Retirement funds and cyber security compromises

In the digital age where demand for capabilities such as online access for members and participating employers plays an integral role in managing financial transactions and personal information by retirement funds, ensuring robust cyber security measures is of utmost importance.

Anita Roodman, Senior Manager: Legal and Technical services, Simeka Consultants and Actuaries

As cyber threats continue to evolve and become more sophisticated, retirement funds must adopt comprehensive cyber security strategies not only to protect the sensitive data and assets entrusted to their care, but also to protect their members from suffering a financial loss through theft and fraud.

In December 2022, the Financial Sector Conduct Authority (FSCA) and the Prudential Authority published a second version of a draft Joint Standard: Cybersecurity and Cyber Resilience Requirements document for further consultation, setting out the minimum requirements and principles for sound practices and processes of cyber security and cyber resilience for categories of specified financial institutions (including retirement funds). It seeks to ensure that these financial institutions implement processes, and have tools and technology, which will prepare them for cyber attacks.

In a recent High Court case, *Hawarden v Edward Nathan Sonnenbergs Inc [2023] 1All SA 675 (GJ)*, the court dealt with the question whether a law firm is liable for a loss where a purchaser of a property fell victim to cybercrime through business email compromise (BEC). In this case, Hawarden made an offer to purchase a property and received an email from the law firm directing her to pay the purchase price to their bank account. However, Hawarden's email account had been hacked and the email received from the law firm was intercepted and altered to reflect a fraudster's bank account details. The court found that the law firm was aware of the risks of BEC prior to the incident and they had failed to warn Hawarden of possible email manipulation. The law firm did not take the necessary safety precautions to safeguard

against BEC causing harm, by conveying its bank account details via email in an unprotected pdf attachment whilst safe channels like multi-channel verification are available to prevent cyber fraud. Their omission to guard against harm was therefore found negligent.

In *Gerber v PSG Wealth Financial Planning (Pty) Ltd (36447/2021) [2023] ZAGPJHC 270*, Gerber held investments with PSG for the purpose of funding retirement. In 2019, a request was received by PSG for payment of a portion of the investment, something Gerber had never requested before. A change of banking details was also included in the email.

PSG requested a bank statement showing the new banking details. A letter was then received, seemingly from the bank, confirming the banking details and that the bank account was opened in 2002. A bank account verification check was done showing that the account did not match the client details, the account was not more than three months old, and the contact details attached to the account were not valid. PSG requested Gerber via email to confirm whether the account was indeed his, which confirmation was received from Gerber's email account.

Next, a message was received from Gerber's email account requesting another payment as well as a statement of all his investments. PSG then inquired whether a statement for his wife's portfolio was also required, which was confirmed. A withdrawal from his wife's account was then requested. PSG only then became suspicious of the email request. After a phone call to Mrs Gerber, it became clear that the Gerbers' email accounts had been hacked. The Gerbers claimed that they suffered a loss as a result of PSG's failure to exercise the skill, care and diligence to ensure that the monies held by it in trust does not fall prey to fraud.

PSG in turn alleged that the Gerbers were negligent in that they did not take all reasonable steps to protect their computer system against hacking.

The court referred to the General Code of Conduct for Financial Services Providers and Representatives (FAIS Code) and concluded that PSG had a contractual obligation to have and effectively employ the resources, procedures and appropriate technological systems to eliminate the risk that clients may suffer financial loss through theft and fraud.

It would be wise for retirement funds to pay attention to the rationale of the courts. In terms of section 7 of the Pension Funds Act, boards of management have a duty to take all reasonable steps to ensure that the interests of members are protected at all times. They further have a duty to act with due care, diligence and in good faith. Boards of management are accountable for the security of fund information and assets, even where day-to-day functions of the fund are delegated or outsourced.

From the court cases, it is clear that at least the following should be done to guard against harm to members:

1. taking steps to verify banking details (not via email);
2. avoiding processes where bank account details are sent via email;
3. using a secure transaction platform;
4. warning members about the danger of cyber fraud and explaining to members how the secure platforms work; and
5. educating fund officers on the risks of BEC fraud.

With the two-pot system being imminent, where members will be able to access a portion of their savings in their retirement fund without going through the employer claim process, processes and security measures should be put in place to prevent fraud. Member communication will become extremely important to warn members about the risks of cyber fraud.

Funds should consult with all relevant parties (third party service providers and participating employers as well as fund officers or board members) to define the fund's approach to managing cyber security risk. Even though the conduct standard is still in draft form, cyber risk is real, complex and evolving, and already requires dynamic controls, processes and response plans. These controls, processes and response plans may have to be fine-tuned to adhere to and comply with the new conduct standard. However, boards of management and joint forums of participating employers cannot wait until the implementation date to consider and prevent cyber risks.