialist insurance provider. Finally, and very importantly, MM wishes to make it clear that the Club's firm policy is to not change its bank account details without first providing clear and advance written notice to all its Members and all other interested parties, including brokers, of any such change. Accordingly, if Members or brokers are ever presented with any advice of 'updated' or 'new' bank details for the Club in any manner other than by way of an official Club notice, they should first verify the situation directly with Club personnel, whom they either know or have dealt with previously, by telephone, email or WhatsApp.