THE GRIFFIN INSURANCE ASSOCIATION

FINANCIAL CRIME
! ALERT !

SOCIAL ENGINEERING FRAUD

In November 2020 we issued a bulletin sharing the experiences of some Members at the hands of cybercriminals. Social engineering fraud was on the rise, with increasing numbers of people being duped by cybercriminals into facilitating a fraud. Common examples were people being tricked into revealing confidential information, such as passwords or bank account details, or into giving access to their computer so that malicious software could be installed. The number of attacks had risen at an alarming rate during the COVID-19 pandemic. Fraudsters were taking full advantage of the sudden shift to remote working and we gave some guidance on how to avoid becoming the fraudsters' next victim.

This issue currently remains one of the areas of highest risk to businesses across the board and we continue to handle notifications from Members who have been the target of an attack. A particular area of exposure for Members surrounds the processes for verifying bank account details. Criminals are infiltrating the communications between parties and pouncing when they see a payment is about to be made. They send what appear to be genuine instructions to change details of the bank account into which funds should be paid. If the instruction is taken at face value and the funds paid to the new account, without first being subject to a robust verification process, any funds paid will arrive in the hands of the fraudsters. The money will be moved on quickly and the chances of making any recovery are very limited.

This current wave of criminal activity poses a very significant risk to all Members. Guidance as to what constitutes a robust verification procedure is given below and it is essential that every Member has something akin to this in place. This should significantly reduce the risk of fraud.

LEGAL & REGULATORY RESPONSIBILITY

The Criminal Finances Act 2017 came into force on 30 September 2017 and the SM&CR came into force for intermediaries on 9 December 2019. These changes in law and regulation have meant there is an increased onus on businesses to be able to demonstrate that they have robust procedures in place when handling financial transactions. This is more important than ever with the continued significant risk which cybercrime presents to businesses.

When handling payments it is essential that Members:

- ensure all reasonable steps are taken in order to prevent payments being made to cybercriminals or fraudsters; and
- avoid committing an offence under the Criminal Finances Act 2017 by acquiescing to or facilitating tax evasion by an invoicing party.

One of the SMF holders within each Member will have been allocated SM&CR prescribed responsibility (d): *"Responsibility for the firm's policies and procedures for countering the risk that the firm might be used to further financial crime."* This person will be accountable for, and so should have oversight of, the bank account verification procedure.

BANK ACCOUNT VERIFICATION PROCEDURE

Every time there is a change to an existing payee's details, or there is a new payee, validation should be sought of those banking details from the payee, in order to verify that they are genuine and correct. A template payee authorisation form should be used for this purpose.

There are some issues which should raise immediate concern as to whether a bank account is a legitimate account belonging to the payee:

- the bank account name is different from that of the payee;
- the bank account location is in a different country to that of the payee;
- payment appears to be requested to an individual person rather than the payee company.

The procedure should always require the account handler (or other person requesting that payment be made to the payee) to telephone their regular contact at the payee and ask them to confirm that the bank details are genuine. Contact details given in communications regarding a payment should never be relied on. Fraudsters are likely to alter telephone numbers and email addresses in communications to divert enquires away from the genuine payee. Instead, the telephone contact details for the payee should be obtained from another source, such as contact details published on the payee's website or from records which are held separately to the account handler's file.

During the validation call with the payee, the account handler should establish the identity of the person he/she is talking to, to confirm it is the regular main contact at the payee. This is likely to require answers to at least two questions about the account that, in the account handler's view, only the genuine payee is likely to be able to answer.

The number called for validation, its source and the questions used to establish the identity of the person spoken to should all be recorded on the payee authorisation form. If existing banking details are being changed, the payee should also be asked to explain why the details are being changed and their answer recorded on the form.

There may be instances where it is impractical for the account handler to make the telephone call to a trusted contact. This may be due to the parties being in different time zones, for example, or there being a language barrier. In these circumstances a trusted local contact may be asked to perform the telephone call. The account handler should then call that contact to verify that the call has been performed correctly and the bank account details confirmed.

WE MAY HAVE A PROBLEM…

Time is of the essence where there is any suspicion that a payment may not have been sent to the intended payee. The banks can usually do little to stop funds disappearing once they have been transferred and so it is essential that the first port of call is our claims team. We will immediately instigate all steps to seek to minimise the possibility of the funds being lost. Where the figures involved justify the associated expense, we will instruct lawyers and tracing agents in the relevant jurisdiction and seek a freezing injunction, if the funds can be located. We did this successfully a year ago, since the sum involved was in the region of £1 million. The legal and other expenses were around £100,000 and so this will not be a viable option where smaller sums may be involved.

We will also advise you of any reports which may need to be made to the police and to the regulator.

RISK MANAGEMENT MESSAGE

Social engineering frauds involving diverting funds to fraudulent bank accounts is a very significant risk posed to all Members. We recommend the following steps to significantly reduce the risk of becoming a victim of such a fraud:

- Review your bank account verification procedure as a matter of urgency. We are available to provide further guidance to Members on this, as required.

- Raise awareness within your business of this heightened risk. There should be a clear message that the procedure in place must be followed at all times, without exception, regardless of the apparent urgency of any payment. Following the procedure will always be commended.

- At the first hint of a problem get in touch with us at Griffin. Do not lose time liaising with the bank or any other party. We will agree all steps that should be taken to protect your position, as soon as we are involved.

Further guidance can be found in Section 21 of the Broker Risk Management Guidelines and Section 17 of the MGA Risk Management Guidelines, which are available on Griffin's Member portal.

All Representative Members will be contacted shortly and asked to provide details of their bank account verification procedure. We are aware that some Members still do not have a sufficiently robust procedure in place and that some continue to place reliance on an informal understanding amongst staff as to the steps that should be taken. We want to ensure that all Members have appropriate written procedures in place, to mitigate this heightened risk of fraud, and will provide support to Members, as required, to help achieve this.

Managers: Griffin Managers
Regis House
45 King William Street
London EC4R 9AN
Telephone 020 7407 3588
Email griffin@tindallriley.com
www.griffin-insurance.co.uk

First Issued: November 2022