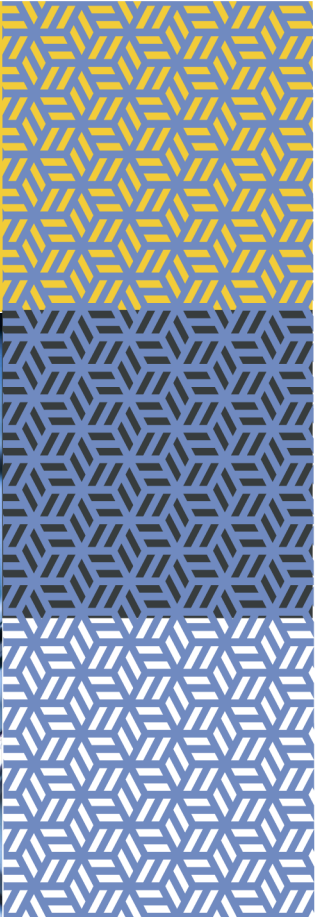
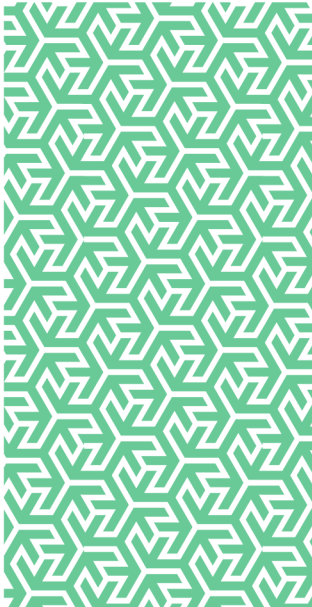


rmp

Risk control
Social Engineering



In partnership with


**GALLAGHER
BASSETT**
GUIDE. GUARD. GO BEYOND.

Risk Control

Social Engineering

Introduction

For public sector organisations, every pound lost through fraudulent activity, is a pound less that is spent on essential front line service delivery to residents. That is why proactive steps are taken to safeguard against all forms of fraud be they internal or external sources.

In recent years, we have become increasingly aware of the rise of payment fraud with cyber criminals looking to capitalise on distracted and busy minds. Every day could be considered 'Friday Fraud' territory when employees are looking to 'tie up loose ends' before the weekend, meet deadlines etc. Criminals take advantage of such busy periods and look to socially engineer employees into cutting corners, ignoring policies, and breaching regulations so that monies are paid away into the fraudster's bank account.

This activity is now translating into claims and 'near misses' with the last quarter alone producing one claim from a metropolitan council potentially in the region of £1m plus and a near miss from a County Council which could have run to many millions, but which thankfully was thwarted at the last moment by the actions of their bank.

What is driving this behaviour is hard to pinpoint; but the prolonged period of pandemic lockdown with key employees working from home certainly lends more confidence to the fraudsters, that systems of control and checking may be a little more relaxed.

Although unrelated, anyone with a mobile phone who has undertaken on-line shopping in the last 12 months will no doubt have had the fraudulent text message to say your delivery is being held up and you are invited to 'trace' your parcel by clicking on the link below, which if you do is likely to be the last thing you will do on your phone.

All of this goes to demonstrate that as technology becomes more sophisticated, so do the techniques and concepts deployed by the fraudsters

What is Social Engineering?

Social engineering is effectively the art of manipulating people so they give up confidential information or are duped into making a payment directly into a fraudster's account.

The types of information these criminals are seeking can vary, but they are usually trying to trick you into giving them passwords or bank information, or access your computer to secretly install malicious software—that will give them access to your passwords and bank information as well as giving them control over your computer¹.

¹ <https://www.webroot.com/gb/en/resources/tips-articles/what-is-social-engineering>

It is usually committed by telephone in combination with email. By faking the identity of someone who the victim believes, often by invoking in them a need for urgency through a call to action or by building trust in a series of apparently legitimate enquiries. This way, the fraudsters convince the victim to make or authorise a payment, bypass protective procedures or grant them access to their systems.

Criminals use social engineering tactics because it is usually easier to exploit your natural inclination to trust than it is to discover ways to hack your software.

Three Tiered Approach

The three levels advocated are not new but when tailored specifically around a particular risk theme or hazard, in this case social engineering fraud, they can be used in a synchronised way that optimises your risk management efforts.

There is always a cost-benefit equation to consider when investing limited risk resources, so this approach adds more weight to the benefit side of the scales.

The three levels to consider are:

1. Operational Risk Controls: Systems and Supervision working together
2. Cultural Factors: Strong leadership and open communication
3. Oversight: Robust second and third lines of defence.

Operational Risk Controls

Each local authority is responsible for establishing appropriate mechanisms to manage the risk of fraud within their own authority. This includes policies, systems and processes and the focus is normally two-fold – reactive counter fraud work including investigations and sanctions and preventative fraud activity focussed on intelligence monitoring to detect fraud hotspots.

Third Party ('Push Payment') Fraud has been on the rise since 2014 when a well-publicised vishing scam enabled by rogue employees of a UK mainstream bank reached the news. It is often underpinned by cybercrime, data breaches, and social engineering, so cyber controls and data protection are important, but well-educated people and robust payment controls can thwart attempts to con someone into paying monies into the wrong hands. Essential controls to build into procedures are as follows:

- i. Obtain evidence of bank account details at the outset of a new payee relationship showing the name of your payee/supplier on for instance, a bank statement, paying in slip, bank card etc. Making this a part of your new payee onboarding/due diligence processes should result in this swiftly becoming second nature. Getting this information early removes a pressure point which criminals can exploit when things may become rushed, and people may be tempted to cut corners. Changing these later becomes a big deal so should be an automatic warning flag for anyone asked to do this.
- ii. Be vigilant to fake emails. Spoof emails are the most common means of perpetrating payment fraud at present but can be detected by hovering over the sender's address to look for subtle changes often a single digit such as an l to a ! which often won't be spotted in a small font. Whilst poor language and grammar used to be obvious warning signs, fraudsters are now more sophisticated at mimicking the individual they are impersonating.
- iii. Be suspicious of any communication about bank accounts at any stage, but especially when advised close to the point when monies are about to be transferred. Whether it's a supposed confirmation 'just to remind you', a change of account, or a request to split funds across different accounts to share proceeds or deal with other purportedly pressing needs, any contact about bank details should be an immediate red flag triggering the following checks:
 - Contact your payee using a trusted telephone number obtained at the payee onboarding stage. Never rely on them calling you "to confirm their email" as it could be the fraudster impersonating on that channel as well. Similarly, a change to contact details should be treated with caution and verified by another means; Needless to say, this safety call should be treated as high priority;
 - Obtain evidence of the changes by going back to Step i and ensuring that the new details are obtained in person or by secure delivery and match the exact name of your payee/supplier. Documents appended to an email are easy to fake including letter headed paper and online style bank statements. Printed bank statements, paying in slips, a picture of a corporate / debit card, the confirmation of new telecoms / email account etc. are harder to fake. Even so, a call or video call to capture a picture of the new evidence via your trusted contact is the safest bet.
 - Fraud proof your payment request / authorisation form (or equivalent) with adequate control stages to be signed off as completed so that the process is never reliant on a single person performing their job perfectly 100% of the time - an unrealistic expectation. Risk controls need to allow for human imperfection by adding

layers that reduce the likelihood of error to negligible. The recent frauds we have seen have been successful as such layers were not part of the everyday process, or were, but not followed.

- Limit immediate faster payments (IFP) to nominal sums for established payees. Please avoid use of this method for transfers of larger funds especially one off payees. IFP is favoured by criminals as is transferred in seconds and can be moved to other accounts (overseas) very rapidly, decreasing the chance of recovery. Evidence from six years of increasing payment fraud shows there is a much better chance of blocking payments to criminals when CHAPS (or BACS) has been used. If all else fails, this could help in recovering some of the monies already transferred to a rogue account.

Take Time to Review

You may also need to review and update the following to include the risk controls outlined in this reminder:

- Written policies and procedures
- Forms and checklists used for making payments
- Quality / risk control gates in workflow screens
- Training and education materials
- Any checklist that you use on suppliers, projects, beneficiaries, files etc. to manage process flow.

Such updates should appear as standing agenda items for relevant meetings, and team leaders at every level should ensure time is given to discussion of these to ensure successful implementation of new and updated policies.

Payment Request Control Layers

Strengthen your financial risk management framework by ensuring there is separation in payment roles within the organisation. No one individual should be able to set up a new payee account and make a payment without peer review and/or supervisor sign off. The following describes a 3-step process but two tiers, or 'dual-authorisation' is the minimum recommended.

- | | |
|---------------------|---|
| i) Requester | Provides the transaction details (e.g. instruction/authorisation, evidence of receipt/completion and/or invoice) and attaches evidence of the client bank account, showing clearly whether these are originals or changed details. Any changes to originals must be accompanied by replacement bank account evidence and a record showing discussion with the payee in a call |
|---------------------|---|

- instigated by one of your staff members, using a trusted phone number used previously.
- ii) Authoriser** Confirms they've conducted a functional verification of the documents to ensure they meet procedural requirements as Stage I. Signing without checking is not verification and only serves to reinforce previous errors and omissions.
- iii) Releaser** Confirms that all evidence is adequate and accurate prior to release of funds and that no anomalies in evidence, client names, or banking arrangements are apparent. Requests for splitting monies across accounts, transferring beneficiary, overseas payments etc. often factor in fraud.
- Stages II and III may be reversed and stages i) & ii) or ii) and iii) may be combined. Critical is at least dual authorisation in whatever form best fits your payment process.*
- iv) Anomalies** In evidence, payee name/s or banking arrangements, no matter how seemingly minor, should be escalated in line with protocol. If you don't have an escalation protocol, one should be written, and staff trained accordingly.

Cultural Controls

Leadership and communication are vital to the success of fraud prevention controls and any risk or quality campaign message can easily be lost if the organisation's culture doesn't support it. Influencing factors include:

- 1. Strong Messaging** - Leaders at all levels need to deliver messages face-to-face to explain objectives and approaches when policies or procedures are introduced or updated. Cascading of messages through all levels needs to be effective and not be diluted in the process. If your procedure asks for sharing and acknowledgement of new and updated policies or procedures, email ticks the box but is not as effective in making sure everyone is on the same page through face-to-face discussions.
- 2. Clear Expectations** - All personnel should understand that compliance with fraud prevention measures and the consequences of failure to do so are built into disciplinary processes. This should be consistent for

everyone so employment contracts, consultant contracts, partnership agreements etc. may all need consideration in this context

- 3. Speak-Up Culture** - Individuals need encouragement to speak up and the confidence that that they will be listened to and supported so a culture of transparency and trust is essential. Challenges to unusual requests (from someone within or external to the organisation) should be fully supported. Leadership messages on speaking up need to permeate right through the organisation to be successful, so take care not to let these be watered down or smothered completely through the management hierarchy. Talk openly about concerns to clear the air about ignoring risk flags, dealing with difficult payees, or even bullying colleagues as they can all undermine controls by pushing staff to cut corners when the pressure is on. As a last resort, official 'Whistle-blowing' channels to external authorities should be available.
- 4. Comprehensive Training Programmes** - This should include induction, regular refreshers, risk-based themes etc. E-Learning has its place, but training in-the-round is better at allowing people to ask questions, air concerns, challenge approaches, and deal with nuances in different functions as there invariably will be. Social Engineering should be included in your training programmes.
- 5. Reminders** - Ongoing reminders keeping social engineering, fraud prevention and risk generally on the agenda, at all levels - featuring in team discussions as appropriate. There is no shortage of stories in the media to use as hooks to keep the subject of social engineering front of mind and to provide new angles and insights as fraudsters become more sophisticated in their plots and 'M.O.'s.
- 6. Culture** - Finally, consider how each of these cultural aspects are delivered in the context of your existing policies and procedures and your audit programmes to assess where any improvements might be made.

Oversight

Independent checks should be in place to give assurance that day-to-day controls are being followed. Effective management systems will also aim for structured review and improvement.

It may not be possible to implement all the following but the more defence layers you have, the less likely fraud will become.

1. In-Line Compliance Checks

Checklists, data fields and control gates can all be used to prompt compliance with agreed procedures and to raise a flag or show an obvious gap that a step has not been completed. Having compliance checks inbuilt into the process provides useful feedback in real time rather than after the fact.

2. Financial Spot Checks

Random checks on processes, parts of processes, or individual higher risk payees / payments can add another defence layer. Knowledge that these happen irregularly and unannounced can also act as a deterrent to would-be in-house fraudsters.

3. Independent File Reviews

Any process of independent review e.g. on specific projects, suppliers, cases etc. can be adapted to include checks to ensure that specified fraud controls measures are being followed at individual matter level. Review and update the checklist in line with procedure updates (generally annually) to ensure it keeps pace with changes in fraud prevention controls.

4. Internal Process Audit

Ensure the scope of your internal audits covers all processes and controls required to prevent fraud. Sometimes there are black holes where auditors are excluded. Finance and HR can be two such areas as records may be viewed as sensitive. If processes are documented, they can be audited. If they are not documented, then the scope of your documented quality management system may need to be reconsidered to cover all risks.

5. External Process Audit

Any third-party auditors should be considering your risk control systems in the context of the current business environment. Social engineering and fraud are now well-known hazards and ones that are not receding so fraud prevention controls should be included in the scope of your external process audit.

6. External Financial Audit

Understand what your Financial Auditors are doing in this regard already and what might be done to extend the scope of this final layer of independent review. It might include specific fraud prevention advice, more in-depth risk-based reviews, training and possibly the use of forensic software.

QBE Crime Prevention Toolkit

QBE have devised a special on-line questionnaire which can help public sector bodies understand their exposures in more detail and assists with gap analysis. Once completed you will receive a report back summarising the findings. The facility is available to all clients where QBE insure the Crime cover and if you would like more details please contact your RMP Account Director.

Summary

Remember...

Training for all relevant staff is critical. Share this note by email by all means but make sure you have an open discussion too so people can ask questions and you can agree what's relevant for your team.

Raising awareness, lowering automatic trust, encouraging people to be curious and empowering them to challenge odd requests (even when it is the 'fake' boss) are all crucial to preventing social engineering fraud.

Changing a bank is a significant task and would not be a last-minute notification. If the newly nominated bank is not a main stream 'big six', it's likely they won't have 'confirmation of payee' (CoP) in place, so that is also a red flag. Bear in mind though, even with CoP in place, it seems it can give false positives for long payee names that are the same at the start, but have a subtle change on the end that is not picked up by the CoP system so always triple check.

Evidence for changes should always be requested (paying in slip, bank card, official bank statement) showing the sort-code, a/c number and name of the account holder all on one source of information. The name of course must match your existing suppliers and not be subtly different (e.g. with a 'trading as' added). If requested at that stage, it may be enough to deter weaker fraudsters. No action should be taken until that evidence is received.

If the request is by email - look at the sender's full email address - is it exactly the same as your payee's or a spoof version. Just hover over the address without clicking on it and you will see the real email address rather than that displayed.

In any case, after such a request is made, refer to your own details for that supplier/beneficiary, use a trusted phone number and contact them to verify - speak to someone you already know if possible. Do not use a phone number provided on the request to change the bank details. Fraudsters have realised that people talking directly to each other thwarts their fraud endeavours so increasingly they are attempting to have contact details (email address and/or phone numbers) amended on systems just prior to

requesting changes to bank details. If that request goes unchallenged and the central record is updated, the safety call made to verify the change in bank details is only destined to fail as it will be answered by the fraudster. To summarise: any request to change a payee's details must be treated with the utmost suspicion.

There needs to be at least two layers of verification - no single individual should be able to authorise such a change. Both should check the evidence and sign off that the phone call to a trusted contact has taken place. Line manager sign-off should be sought where any doubt remains.

If fraud takes place, or is hopefully detected and prevented, it should always be reported to Action Fraud. They might not respond individually or be able to solve your own case, but they can build up a picture to prevent in future attacks.

Fraudsters will try and exploit the vulnerability of local authorities whilst their attention is diverted and focussed on continuing to deliver front-line services with reduced capacity and restricted movements and/or operating capability.

Scams and frauds come in all shapes and sizes and all organisations are at risk. Local authorities always need to be alive to these, but the increased exposure that COVID-19 brings, means an even higher level of vigilance is needed so staff will need regular reminders on this count, particularly if working from home.

Message of Thanks...

A message of thanks to QBE Risk Solutions, European Operations Financial Lines for their assistance in the production of this guidance document.

Further information

For access to further RMP Resources you may find helpful in reducing your organisation's cost of risk, please access the RMP Resources or RMP Articles pages on our website. To join the debate follow us on our LinkedIn page.

Get in touch

For more information, please contact your broker, RMP risk control consultant or account director.



Risk Management Partners

The Walbrook Building
25 Walbrook
London EC4N 8AW

020 7204 1800
rmpartners.co.uk

This newsletter does not purport to be comprehensive or to give legal advice. While every effort has been made to ensure accuracy, Risk Management Partners cannot be held liable for any errors, omissions or inaccuracies contained within the document. Readers should not act upon (or refrain from acting upon) information in this document without first taking further specialist or professional advice.

Risk Management Partners Limited is authorised and regulated by the Financial Conduct Authority. Registered office: The Walbrook Building, 25 Walbrook, London EC4N 8AW. Registered in England and Wales. Company no. 2989025.