American Bankers Association

Naomi Camper
Chief Policy Officer
202-663-5461
ncamper@aba.com

December 13, 2023

The Honorable Charles Schumer
Majority Leader
United States Senate
Washington, D.C. 20510

The Honorable Mitch McConnell
Minority Leader
United States Senate
Washington, D.C. 20510

Re: S.J. Res. 50 - A joint resolution providing for congressional disapproval under chapter 8 of title 5, United States Code, of the rule submitted by the Securities and Exchange Commission relating to "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure"

Dear Majority Leader Schumer and Minority Leader McConnell:

The American Bankers Association (ABA) welcomes and strongly supports S.J. Res. 50, a joint resolution providing for congressional disapproval of the rule submitted by the Securities and Exchange Commission (SEC) relating to "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure."

On July 26, 2023, the SEC adopted final rules for new disclosures requiring registrants to publicly report—including immediately on Form 8-K—any cybersecurity incident they determine to be material; to describe the material aspects of the incident's nature, scope, and timing; and to describe its material impact or reasonably likely material impact on the registrant. The registrant will be required to make this disclosure four business days after it determines that a cybersecurity incident is material, unless the Attorney General determines that disclosure would threaten national security or public safety.

The banking industry is committed to protecting customers and their data from cyberattack. Banks are already required to report computer security incidents to their primary regulator and notify their customers if their data is stolen. Fighting cyberattacks is critically important, but the SEC's cyber disclosure rule's four-day reporting requirement requires an unnecessary and dangerous public identification of the business that's been hacked, inviting other bad actors to target that business. This requirement would make critically sensitive information public before the problem is actually fixed, potentially interfering with efforts by law enforcement to stop attackers. Ultimately, this flawed public reporting requirement allows attackers to exploit a company's cyber vulnerability, endangering investors and thwarting efforts to mitigate contagion risks.

We encourage you to advance this resolution of disapproval.

Sincerely,

Naomi Camper
Chief Policy Officer
American Bankers Association

American Bankers Association

Naomi Camper
Chief Policy Officer
202-663-5461
ncamper@aba.com

Cc: Members of the United States Senate