



December 1, 2025

By e-mail only to: regcomments@gcb.nv.gov

Nevada Gaming Control Board
Attention: Executive Secretary
7 State of Nevada Way
Las Vegas, Nevada 89119

RE: Request for consideration of a change to Regulation Reg. 5.260
For presentation to the Nevada Gaming Control Board
At its workshop dated December 4, 2025

Dear Chairman, Members, Executive Secretary and Board Staff:

On behalf of the Nevada Resort Association, we respectfully submit our comments on the proposed amendments to Regulation 5.260.

Regulation 5.260 addresses cybersecurity. More specifically, Regulation 5.260 4 directs the actions of a covered entity that experiences a cyber attack to its information system resulting in a material loss of control, compromise, unauthorized disclosure of data or information. Regulation 5.260 4(a) specifically states:

(a) ~~Provide written notification~~ Notify the Chair of the cyber attack ~~to the Board~~ as soon as practicable but no later than ~~72~~ 24 hours after becoming aware of the cyber attack.

Regulation 5.260 4(c) specifically states:

(c) Provide the Board with written updates regarding the cyber attack incident every 30 days from the initial reporting until the cyber attack incident is fully resolved and documented.

Request for maintaining the 72-hour reporting deadline in Regulation 5.260 4(a)

This public statement asks the Nevada Gaming Control Board to consider maintaining the current 72- hour timeframe based on practical application and industry experience. Most vendor contracts require notification to the covered entity within 48 hours of discovering a cyber incident. If a vendor uses the full 48 hours permitted under contract, the covered entity may

reasonably require the remaining 24 hours to review the vendor's report, conduct its own initial assessment, and prepare an informed notification to the Chair.

We also note that the General Data Protection Regulation (GDPR) sets a 72-hour reporting standard for notifying government entities of data breaches. Aligning Regulation 5.260 with this established and reasonable standard would provide licensees with the time needed to develop a meaningful and accurate analysis and mitigation plan while ensuring timely communication to the Nevada Gaming Control Board.

Request for clarification regarding the requirements of “fully resolved and documented” in Regulation 5.260 4(c)

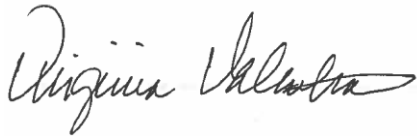
This public statement seeks to understand the Nevada Gaming Control Board's intent in Regulation 5.260 4(c) regarding who reports and what contents are required in the written update. We respectfully seek clarification as to whether it is the Nevada Gaming Control Board or the covered entity which determines whether the “incident is fully resolved and documented.” Respectfully, we also request more clarity on what information is required to be included in the “written update” to support consistent reporting across licensees and ensure compliance.

This public statement asks the Nevada Gaming Control Board to consider:

(c) Provide the Board with written updates regarding the cyber attack incident every 30 days from the initial reporting until the covered entity reports the cyber attack incident is fully resolved and documented.

Thank you for your consideration.

Sincerely,

A handwritten signature in black ink, appearing to read "Virginia Valentine", with a stylized flourish at the end.

Virginia Valentine
President & CEO