Out of the Ordinary

Investec

Experian data breach

Frequently asked questions
For corporate clients

1. What did the Experian data breach entail?

As reported in the media on 19 August 2020, Experian - a consumer, business and credit information services agency - has experienced a breach of data. This breach originated outside of Investec and has not affected any of our systems.

For corporates, we have been advised that most of the data shared is available on the CIPC database.

Experian was successful in obtaining and executing an Anton Piller order which resulted in the suspect's hardware being impounded and the misappropriated data being secured and deleted.

2. How did the fraudsters obtain my data?

Experian's investigations indicate that an individual in South Africa, claiming to represent a legitimate client, fraudulently requested services from Experian. They are investigating the full impact of this data breach.

3. What does SABRIC and the SAFPS do?

SABRIC is the South African Banking Risk Information Centre (SABRIC). It is a non-profit company formed by the banks and cash in transit industries to combat organised bank-related crimes.

Southern African Fraud Prevention Service (SAFPS) is a non-profit organisation focused on fraud prevention and leads the fight against fraud and financial crime.

SAFPS assists in preventing fraud and impersonation as a result of identity theft to protect the public from the associated financial consequences.

4. How did my credit information end up on to this bureau's database?

The National Credit Act, aimed at curbing reckless lending, mandates that all South African banks and credit providers must submit credit information to all credit bureaus. When you apply for credit or a loan, you consent for your data to be shared.

If you are credit active, your personal information is stored with all South African credit bureaus. The information is used to make the necessary credit checks before granting a loan or credit product.

5. How could the information about me potentially be used by a fraudster?

The details obtained could potentially be used by third parties in various ways to commit fraudulent scams, such as application or tender fraud and the changing of banking details via an email hack (leads to the interception of emails and invoices that contain bank details). Those details are then changed by the fraudsters.

6. How long has Investec known that my data was breached?

Experian advised all of the banks in August 2020.

7. What is the profile of the data that the fraudsters obtained?

For corporates, we have been advised that most of the data shared is available on the CIPC database.

8. What proactive measures can we as a corporate take?

As a precaution, always verify the bank details you are paying with the third party involved and make sure that your clients know what your bank details are.

9. Is the data breach contained to South African corporate entities only?

At this point, it appears that only South African corporate and individual entities are affected.

10. What risk mitigation strategies do you have in place to protect my account from potential fraud?

Investec takes the security of our client data very seriously and we have strategies in place to detect potential fraud. We have a layered approach in our fraud detection and prevention strategy and do not rely on any single system or control to protect you. If we suspect fraud we will contact you immediately.

11. How many corporate entities have been affected by the data breach?

We have been advised that 793 749 entities have been affected.