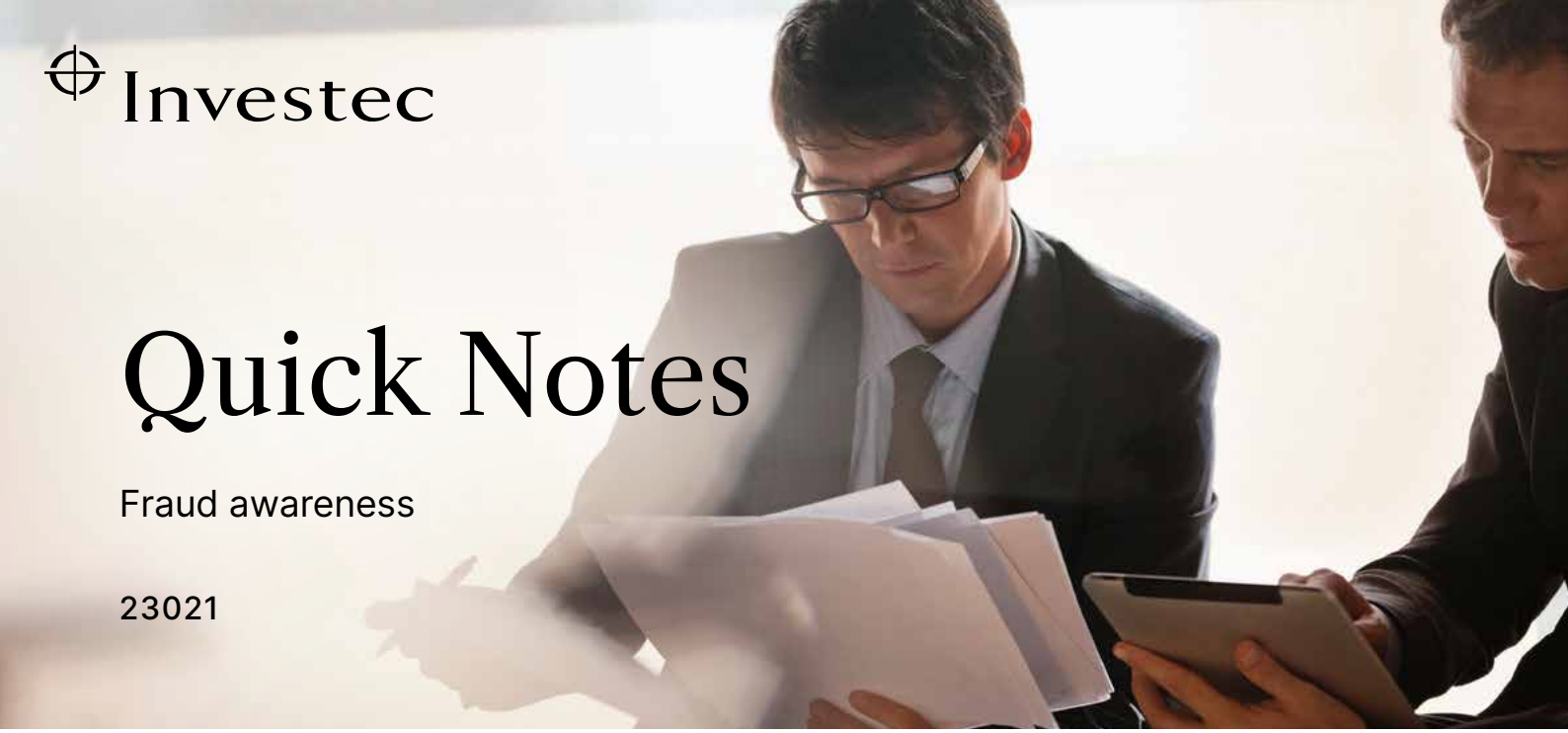

Quick Notes

Fraud awareness

23021

What is email account compromise?
How can email account compromise attacks be prevented?

Safeguard your email account.

- Use strong passwords that are lengthy and a combination of numbers, letters and special characters.
- Enable two factor authentication.
- Don't repeat passwords across service providers.
- Be cautious of emails that contain links requiring you to share personal information. Do not be deceived by urgent requests that require you to share your credentials.

Protecting your email inbox is vital. It's important to remember that an attacker doesn't need to compromise your account for an attack to be effective. Anyone involved in the communication can be hacked, allowing an attack to succeed through spoofing techniques. This means that even if your inbox is secure, an attacker can still impersonate a trusted party and successfully execute an attack.

Therefore, it is crucial to always follow the next prevention technique to safeguard against a successful email account compromise attack.

Verify banking details that were sent to you by email.

- When you receive an email requesting contact details to be updated or payments to be made, ensure you call the sender on the number that you have on your own records, to confirm the request.
- Verbally verify specific details, such as the account number or new contact information, to ensure the legitimacy of the request.
- Don't assume that bank information referenced with the correct name and surname or company name is legitimate.
- 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

- Review of daily movement reports with transaction details - these should be printed and signed off daily.
- Account audit trails – these should be scanned for unusual activity 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 strictly prohibited.
- When a member of staff leaves your employment, you should notify us immediately to enable us to remove a user's access to the system.

CCM Fraud reporting number

Should you suspect fraudulent activity on any of your Investec accounts please immediately phone the Investec Global CSC (available during banking hours) the number is 0860 33 55 77.

We recommend saving this number on your cell phone for ease of access.

Once the relevant beneficiary bank has been notified of the fraud event by our team you will need to provide the following to us within four working days:

- SAPS Case number.
- Copy of an affidavit. The affidavit must include a commissioner's stamp, a detailed account of the incident, and specific payment details including the date, amount and beneficiary account number.
- Any evidence that you may have in respect of this matter. It may be in the form of documentation or communication regarding the incident.

For any queries, please contact your Investec for Intermediaries consultant or our CCM Inland or Coastal Servicing teams.

Regards

Shavonne Bagley

Shavonne Bagley
Head of Client Servicing