FAQs following recent cyberattack

What happened?

Online criminals gained access to our onsite data centre, via a suspected phishing attack. The hackers released a ransomware virus, which accessed some personal staff and resident data. Whilst data was encrypted, we are confident that this can be recovered from backup data. To date, there is no evidence of the data being stolen.

What's changed since the last official statement?

There has been, and continues to be, an investigation into the attack and to date, there is no evidence of customer or staff data being stolen.

What is the difference between compromised, accessed, encrypted, and stolen?

"Compromised" means that someone or something has maliciously accessed data, without permission, and could have done some damage. In this case, the attackers compromised our data centre.

"Accessed" means that the data was viewed. We are aware that these attackers accessed some personal staff and resident data.

"Encrypted" means that data has been changed into another form, or code, so that only people with a password can read it. Whilst some of our data was encrypted, we are confident that this can be recovered.

"Stolen" also known as data theft, is the act of stealing digital information stored on computers, servers, or electronic devices with the intent to sell confidential information. Based on our investigation, to date, there is no evidence that resident or staff data has been stolen.

CONTINUED

When will we know more?

Our investigation continues with the Information Commissioner's Office (ICO), but we will release a statement following its conclusion.

When did the company learn of the incident?

On Sunday 1 November 2020, we became aware of a major IT incident. As part of our controlled response, we took most of our IT systems offline and in the short term, the attack limited us to emergency operations. 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.

What steps should I take?

We recommend that residents 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.

Do I need to change my passwords?

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

CONTINUED

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

Despite our quick action, some personal resident and staff data has been accessed, however, the ongoing forensic investigation has suggested that, to date, there is no evidence of the data being stolen. We will continue to provide updates, via our website and social media.

How do I get in touch whilst your systems are down?

Our teams are working tirelessly around the clock to bring our systems back online, and we apologise for any inconvenience this may have caused. You can still contact us on Twitter *@SuffolkHousing*, by telephone *01284 767 224* or by email *enquiries@suffolkhousing.org*

Can I still pay my rent?

Yes, our phone lines are back up - please call *01284 767 224* to pay your rent.

I need a repair – what should I do?

To book a repair, please call *01284 767 224*.

Is this a new cybersecurity incident?

There has NOT been an additional incident. These FAQs are based on our findings from 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.

CONTINUED

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 and who has been impacted. We continue to work with the Police and other third parties as part of our criminal investigation.

What are you doing to prevent this happening again?

We take the privacy and security of our resident and staff data very seriously, and we are reviewing our cybersecurity practices with internal and external specialists.