



Beacon CRM Cyber-Security Incident – FAQ

Published 4 August 2026

We are sorry that information held for MCR Pathways in Beacon CRM may have been affected by a cyber-security incident. We understand that this may be concerning. This FAQ explains what we currently know, the information that may be involved, what action MCR Pathways has taken and the simple steps you can take to stay safe.

The investigation is continuing. We will update this FAQ if material new information becomes available.

Need help or have a question?

Email: incident@mcrpathways.org

Telephone: 0141 221 0200

1. What has happened?

Beacon CRM, a third-party system used by MCR Pathways, has told customers that it experienced unauthorised access to its systems. Beacon's current understanding is that compromised credentials were used to gain access and copies of database backups were made. Beacon has said that it has not conclusively confirmed the copying or taking of customer data, but the evidence currently suggests that the backup copies were likely downloaded.

2. What is Beacon CRM and why does MCR Pathways use it?

Beacon is a customer relationship management system. MCR Pathways uses it for fundraising, supporter engagement, and some fundraising-event administration. Beacon processes this information on our behalf as our data processor.

3. Was MCR Pathways itself hacked?

No. The incident involved unauthorised access to Beacon's systems, not MCR Pathways' wider IT systems or network. Beacon is a third-party platform that we use for specific fundraising, supporter and partnership information.

We have no evidence that MCR Pathways' other systems were accessed or affected. This includes the separate systems used to hold young people's case, mentoring and safeguarding information.

MCR Pathways remains responsible for the personal information we chose to store in Beacon, so we are assessing the potential impact and responding to the incident as the data controller.

4. Who may be affected?

People whose information was held in MCR Pathways' Beacon account before 5am BST on Monday 27 July 2026 may be affected. This may include current or former donors, fundraisers, event participants, supporters, or newsletter subscribers. Not every person has the same types or amount of information recorded.

5. What information may have been involved?

Depending on your relationship with MCR Pathways, the information may include some of the following:

- your name and contact details, such as email address, telephone number or postal address;
- your relationship with MCR Pathways and relevant organisations;
- donation dates and amounts, fundraising activity and Gift Aid information;
- event participation, communication preferences and contact history;
- a date of birth, where one had been provided; and
- for a small number of people, personal information provided in a fundraising-event application.

MCR Pathways has completed a detailed review of the fields used in Beacon. We are reviewing the small number of records containing more personal event-application information separately and will contact individuals directly where appropriate.

6. What information was not held in Beacon?

Our review has established that the MCR Pathways information held in Beacon does not include:

- bank-account details or payment-card information;
- passwords or authentication credentials;
- passport details, driving-licence details or National Insurance numbers; or
- identified young people's case, mentoring or safeguarding records.

Young people's case, mentoring and safeguarding information is held in separate systems.

7. Does this give someone access to my bank account, card or online accounts?

No bank-account or card information is held in Beacon for MCR Pathways' fundraising function, and our Beacon records do not contain passwords or authentication credentials. This incident does not itself give someone access to your bank account, card or online accounts. However, contact details and knowledge of your relationship with MCR Pathways could be used to make a scam message appear more convincing.

8. What is the main risk to me?

For most people, the most realistic risk is receiving a targeted phishing email, text message or telephone call. A scammer might refer to MCR Pathways, Beacon, a donation, a fundraising event or another detail to encourage you to click a link, make a payment or reveal further information. The fact that information may have been involved does not mean that it has been misused or that you will experience harm.

9. What should I do?

You do not need to take any urgent financial action solely because of this incident. We recommend that you:

Be cautious about unexpected emails, messages or calls claiming to be from MCR Pathways, Beacon or a fundraising platform.

Do not click an unexpected link or attachment, make a payment through an unsolicited link, or share passwords, security codes, bank details or card information.

Check a request independently by contacting the organisation through details on our official website (www.mcrpathways.org) rather than using contact details in the message.

Be alert to pressure, urgency, requests for secrecy or messages that ask you to act immediately.

Report suspicious messages and any actual fraud using the trusted routes in question 11.

10. Do I need to change my passwords or contact my bank?

Because passwords, bank details, card details and other authentication credentials are not stored by MCR Pathways in Beacon, you do not need to change passwords or contact your bank solely because of this incident.

If you have responded to a suspicious message, shared financial information or noticed unusual activity, change your passwords and contact the account provider or bank immediately using a trusted number.

11. Where can I report a suspicious message or fraud?

The National Cyber Security Centre provides advice and a route for reporting suspicious emails, websites, text messages and calls:

ncsc.gov.uk/collection/phishing-scams

If you believe you have experienced fraud, report it to Action Fraud:

actionfraud.police.uk or call 0300 123 2040. In Scotland, reports of fraud can also be made to Police Scotland by calling 101.

12. What has MCR Pathways done in response?

MCR Pathways began its investigation promptly on 3 August 2026, the day we were informed. We have:

- reviewed the categories of information held in our Beacon account and assessed the potential risk to individuals;
- reported the personal data breach to the Information Commissioner's Office within 72 hours of becoming aware of it;
- replaced all API keys connected with our Beacon account;
- reviewed connected services, integrations and access arrangements as part of securing the account;
- continued to seek information and assurance from Beacon as its investigation progresses; and
- prepared advice for people who may be affected and a process for contacting individuals directly where appropriate.

13. Has the data definitely been downloaded or misused?

Beacon has said that data exfiltration has not yet been conclusively confirmed, although the evidence currently suggests that copies of database backups were likely downloaded. MCR Pathways has not been informed of evidence that its information has been misused. We are taking a precautionary approach while the investigation continues.

14. Will MCR Pathways contact me directly?

Based on the information currently available and our assessment of the likely impact, we consider that the incident presents a low risk for the great majority of people whose information was held in Beacon. Their information does not meet the threshold of presenting a high risk to their rights and freedoms, so they will not receive an individual notification about the incident. This public notice and FAQ provide the relevant information and practical advice for those people.

A very small number of records linked to the application process for one specific fundraising event contain more private information. These records may present an elevated level of risk and are being reviewed separately. We will contact the individuals concerned directly to explain what information may have been involved and provide any specific advice that may be appropriate.

We will keep our assessment under review. If further information from Beacon changes our understanding of the incident or indicates that anyone else faces a higher risk, we will contact those individuals directly.

15. How will I know if the position changes?

We will update our website and this FAQ if we receive material new information. Where an update is particularly relevant to an individual, we will contact them directly where appropriate.

16. How will I know that a message from MCR Pathways about this incident is genuine?

Any direct communication from MCR Pathways about this incident will come from an official MCR Pathways email address. We will not ask you to provide a password or security code, make a payment, or give us bank-account or payment-card information.

If you are uncertain whether a message is genuine, do not click any links or use the contact details contained within it. Contact us independently at incident@mcrpathways.org or through the contact details published on the MCR Pathways website.

17. What does “attachments” mean?

An attachment is a file that was uploaded and stored directly within a Beacon record, such as a document or other supporting file. We are reviewing the attachments held in our account as part of our assessment.

18. Why did MCR Pathways retain my information?

MCR Pathways retains different types of information for different periods, depending on why it was collected and any legal, financial or regulatory requirements that apply. For example, some donation and Gift Aid records must be retained for financial and tax purposes.

19. What can I do if I am unhappy with MCR Pathways' response?

If you have concerns about how MCR Pathways has handled your personal information or responded to this incident, please contact:

Colin Adam - Data Protection Lead
incident@mcrpathways.org

You also have the right to raise a concern with the Information Commissioner's Office. Information about making a complaint is available at www.ico.org.uk/make-a-complaint.

20. Who can I contact with questions or concerns?

Email: incident@mcrpathways.org
Telephone: 0141 221 0200