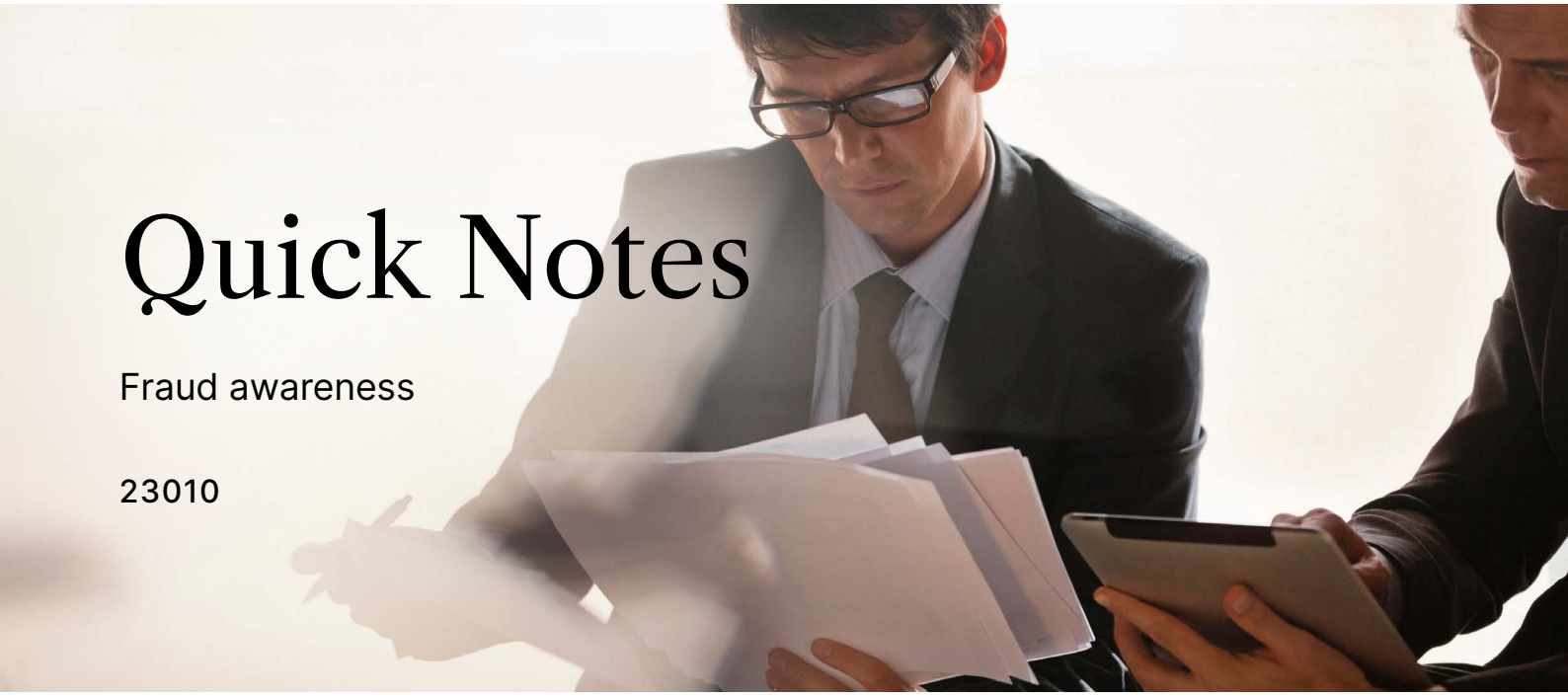

Quick Notes

Fraud awareness

23010

Payment controls to consider implementing to reduce the risk of falling prey to fraud

- Staff should always follow up email instructions with a phone call to the client's original contact number
- Consider implementing a policy whereby payments are only made to a bank account in your client's own name and that no third-party payments are permitted
- Client authentication and verification questions could be established and utilised to verify client instructions
- Payment limits can be established for instructions received by email
- Always ensure that you take an instruction for payment from a person authorised on the account to do so

CCM system controls

- Daily movement reports with transaction details - these should be printed and signed off daily
- Account audit trails – these should be scanned for unusual activity or activity out of the norm on a specific account (could be a flag for internal or external fraud)
- Segregation of duties – multiple user access: have different staff setting up, approving and authorising payments on client accounts
- Sharing of passwords is prohibited
- When a member of staff leaves your employment, you should notify us to enable us to remove a user's access to the system

If you suspect fraud on your client's account or intermediary profile, please contact our 24/7/365 Global Client Support Centre on +27 (0) 11 286 9663 or 0860 110 161 or the Fraud Line on +27 (0) 11 290 8955.

Regards

Shavonne Bagley

Shavonne Bagley
Head of Client Servicing