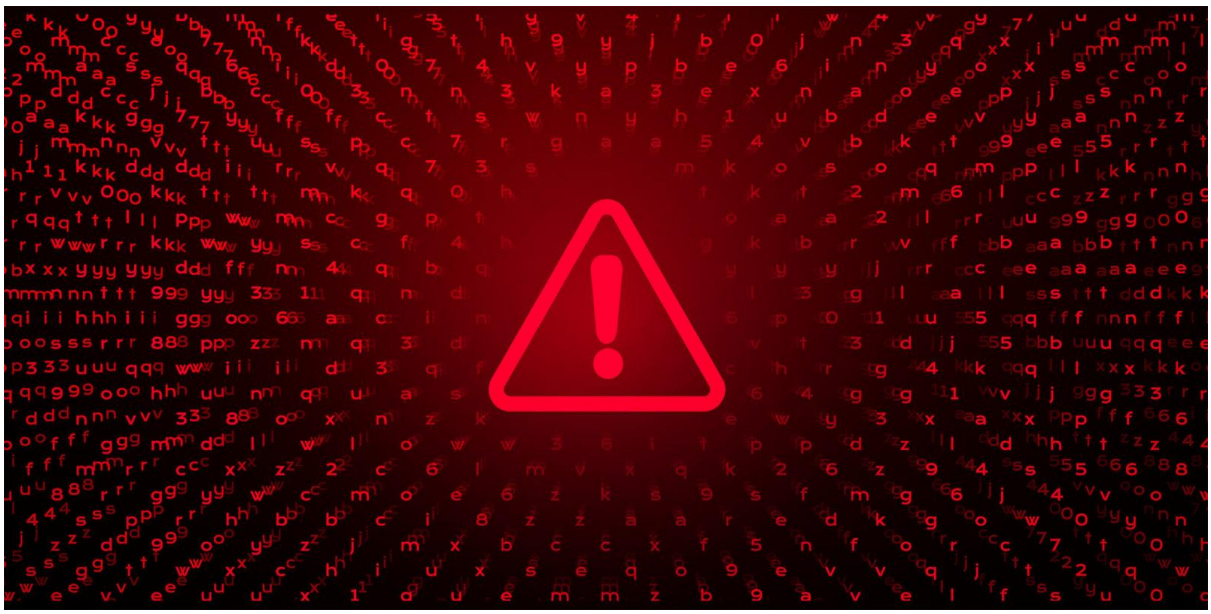
Experian offers mea culpa after massive data breach blunder

By Ray Mahlaka• 23 August 2020



(Image: Adobestock)

Credit bureau Experian has been left with egg on its face after it willingly handed over personal details of as many as 24-million consumers and nearly 800,000 businesses to a suspected fraudster. Experian insists that the data breach has been 'contained' as no consumer credit information or financial information was obtained by the fraudster.

The data breach at Experian, one of SA's largest credit bureaus, will probably go down in history as the country's largest and a self-created blunder.

Experian accidentally engineered the data breach when it willingly handed over personal details belonging to as many as 24-million consumers and nearly 800,000 businesses to an individual that it now describes as a "fraudster".

According to Experian, it was duped into handing over consumer information such as ID numbers, telephone numbers, and physical and e-mail addresses to an individual who claimed to represent the credit bureau's undisclosed client. In other words, the individual was supposedly authorised to have that confidential information, which is provided to clients "in the ordinary course of business".

The credit bureau industry holds sensitive data on millions of consumers as it collects their personal information from banks, retailers and other businesses. The industry is an important function in SA's credit system as banks, retailers and real estate

landlords collect data from credit bureaus such as Experian to determine clients' ability to pay back loans or financial fitness to enter into a residential lease agreement.

Experian insists that the data breach has been "contained" as no consumer credit information or financial information was obtained by the suspected fraudster or "has been used for fraudulent purposes".

"Our investigations also show that the suspect had intended to use the data to create marketing leads to offer insurance and credit-related services," the company said in a statement last week.

But that sensitive information landed in the wrong hands is enough to create panic — and rightly so.

Experian said it had seized the hardware that the suspected fraudster had stored the personal information in, which was then "deleted". It seized the hardware by seeking an Anton Piller order via the courts — an application that is done in secret to allow for search and seizure procedures without prior warning to the affected party to secure evidence. It's unclear if Experian launched criminal charges against the suspected fraudster.

Experian didn't respond to *Business Maverick*'s request for comment through emailed questions at the weekend by the time this article was published. But its CEO Ferdie Pieterse offered an apology to customers:

"I would like to apologise for the inconvenience caused to any affected parties." (We will update this article when we receive Experian's response)

According to *Business Insider*, Experian handed over the sensitive information to the suspected fraudster between 24 May and 27 May. The company detected the breach nearly two months later on 22 July, applied for the Anton Piller order on 13 August, and only publicly announced the data breach on 19 August.

Asked why it didn't immediately inform the public about the breach when it was discovered, Experian told *Business Insider*:

"[W]e delayed publishing the incident due thereto that the Anton Piller is reliant on the element of surprise and we, therefore, could not make the incident public."

Fines and jail time

The data breach would normally land Experian in hot water with SA's information regulator, whose office places the responsibility of safeguarding sensitive information to companies under the Protection of Personal Information Act (POPI). Under the POPI Act, the regulator could slap Experian with an administrative fine of up to R10-million or its directors could face imprisonment for a period of not more than 10 years.

But Experian and other companies are not liable to the POPI Act as sections of it came into effect from 1 July 2020 and companies have until 1 July 2021 to comply with the Act's various obligations.

Experian has already informed the information regulator, advocate Pansy Tlakula, about the data breach.

The data breach has prompted SA's banking sector to be on high alert; commercial banks including Standard Bank, FNB, African Bank, Investec, Absa and Nedbank have informed customers that they could potentially be victims of the incident.

As of Friday 21 August 2020, the banks warned customers to be vigilant as their compromised personal information could be used in identity theft attempts or to dupe customers into handing over more personal information. Although banks said the banking-specific information belonging to customers (only personal information) was not compromised, they have moved to beef up their fraud prevention/detection strategies.

Experian's data breach incident has raised important questions about the strength of its security control measures when all it takes is an imposter for sensitive information to fall into the wrong hands.

After all, incidents, where sensitive information is compromised are usually caused by external forces such as sophisticated cyberattacks — like the one faced by life insurance company Liberty, when hackers breached its IT systems in June 2018.

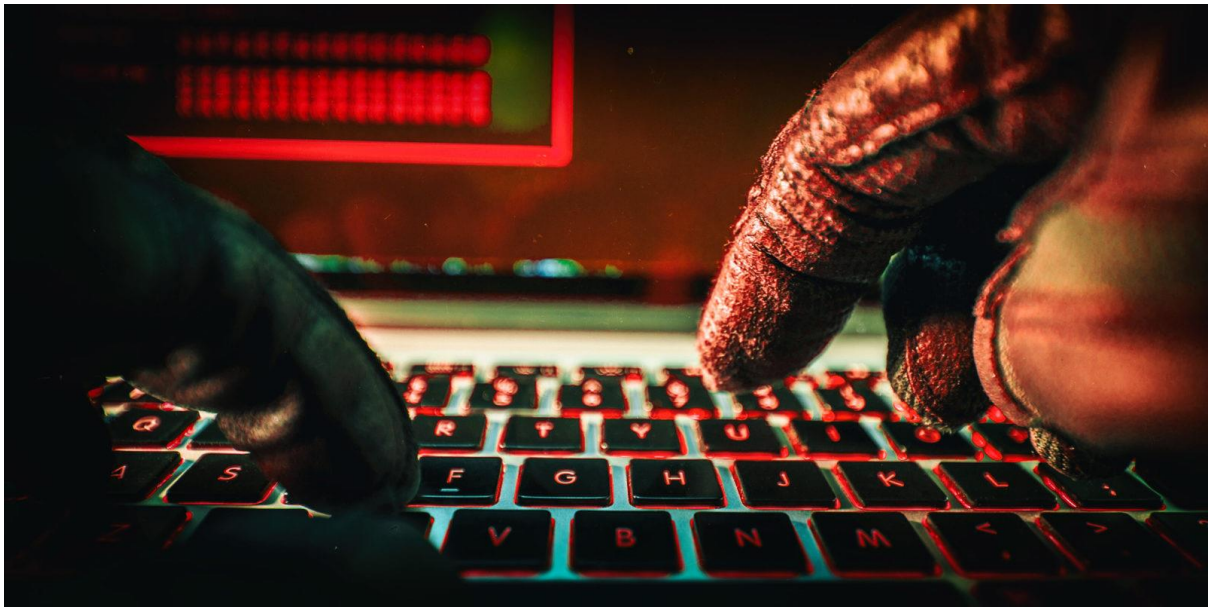
At the time, hackers claimed to have seized confidential information on Liberty systems — including banking details and medical reports of consumers — alerted the insurer to potential vulnerabilities in its IT systems and demanded payment, which the company refused. Short-term insurer Momentum Metropolitan recently said it had suffered a data breach, although it said investigations indicate that no client data had been accessed. **DM/BM**

Source:https://www.dailymaverick.co.za/article/2020-08-23-experian-offers-mea-culpa-after-massive-data-breach-blunder/

BUSINESS MAVERICK OP-ED

The unanswered questions following the Experian data breach

By Tim Cohen• 30 August 2020



If data has become the new oil, the wild peculiarities of the oil industry are going to become the new normal – and we'd better brace ourselves for it. (Photo: Adobestock)

A host of unanswered questions arises from the Experian data breach, which is really SA's first experience with a very large-scale invasion of financial privacy. But at the core, the relatively small SA example touches on much broader questions: How safe are we; how safe is our data; are we to become inadvertent victims of a new data war which rages around us, controlled by forces we can't easily see or control?

*First published in **DM168**.*

These invasions are already features of the modern digital experience around the world, and the SA example follows such varied instances as Twitter being duped out of information in July on accounts of high-profile individuals like Barack Obama, Elon Musk and Bill Gates, no less. On the other extreme, earlier this year, a cool three billion records were accessed from Clearview AI, a face recognition company.

Data breaches are becoming more regular, larger in size and more effective. If data has become the new oil, the wild peculiarities of the oil industry are going to become the new normal – and we'd better brace ourselves for it.

So what actually happened in the Experian case, and what can we learn from it? The first part of the question is actually part of the problem because the details are a bit fuzzy, possibly because the participants themselves are perhaps understandably worried about compounding the nightmare by releasing information that later turns out to be wrong.

The timeline went something like this: on 19 August renowned tech journalist Duncan McLeod reported on website techcentral that credit bureau Experian had suffered a

massive data breach, exposing the personal information of as many as 24 million South Africans and nearly 800,000 businesses to a "suspected fraudster".

McLeod was reporting on a statement released by the South African Banking Risk Centre (Sabric), which said Experian had reported the incident to law enforcement authorities and was working with "appropriate" regulatory authorities.

The centre said South African banks have put in place "robust risk mitigation strategies to detect potential fraud on accounts and protect their customers". You have to willfully suppress your cynicism at that statement, particularly since the breach was clearly not the work of a tech genius punching complicated algorithms into a laptop as Hollywood would have us believe, but it was duped out of Experian by a bog-standard con artist posing as a client. What's worse, the information was willingly handed over on nothing more sophisticated than a memory stick. Yeee-ouch!

Anyway, up to this point, Experian has said nothing. First mistake. To be fair, as soon as the information was out, Experian did put a notice on their website later in the day. But reading this statement, you would think someone accidentally spilt hot coffee on their mouse pad.

What was gleaned was information "that is provided in the ordinary course of business or which is publicly available. We can confirm that no consumer credit or consumer financial information was obtained." Turns out that last bit was kinda iffy.

They can put out a call centre request and if they know just some of your details, they can come across as a figure of authority wanting to help. Next thing, you have "refreshed" your bank password and your money is gone. If only one in a hundred falls for it, that's still 240,000 bank accounts.

Anyway, we can all rest easy. "Our investigations do not indicate that any misappropriated data has been used for fraudulent purposes," the statement said. But people should be on guard.

This is the kind of reaction we have come to know and love from what might be called the "data community". We can summarise it thus: there is a problem but it's actually not a problem, and to the extent that it is a problem, it's your problem. The headline of the story said it all: Experian data breach: It's not as bad as feared.

Well, that sort of depends on what you fear… or what you should fear. Experian said in its statement that it had identified a suspect and obtained an Anton Piller court order against them. This resulted in the suspect's hardware being impounded and the misappropriated data being secured and deleted.

But there is a problem here too. It turns out that the breach actually happened between 24 May and 27 May. The company detected the breach nearly two months later on 22 July, applied for the Anton Piller order on 13 August, and only publicly announced the data breach on 19 August.

There are some pretty big gaps here. What are the chances Experian, which offers ironically, services in combating data breaches, was kinda hoping this could all be

buried on the qt? After all, the company said: “Our investigations also show that the suspect had intended to use the data to create marketing leads to offer insurance and credit-related services.” So you see, no problem.

Well, the banks were having nothing to do with that, because there is a problem. First, if you had been caught, you would say that, wouldn’t you? What you wouldn’t say is you handed it to a friendly guy from Eastern Europe. Second, the intention of fraudsters who target what is laughingly known as “public information” is that it is used as a lever.

They can put out a call centre request and if they know just some of your details, they can come across as a figure of authority wanting to help. Next thing, you have “refreshed” your bank password and your money is gone. If only one in a hundred falls for it, that’s still 240,000 bank accounts.

And the loser here wouldn’t be Experian but the banks, who would be dealing with some very angry clients. So banks were forced to put out carefully worded statements. The aim was to ensure clients would not get paranoid about their data but also that they should be paranoid about their data, because the ultimate defence against phishing scams is not sophisticated algorithms but users themselves.

And that is the ultimate problem; banks want this to be our problem, and in some ways it is. But when you have buckets of information that can be reduced in size to a book of matches, you have what might be called a volume conundrum.

Crimes that were once impossible because of the sheer volume of data involved are now eminently possible. And putting the best possible gloss on this, the Experian example, a close shave in some ways, should be a wake-up call to us all. **BM/DM**

Source:https://www.dailymaverick.co.za/article/2020-08-30-the-unanswered-questions-following-the-experian-data-breach/