What is a data breach?

A data breach occurs when information held by an organisation is stolen or accessed without authorisation.
Criminals can then use this information when creating phishing messages (such as emails and texts) so that they appear legitimate. The message has been designed to make it sound like you're being individually targeted, when in reality the criminals are sending out millions of these scam messages. Criminals may even send messages pretending to be from an organisation that has suffered a recent data breach.
Even if your details are not stolen in the data breach, the criminals will exploit high profile breaches (whilst they are still fresh in people's minds) to try and trick people into clicking on scam messages.

Has Fawry suffered a data breach?

We believe a ransomware hacker gained access to an isolated part of Fawry systems which we use to test new products and changes to our live platform.
At the time, the personal details of some customers were present on this testing platform, including information such as home addresses, email addresses, phone numbers and dates of birth. We believe the hackers may have downloaded some or all of this data and that it may or may not be published online.
Fawry remains confident that this data will not impact on the safety or security of financial transactions on its platform, but you should exercise caution and be on alert because criminals can use this information when creating phishing emails or texts, that are designed to look like they have come from a legitimate source.

How does this affect you?

None of the data stolen in the cyber-attack poses a security risk to you. Similarly, no Fawry customers have lost any money. You can continue to use Fawry's live platform with confidence that it has always remained secure.

What do you need to do?

Unless you suspect suspicious activity (see 'How to keep yourself safe'), no customer action is required. If it is advisable to update your security information – such as passwords – we will be in touch directly through our official channels.

How to keep yourself safe.

We will only ever contact you by [email/text message/phone]. If you receive an approach from someone claiming to be from Fawry on any other channel, this is likely to be a scam.
We will never ask for your account details or passwords. If you receive an approach from someone asking you to confirm your account number, passwords or transactions, this is likely to be a scam.
Typical scams also involve messages claiming to be from an organisation that has suffered a recent data breach that may ask you to log in to verify your account or reset your password. These scam messages often contain links to websites that look genuine, but which store your real details once you've typed them in.

If you suspect suspicious activity.

If you believe you have been subject to phishing approach or that your account might be at risk, please call our customer support team on: 16421 or visit our website www.fawry.com

How will you stop this happening again?

We are working with Group-IB, a multinational cyber threat consultancy, to continue providing active monitoring of Fawry's systems for the foreseeable future and validate the need for any extra security measures as required, as they have advised for other international banks who have suffered similar data breaches.
Group-IB and Fawry are continuing their investigation into the incident and will work with the relevant authorities to implement best practices to prevent a similar attack in the future.
In addition, Fawry is in active discussions with a range of global consultancy firms to review the group's policies for governance and risk assessment to advise on the adoption of the latest international frameworks.
The safety and security of our customers' assets remain our absolute priority, and we are committed to take all necessary steps to avoid similar incidents in the future.