Data Breach Q&A

1. **When did you become aware of the breach?**

We became aware of the breach on Monday, 16th September 2024. Upon discovering it, we took immediate steps to ensure no further data was compromised.

2. **How did the breach happen?**

The breach was due to a cyber-attack. The issue that allowed the attack to succeed has now been closed so our system is once again fully secure, and we have engaged experts to ensure it remains so.

3. **What type of personal data was involved?**

The information exposed included customer names, phone numbers, addresses and email addresses (where provided). No financial information or passwords were exposed.

4. **Have passwords, financial details or sensitive information been affected by the breach?**

The only information taken is customer names, company name (if provided), telephone numbers, addresses and email addresses.

5. **What does this breach mean for me?**

Your personal data was impacted, with the following being exposed (where provided):

- Name
- Company name (if stated)
- Telephone number
- Address
- Email Address

We are not aware that your personal data has been misused in any way, however, due to the exposure of your details, we would advise that you are highly vigilant to the risk of fraud. For example, there is the potential for you to receive phishing emails through which you may be impacted.

6. **Has my personal data been retrieved?**

Your personal data was exposed, so while we are not aware that it has been misused in any way, there remains a possibility that your data could be used to scam you. While no financial or password data has been exposed, you should be vigilant to the risk of fraudsters using your contact details (e.g. phone, email address) to attempt to get more sensitive information from you. Please read the detailed advice below to ensure you know how to protect yourself.

7. What should I look out for?

We are contacting all individuals affected by this data breach, and we strongly encourage you to take the measures outlined to protect yourself from any possible risk.

In particular, you should look out for phishing emails or emails that look suspicious (e.g. emails you receive that you are not expecting). You should also keep an eye out for any fraudulent activity on all your accounts. If you receive suspicious SMS/Texts, always forward them to 7726. No matter which mobile operator you use, this number is used in the UK to report SPAM.

The following websites are useful resources for any concerns you may have about data security:

How to spot a scam email, text message or call:
https://www.ncsc.gov.uk/collection/phishing-scams/spot-scams

How to understand unusual activity:
https://ico.org.uk/your-data-matters/identity-theft/
https://ico.org.uk/media/1042838/personal_information_toolkit.pdf
https://www.met.police.uk/advice/advice-and-information/fa/fraud/personal-fraud/identity-fraud/

How to report emails, texts, websites, adverts or phone calls that you think are trying to initiate scams: https://www.ncsc.gov.uk/collection/phishing-scams

8. Can I be confident that my data is secure?

We are very sorry for the inconvenience caused on this occasion. But rest assured, we take our customers' data extremely seriously. We have taken immediate steps to secure all data (supported by a cyber security expert) to ensure that our processes and systems remain as secure as possible going forward.

9. When was your cyber security last tested? How regularly are they tested?

An external award-winning security company tests our loyalty app and website, they run complete 360 tests at least once a year, or before any significant changes. Along with this, we use different companies to run weekly and monthly external security scans to validate our development partners' Secure Development Life Cycle. Our eCommerce is PCI-DSS compliant and is validated by external auditors annually.

10. Who should I contact if I have any additional questions?

If you have any further queries, please do not hesitate to contact us at dataenquiries@harveynichols.com.