Flagship Group

FAQs following recent cyberattack

What happened?

Online criminals gained access to our onsite data centre, via a cyberattack. The hackers released a ransomware virus, which accessed our network, encrypting our databases and compromising some personal staff and customer data. Our forensic investigation has so far identified that a small amount of data was also removed from our network.

When did the company learn of the incident?

On Sunday 1 November 2020, we became aware of a major IT incident, that took most of our systems offline, and limited some of our services. On discovering the incident, as a precautionary measure, we immediately took all our systems offline to prevent the issue spreading further.
We found out the severity of the incident on 4 November 2020 and issued an official statement via our website, social media, and the press. We commenced a forensic investigation which is still ongoing.

What steps should I take?

We recommend that customers be vigilant in reviewing their account statements and credit reports, and that they immediately report any unauthorised activity to their bank. We also recommend that they monitor their personal information and visit ***https://ico.org.uk/your-data-matters/identity-theft*** to obtain information about steps they can take to better protect against identity theft.

CONTINUED

Do I need to change my passwords?

We recommend that customers be extra vigilant, report any suspected phishing attempts to the authorities and amend passwords to prevent login attempts from third parties.

Why are you only just notifying me? I already know about this from a third party.

To prevent the issue spreading further, we immediately took our systems offline. However, this limited the number of secure communication channels available to notify customers. We issued our initial statement through social media, a website holding page and via the press, to help notify more customers simultaneously. As our investigation progresses, we are updating and contacting affected individuals.

Who has been affected and what information may have been impacted?

We can confirm that despite our quick action to contain the attack, it now appears from our ongoing forensic investigations that some personal customer and staff data has been accessed and the ongoing forensic investigation has suggested that, to date, a small amount of data has been extracted from our network. As our investigation progresses, we will continue to provide updates, via our website and social media, as appropriate. We are also updating and contacting affected individuals.

Why are my details incorrect?

We have contacted all customers based on the most recent secure data we have. We apologise if we've made a mistake. We kindly ask that you get in touch with us to update your contact details.

CONTINUED

Is this a new cybersecurity incident?

There has NOT been an additional incident. These FAQs are based on our ongoing investigation of the cybersecurity incident announced November 4, 2020.

Is the issue contained?

We have taken steps to stop the spread of the attack, which have been successful.

How did this happen?

We have been intensely investigating the scope of the intrusion, with the assistance of a leading, independent cybersecurity firm, to determine what information was accessed, how this happened and who has been impacted. We continue to work with the Police and other third parties as part of their criminal investigation.

What are you doing to prevent this happening again?

We engaged a leading, independent cybersecurity firm to conduct an assessment and to advise us on the implementation of measures to help prevent this type of incident from happening again.

We take the privacy and security of our customer and staff data very seriously and we have high levels of security measures in place to protect data. Following the attack, we have been working closely with our internal team and specialist advisers to review and monitor our cybersecurity practices on an ongoing basis.