
From: Mandy Stevens <mandy.stevens@vet-ct.com>
Sent: Thursday, April 10, 2025 5:54 AM
To: Consumer Protection Mailbox
Subject: Data breach report

You don't often get email from mandy.stevens@vet-ct.com. [Learn why this is important](#)

Good morning,

We had a data breach as outlined below that may have impacted 1 Idaho resident.

At approximately 9.00 a.m. BST on Monday 7th April 2025, we became aware of a potential data breach.

During their morning meeting, the finance team reported suspicious activity in their email accounts and immediately informed the IT team.

The suspicious activity was that the Finance Director had emailed the Accounts Payable team asking for an invoice to be paid. This invoice was queried at the morning meeting and the Finance Director had not sent the email requesting this payment although it had appeared to come from her email account.

The IT team investigated immediately and found that an IP address in Russia had compromised the Finance Director's account.

There was no evidence of any documents being downloaded or forwarded from the system.

However, within the 10,000 sent items was a copy of a 1099 which contained the employees SIN number and home address. We have informed the employee and we are arranging credit monitoring support.

Please let me know if you require any further information.

Kind regards
Mandy

--

Mandy Stevens (she/her)
People Manager

Need support?

I'm always here to help—feel free to reach out anytime or schedule a meeting via this [link](#). For additional external support, our [Employee Assistance Program \(EAP\)](#) is also available.

