MEMO

To: All Staff

From: Help Desk

Date: June 10, 2024

RE: **Important Cybersecurity Incident**

We are writing to make you aware of a recent security incident involving Cisco's Duo multi-factor authentication service that has impacted our organization.

On April 25, 2024, Cisco disclosed that an attacker compromised a Duo cloud service and gained unauthorized access to customer data. This included phone numbers, carrier information and SMS logs used for multi-factor authentication.

Our security team has analyzed the data and notified staff members whose information was exposed.

If you were not contacted, your Duo account details were not part of this incident. However, it's always prudent to review your accounts for any suspicious activity.

Protecting Against Phishing
One of the primary risks from this incident is increased phishing attempts targeting our staff. Attackers may try to trick you into sharing login credentials or other sensitive data.

To protect yourself and our organization:
- Be extremely cautious of any unsolicited emails, texts, phone calls or other communications asking for your login credentials or personal information.
- Verify the legitimacy of any such requests by contacting the sender directly using known contact information - do not use the contact details provided in the suspicious message.
- When in doubt, do not respond and report any suspected phishing attempts to Help.Desk@tbh.net
- Use unique, complex passwords for all your accounts and enable multi-factor authentication wherever possible.

Our team is actively monitoring for any threats related to this incident. Please stay vigilant and let us know if you have any other concerns.

Thank you for your attention to this important matter. If you have any questions please reach out help.desk@tbh.net.

Exceptional **care** for every patient, every time.

STRATEGIC PLAN
2026