c/o PO BOX 481
Fareham
Hampshire
PO14 9FS

Tel: 02380 478922
Email: npcc.foi.request@cru.pnn.police.uk

28/04/2023

**FREEDOM OF INFORMATION REQUEST REFERENCE NUMBER: 133/2023**

Thank you for your request for information regarding ACRO data breach investigation; which has now been considered.

**Applicant Question:**

I would appreciate an explanation as to how and why my data was breached. Please inform me when you reported this matter to the Information Commissioner's Office and what the outcome of the Information Commissioner's Office investigation has been.

I also want to know what actions Acro has taken to prevent a similar breach from happening in the future. It is important that the company takes the necessary steps to prevent any further compromise of customer data. I would like to know about the security measures that were in place before the breach occurred, and what additional measures have been implemented since the breach was detected.

Please provide me with detailed information about the security systems that were in place, including how they were designed to protect customer data, and what monitoring systems were in place to detect breaches. Also, please outline the steps Acro has taken to address the breach and to provide support to affected customers.
I also request the following:

1. A copy of your Data Protection Policy;
2. Your Customer Privacy Notice;
3. A copy of the Breach Register entry relating to this matter;
4. Any Data Protection Impact Assessment carried out relating to your internal processing which relates to the processing of my data;
5. Your Policy on/concerning data retention periods;
6. Your internal investigation documents concerning this matter;
7. Any correspondence with any other organisation concerning this matter.

**NPCC Response:**

Unfortunately, your request exceeds the fees limit as outlined by the Secretary of State in that to ascertain exactly what information may be held by the NPCC, would take longer than 18 hours. This response serves as a refusal notice under Section 17 of the Freedom of Information Act 2000 (the Act). Please see the legal annex for further information on the exemptions applied in respect of your request.

To assist you further, I can confirm that to comply with question 7 would require a manual review of a number of mailboxes, across several internal departments, to retrieve emails to all external organisations in relation to this matter.

We have identified engagement is required with more than 9 internal departments, and in excess of 25 staff to interrogate their mailboxes for any correspondence with external organisations. We have further identified in excess of 100 organisations in correspondence with ACRO about this matter.

As an estimate we requested 1 member of staff to complete retrieval of their emails in relation to 1 of these organisations. This search retrieved 250 emails from the date of the incident. Taking a conservative estimate of 30 seconds per email to establish if the content related to the cyber breach, this amounts to 125 minutes. To achieve this across all organisations identified would take an estimated 12,500 minutes, or 208 hours. This would then need replicating for each staff member and department identified as liaising with external organisations.

In wishing to assist you, outside of the Freedom of Information Act and as a gesture of good will, my colleagues have provided the information below in relation to your questions;

"The customer portal on the website was taken off line on the same day we were made aware of a potential issue. There is an information page available for customer information, providing email addresses for applicants to use to apply for ACRO products. Our website remains offline. We are working to implement a new website, which will be the subject of rigorous assurance, security testing and governance. This will include a Data Protection Impact Assessment (DPIA).

We follow a wide range of data protection principles on a day-to-day basis to ensure the correct processes are in place to safeguard customer information; however there is no specific DPIA for data processing in these specific circumstances. There is no legal requirement have a DPIA in place for processes that were implemented before May 2018."

In addition to this response letter is a redacted copy of the ACRO Data Breach Guidance and Privacy Policy which may be helpful to you.

A consideration would be for you to make a further request omitting question 7 or restricting any communication to specific organisations or departments. However, further FOI exemptions may apply.

Yours sincerely

Justine Brisley

www.npcc.police.uk

**COMPLAINT RIGHTS**

Internal Review

If you are dissatisfied with the response you have been provided with, in compliance with the Freedom of Information legislation, you can lodge a complaint with NPCC to have the decision reviewed within 40 working days of the date of this response. The handling of your request will be looked at by someone independent of the original decision, and a fresh response provided.

It would be helpful, if requesting a review, for you to articulate in detail the reasons you are not satisfied with this reply.

If you would like to request a review, please write or send an email to NPCC Freedom of Information, c/o PO Box 481, Fareham, Hampshire, PO14 9FS.

## Annex A

Section 17 of the Freedom of Information Act 2000 requires the NPCC, when refusing to provide information by way of exemption in question and (c) states why the exemption applies. In accordance with the Freedom of Information Act 2000 this letter acts as a refusal notice to those aspects of your request.

**The legislation: Section 12 – the legislation:**

The provisions of section 12(1) of the Act are engaged in response to your request as the NPCC are unable to confirm what information it might hold in relation to your request because to do so would exceed the 'appropriate limit' – i.e. the cost limit. Section 12 of the Act provides:

**(1) Section 1(1) does not oblige a public authority to comply with a request for information if the authority estimates that the cost of complying with the request would exceed the appropriate limit.**

(2) Subsection (1) does not exempt the public authority from its obligation to comply with paragraph (a) of section 1(1) unless the estimated cost of complying with that paragraph alone would exceed the appropriate limit.

These sections of the Act provide that the NPCC is not obliged to comply with its duties under section 1(1) of the Act – i.e. our duty to confirm or deny what information is or is not held, and to supply any information held in response to a request – if to do so would exceed the 'appropriate limit'.

The 'appropriate limit' is defined in the Freedom of Information (Appropriate Limit and Fees) Regulations 2004. Section 3 and 4 of these regulations provide that an authority can take into account the costs it reasonably expects to incur in relation to a Freedom of Information request in regards to the following four activities associated with handling that request:

(a) Determining whether or not it holds the information
(b) Locating that information, or document(s) which might contain the information
(c) Retrieving the information, and
(d) Extracting the information from a document containing it

The regulations then confirm that the appropriate limit (in the case of a body such as the NPCC) is £450 and that any work estimated or carried out in respect of the above four activities is to be estimated at a rate of £25 per hour.

Therefore, the NPCC can refuse to handle an FOI request for information under section 12 of the Act if it reasonably estimates that it would take more than 18 hours of work to carry out the above four activities in relation to that request. If the limit is exceeded**, there is no requirement for the NPCC to conduct work up to that limit – the limit applies to the whole request and there is not a requirement to answer other parts of a request even if only one area of the request on its own engages the limit.**

**Legislation – Section 16**

(1) It shall be the duty of a public authority to provide advice and assistance, so far as it would be reasonable to expect the authority to do so, to persons who propose to make, or have made, requests for information to it.