

Alabama Board of Nursing Cyber Security Incident

What happened?

Upon learning of a recent cybersecurity incident, the **Alabama Board of Nursing** immediately coordinated with the **Alabama Office of Information Technology (OIT)** and outside cybersecurity specialists, including a third-party incident response team. These entities worked collectively to contain the unauthorized activity, investigate the scope of the occurrence, plan for restoration services, and strengthen ABN's technology environment. The Board is cooperating with the Federal Bureau of Investigations and the Alabama Law Enforcement Agency concerning the incident.

A comprehensive forensic investigation identified suspicious activity within the Board's technology environment in August 2026 and further confirmed malicious activity within portions of the Board's technology environment as of September 1, 2026.

Does ABN know what information was taken?

Prompt containment actions successfully prevented this ransomware attack from further escalation, but investigators confirmed that some data was collected and downloaded. Although forensic limitations from the ransomware deployment mean the investigation could not establish definitively if information belonging to every Alabama nurse, applicant, licensee, or member of the public was fully accessed, the Board has reason to believe that data containing Sensitive Personally Identifying Information (SPII) and/or Protected Health Information (PHI) may have been exposed. This data environment could have included information such as licensee names, dates of birth, Social Security numbers, driver's license numbers, professional licensing information, and medical information.

What is ABN doing in response?

In compliance with state security protocols, the Board and the Alabama Office of Information Technology took the affected systems completely offline, contained the known malicious footprint, and are in the process of progressively restoring secure services. Enhanced cybersecurity controls, advanced network monitoring tools, and additional credential authentication practices have been and will continue to be deployed to mitigate the risk of future incidents.

What steps can nurses and other individuals take?

Pursuant to Alabama law, the Board recommends that all licensees, applicants, and stakeholders review the following protective measures against identity theft and fraud:

- **Be alert for phishing and impersonation attempts.** Exercise high caution regarding unexpected emails, text messages, or telephone calls referring to nursing licenses, renewals, fees, account verification, this cybersecurity incident,

refunds, investigations, or credit monitoring. Do not click unexpected links, open unverified attachments, or provide personal info.

- **Use strong, unique passwords.** Immediately change the password for any personal or employment account where you reused the same or a similar password associated with your Board-related portal. Ensure you do not reuse passwords across government, banking, personal email, and social media platforms.
- **Enable multifactor authentication (MFA).** Turn on MFA wherever available, particularly for your primary email, financial, healthcare, and employment accounts.
- **Review financial and identity-related activity.** Regularly monitor bank statements, credit card statements, credit reports, insurance explanations of benefits (EOBs), and tax accounts for any unauthorized or unrecognized activity.
- **Consider a credit freeze or fraud alert.** Placing a credit freeze on your file is entirely free, does not impact credit scores, and prevents unauthorized individuals from opening new accounts in your name. Alternatively, a fraud alert warns potential creditors to perform extra identity verification. You may also wish to commence credit monitoring or ID theft protections offered by third parties.
- **Report suspected identity theft.** If you discover unauthorized transactions or suspect identity theft, notify your financial institution immediately. You can also file a formal report and receive a customized recovery blueprint through the Federal Trade Commission's official resource at [IdentityTheft.gov](https://www.identitytheft.gov).

Individuals should exclusively rely on verified updates published via the [Alabama Board of Nursing Official Website](#). The Board will never proactively ask you to provide account credentials or passwords via email, text message, or unsolicited phone calls. Additional individual notices or public updates will be deployed as material new facts or further statutory reviews dictate.

The Alabama Board of Nursing deeply regrets any disruption or concern this event has caused the nursing community, employers, and the public. We appreciate your continued patience as we securely finalize our system recovery.

Questions and Contact Information

Questions or inquiries regarding this incident and notice may be directed to:

cybersecurityevent@abn.alabama.gov

Alabama Board of Nursing
P.O. Box 303900
Montgomery, Alabama 36130-3900