COVID-19 BUSINESS SUPPORT - ISSUE 8

# SME DIGEST

ADVICE FOR SMALL & MEDIUM SIZED ENTERPRISES

Edited by Adam Bernstein

CORONAVIRUS FRAUD ALERT

# BEWARE OF THE CORONAVIRUS FRAUDSTER

You'd think in times such as these that even the criminally minded would take a step back and think carefully about their actions. But no, they – specifically fraudsters – see it as just another opportunity to steal what they cannot legitimately earn.

*By Adam Bernstein*

The problem for most, and one which opens the door to fraudsters, is that individuals and organisations alike have been following the advice from the government in relation to social distancing with the result that some workers who aren't furloughed are working remotely. It's precisely because workers are still finding their feet that the unknown along with a lack of face-to-face contact with colleagues has made it harder to detect inbound fraud.

Fraud attempts are manifesting themselves in a number of ways, but primarily through email. If you've not yet had any Coronavirus-related fraudulent emails you're very lucky – to see what's around just take a look on Google. There are countless warnings from the Crown Prosecution Service, the Financial Conduct Authority, National Cyber Security Centre, HMRC, Serious Fraud Office, and Action Fraud.

Indeed, Action Fraud is apparently seeing an increase in cases related to Coronavirus – it saw a rise of 400% in March alone. Its website actionfraud.police.uk offers a number of headlines that make interesting reading.

**What does this mean for you?**
Apart from dealing with the fallout from the Coronavirus melee, firms need to pay more attention to how they're working and the opportunities for the criminally minded to exploit weaknesses introduced into processes. Sight shouldn't be lost of the controls and processes that, by necessity, are being 'officially' bypassed to allow firms to carry on as best they can. For example, where in normal times three people may have been involved in the payments process – one to prepare and two to cross check and authorise payments – it may be the case that there's only one now to prepare and just another to authorise. It's possible that multiple roles are being heaped onto remaining staff who haven't been furloughed.

So, with this in mind, it's worth briefly looking at the types of fraud that a firm might be presented with after all, forewarned is forearmed.

## Employee related fraud

This might involve a request to change a worker's bank details that are used for payroll. Where any request is made, this should be checked in person with the individual that it relates to. Changes should never be made on the basis of an email received without a cross check.

## New supplier fraud

Whenever a new supplier is introduced to an organisation there is the potential for fraud. Very simply, any new payees should be verified with the individual ordering the good or service and also by independently checking with the supplier (by finding contact details separately).

## Payment diversion

Allied to the two above, this fraud is so simple as all it's trying to do is have a payment diverted - via email, fax or letter - from a legitimate bank account to that belonging to a fraudster. Again, the solution is to ensure that every request is met with a process that demands verification through independent means.

## Procurement fraud

With an eye to the news, new scams may relate to the sale of personal protective equipment, such as face masks and gloves online. While some are selling inferior goods others are just not delivering after payment has been made.

## Internal fraud

As noted earlier, Coronavirus has led to staff being furloughed, home working and the desegregation of duties. Considering human weaknesses, firms should put in place extra processes that minimise the incentive for workers to commit internal fraud.

## Remote working and IT fraud

This type of fraud is not new but is being further exploited. Invariably a worker will receive an email or a call from an external body claiming that they've noticed a problem on the worker's computer. The third party is offering a fix which normally means inadvertently ceding control of the computer which will then permit fraud. A good example is a keylogger which the third party can use to note down bank accounts and log on credentials. Staff should be told to report any communications that don't come from an official source.

## Courier fraud

This fraud is particularly nasty as it involves a third party pretending to be a bank or other such organisation; the aim is to deceive the individual to move monies to a 'safe' bank account while a fictitious fraud is dealt with. Staff should be told that – both in the world of work and home – they will never be called by a financial organisation to move monies. Unsolicited calls should be terminated, and the matter reported to management.

## Phishing fraud

Frauds of this nature attempt to trick people into either opening malicious attachments which could lead to fraudsters stealing organisation's sensitive information, email logins and passwords, and banking details or lead the recipient of the email to a lookalike website which impersonates HMRC or another body. Again, if an email like this is received it should be deleted. If in doubt, separately navigate to the body's website and look for the padlock symbol and https in the address bar.

# Action Points...


- Give all staff a refresher on internal policies noting that there's a **zero-tolerance** to anything illegal within the business. While this raises awareness of the matter it also reinforces to staff that fraud won't be tolerated
- Keep a watchful eye on ***actionfraud.police.uk*** for the latest news stories on fraud. It'll give a lead on the types of fraud that are being perpetrated
- Stay in contact with suppliers – and anyone else the business pays – to keep frauds to the minimum. Check all payee details and any changes. Use phone or video calls to check if appropriate
- Invest in good anti-virus software and instruct staff to not click on links or attachments in unexpected or suspicious emails
- Remember that no financial institution will ever call and ask for monies to be transferred
- Report all frauds to Action Fraud



TAP™ PPA LAND POWER PUBLICATIONS