QBE Risk Solutions
Risk Alert

Fraud Prevention: Avoiding being a victim of banking fraud.

Solicitors' Professional Indemnity
Winter 2020/21

Made possible
QBE

QBE Risk Solutions
At your service

Fraud Prevention – Important Reminder

Banking Fraud Warning

Fraud has been on the increase over recent years, and the Covid-19 pandemic has seen an exponential rise in online and telephone frauds impacting professional firms as well as individuals. A recent flurry of payment frauds our clients have experienced are illustrative of that. With the property market anticipating continued high demand, expectations of a continued increase in house prices during 2021, and high levels of remote working, conditions are ripe for 'Friday-Fraud' where solicitors are socially-engineered into cutting corners, ignoring policies, and breaching regulations so that client monies are paid away into the bank accounts of criminals.

Seven Critical Fraud Risk Controls

Implement our seven critical risk controls to reduce the risk of becoming a victim of banking fraud. If you need any help at all in understanding or implementing these controls, please get in touch with us.

1. **Always obtain evidence** of bank account details at the *outset* showing the name of your client/s on for instance, a bank statement, paying-in slip, bank card etc. Building this into your wider Know your client (KYC) / AML processes should result in this swiftly becoming second nature.

2. **Warn your clients** about the risk of fraud. We have provided a **Model Guidance Note for Clients** for adaptation as required. Specific attention should be drawn to this warning, preferably face-to-face but otherwise via clear signposting. Clients are part of the payment process but are probably the weakest link; using web-based email, insecure Wi-Fi, inadequate firewalls, antivirus controls, and out-of-date software, they are easy prey for fraudsters to find a route into the payment chain.

3. **Be vigilant** to fake emails, particularly nearing the time of transfer of funds to your clients. 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.

4. **Be very 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 client using a telephone number given at the start - don't 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;
   - obtain evidence of the changes by going back to Step 1 and ensuring that the new details are obtained in person or by secure delivery and match the exact name of your client.

5. **Fraud-proof your Payment Request Form** 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 so 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. **Example control layers are shown in the table overleaf. In small firms one person may perform dual functions but should still act independently.**

6. **Use SEPA/SWIFT/CHAPS to make payments of large sums.** Evidence from six years of increasing payment fraud shows we have a much better chance of blocking payments to criminals when SEPA/ SWIFT/CHAPS payments (as appropriate) are made. If all else fails, the time delay in processing such payments can help in recovering some of the monies if transferred to a rogue account.

7. **Ensure these protocols are being followed by means of ongoing file reviews and audits.** Incorporating fraud prevention control checks within key stage supervisory file reviews and your file audit process will help ensure that your fraud risk controls are embedded and become part of your risk culture.

Made possible
QBE

QBE Risk Solutions
At your service

Fraud Prevention – Important Reminder

Strong leadership is vital

Please circulate this reminder without delay but put your leadership structures to work to make sure this information is discussed in the round with all relevant teams, where expectations can be made clear, and any questions and concerns dealt with openly.

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
- File review checklist - to ensure via your audit process that controls are embedded.

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.

QBE Fraud Prevention Toolkit

QBE's Fraud Prevention Questionnaire (accessible via our QRisk portal) will help you identify and address any priority risk improvements to reduce your exposure to fraud.

Our Fraud Prevention Toolkit contains further guidance and models and is available via QRisk: https://qrisk.qbe.com/ (QBE client login required).

Payment Request Control Layers

I) Requester	provides the transaction details and attaches evidence of the client bank account, showing clearly whether these are originals or changed details. Changes must be accompanied by the Attendance Note showing discussion with the client in person or via a phone call instigated by the requester using a phone number provided at the outset.
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.*
IV) Anomalies	in evidence, payee name/s or banking arrangements, no matter how seemingly minor, should be authorised at the highest level, e.g. by your **MLRO.**

Thank You

Thank you for taking fraud prevention seriously, particularly if our recommended controls are already embedded within your practice.

If you want to discuss this or any other aspect of your fraud risk controls, please contact your broker or email one of the QBE Risk Solutions team – details below.

Contact QBE Risk Solutions

Deborah O'Riordan
Practice Leader
Deborah.O'Riordan@uk.qbe.com

Jaini Gudhka
Senior Risk Manager
Jaini.Gudhka@uk.qbe.com

Calum MacLean
Senior Risk Manager
calum.maclean@uk.qbe.com

QBE European Operations

Plantation Place 30 Fenchurch Street
London EC3M 3BD
tel +44 (0)20 7105 4000
QBEeurope.com

Made possible
QBE