Safeguarding your practice against fraud

29 April 2024

With the current prevalence of fraud, clients and intermediaries of financial institutions must stay vigilant and aware of the fraud trends in order to protect themselves against attacks. We share some tips about fraud detection and prevention, and indicate the measures implemented by Glacier in this regard.

More opportunities for fraudsters

Along with the global increase in digital transactions and online interactions over the last few years, cybercriminals and fraudsters now have more opportunities to access and exploit sensitive information and as a result there has been a concerning rise in fraud and cyberattacks in the financial services industry.

The financial services industry continues to adapt and improve fraud detection, prevention and monitoring measures in order to combat the continuously evolving fraud risks whilst maintaining a client-centric experience.

Financial institution fraud trends

1. Identity Theft & Fraud

Example: A client's personal details are stolen and used to open a bank account in their name. An instruction to change client contact details is then sent electronically to a financial services provider from the fraudster. Subsequently, a withdrawal instruction is sent with new banking details of the fraudulent bank account that was opened with the client's legitimate information.

Mitigating actions

- Signed instructions required: For any changes to personal information, e.g. email address, contact numbers, address, Glacier requires a signed instruction from the client.
- Confirmation of bank changes: Glacier will also telephonically contact the client or their financial intermediary to confirm all change-of-banking-details instructions received.

- Withdrawal confirmation emails: Financial intermediaries should take note of the ‘confirmation of withdrawal’ emails sent by Glacier especially for withdrawal instructions which were not submitted via their office.

2. Impersonation

Example: A fraudster (sometimes a family relative) impersonates the client and calls into a financial institution’s call centre attempting to obtain information regarding a client’s investments.

Mitigating actions

- Glacier verification process: Security questions are used to verify a caller’s identity and protect client information. An impersonator would usually fail verification questions.
- Monitoring of red flags: In addition to the verification process, we monitor for any additional red flags. The common red flags in these types of calls would be acting nervous, evasive, or irritable.
- Intermediary consultation: If the verification questions are not answered successfully, the client’s financial intermediary will be contacted.

3. Email account compromise

Example 1: Hackers illegally gain access to an intermediary’s email account through a phishing attack (stealing the username and password) or password spraying (where the email account holder has weak passwords). The hacker then intercepts emails between the intermediary and their clients to obtain sensitive data and send emails fraudulently requesting payment on behalf of a financial institution.

Example 2: Cybercriminals send spoofed emails (fake sender address) seemingly coming from a financial institution to a client or intermediary with false banking details.

Be vigilant

- Symptoms of a possible compromise:
    - Unknown emails in your sent items
    - Missing emails
    - Not receiving emails from certain senders/institutions

- How to recognise email compromise attacks:
    - Spoofed sender domain, e.g. @glacierr.co.za
    - Email contains typos and grammatical errors
    - Urgency in the e-mail subject and body
    - Requests for urgent payments to bank account provided

4. Deceased estate fraud

Example: Criminals illegally obtain the documents used to register a deceased's estate at the Master's Office (death certificate, identity document and list of all assets held by the deceased estate). The criminal then makes contact with the deceased's financial institutions to liquidate the assets of the estate to the benefit of the criminal. The criminals open estate late bank accounts, submit fraudulent death claims to the various institutions and have the liquidated assets paid into the fraudulent bank accounts

Mitigating actions

- New QR code on deceased estate appointment letters: Due to the increase in fraudulently manipulated appointment letters issued by the Master, the letters will now carry a Quick Response (QR) code linked to the Master's system which can be used to verify and validate appointment letters issued. The Master's offices in Johannesburg and Durban have been issuing QR codes since March/April 2023, while the start date for the rest of the country is still to be confirmed.

- Tips to prevent deceased estate fraud: The executor or family should contact the various institutions as soon as possible to provide the information of the executor or authorised person(s), such as name, email address and contact number. The financial intermediary should ensure that the family, next-of-kin, and beneficiary contact information is updated prior to the death of the client.

Glacier Financial Solutions (Pty) Ltd.

A member of the Sanlam Group
Private Bag X5 | Tyger Valley 7536 | Email client.services@glacier.co.za | Tel +27 21 917 9002 / 0860 452 364 | Fax +27 21 947 9210 | Web www.glacier.co.za | Reg No 1999/025360/07
Licensed Financial Services Provider | Glacier Financial Solutions (Pty) Ltd. is also a Licensed Discretionary Financial Services Provider FSP 770, trading as Glacier Invest | Sanlam Multi-Manager International (Pty) Ltd. | A member of the Sanlam Group

Private Bag X8 | Tyger Valley 7536 | Tel +27 21 950 2600 | Fax +27 21 950 2126 | Web www.smmi.com *|*Reg No 2002/030939/07
Licensed Discretionary Financial Services Provider, acting as Juristic Representative under the Glacier Financial Solutions FSP 770
Glacier International is a division of Sanlam Life Insurance Limited
Sanlam Life Insurance Ltd. | Email life@sanlam.co.za | Tel + 27 21 916 5000 / 0860 726 526 | Fax +27 21 947 9440
Reg No 1998/021121/06 | Licensed Financial Services Provider