INDEPENDENT COMMUNITY BANKERS of AMERICA®

Robert M. Fisher, *Chairman*
Brad M. Bolton, *Chairman-Elect*
Russell L. Laffitte, *Vice Chairman*
Gregory S. Deckard, *Treasurer*
Tim R. Aiken, *Secretary*
Noah W. Wilcox, *Immediate Past Chairman*
Rebeca Romero Rainey, *President and CEO*

October 19, 2021

The Honorable Gary Peters
Chairman
Senate Committee on Homeland Security
and Governmental Affairs
United States Senate
Washington, D.C. 20510

The Honorable Rob Portman
Ranking Member
Senate Committee on Homeland Security
and Governmental Affairs
United States Senate
Washington, D.C. 20510

Dear Chairman Peters and Ranking Member Portman:

On behalf of community banks across the country, with more than 50,000 locations, thank you for your leadership in enhancing the nation's cybersecurity by introducing S. 2875, the Cyber Incident Reporting Act of 2021. The Independent Community Bankers of America (ICBA) believes the sharing of advanced threat and attack data between federal agencies and financial sector participants is critical to helping manage cyber threats and protect critical systems. We support the legislation's goal of improving information sharing of cyber threats and incidents between the Cybersecurity and Infrastructure Security Agency (CISA) and the private sector. As Congress considers cyber incident reporting legislation and its potential inclusion in the 2022 National Defense Authorization Act, we urge you to take into account the following considerations due to the impact a new reporting regime would have on community banks.

- **Reporting timeline.** Reporting cyber incidents to CISA within 72 hours may not be possible for smaller community banks, since they often have much smaller staff and are more reliant on third-party service providers for key components of their cybersecurity programs, compared to larger entities. We appreciate how the legislation enables the director to establish a flexible, phased reporting timeline that allows entities to prioritize incident response over compliance. However, we urge legislation to include explicit allowances in the time to report for smaller entities given those limitations, such as five business days. This would give smaller community banks adequete time to work with their vendors and their core processors to investigate a cyber incident so they can report timely and accurate information to CISA. It would also result in more helpful reports for CISA because if the timeframe is too short, covered entities may err on the side of caution and report cyber activity before its been validated.

- **Reporting of cyber incidents.** Reporting requirements should focus on actual cyber intrusions. ICBA strongly opposes efforts to require reporting of "potential"

cybersecurity intrusions. The scope and quantity of reports would be far too broad, prior to verification of a cybersecurity intrusion, burdensome to community banks, and counterproductive to CISA's efforts to be able to respond to actual cyber intrusions due to the amount of over-reporting.

- **Harmonizing federal reporting requirements.** Community banks already report incident information to several different governmental agencies, departments, and private organizations when an incident occurs. Community banks must report incident information to their primary regulator, to FinCEN through Suspicious Activity Report (SAR) filings, and share information with the Financial Services Information Sharing and Analysis Center ("FS-ISAC"). Community banks also report an incident to its financial regulatory agencies, where customer data is accessed or there is an impact to systems that hold customer data. We appreciate the legislation's approach to harmonize incident reporting requirements with current financial services sector regulations and guidance. It would be very burdensome for community banks to submit duplicative reports to multiple agencies. Reporting should be made to either CISA or the appropriate sector risk management agency (SRMA), which should then disseminate reports to other relevant agencies such as regulators.

- **Public-Private Information sharing.** ICBA strongly supports the establishment of a Cyber Incident Review Office to receive, aggregate, and analyze reports submitted by covered entities to enhance cybersecurity awareness of threats across critical infrastructure sectors and publish quarterly public reports describing its findings and recommendations. To ensure community banks receive the most timely and actionable data, legislation should require unclassified reports be published monthly. It would also be beneficial if there were monthly classified briefings for those in the financial services sector with secret or top-secret clearances. Community banks' cybersecurity programs would benefit greatly from intelligence gathered by the reporting process.

- **Small businesses definition.** The Small Business Administration defines a 'small business' as generally an independently owned for-profit enterprise that employs 500 or fewer persons. We suggest the legislation allow small critical infrastructure operators, such as small community banks, that are covered entities with 500 or fewer employees, to be defined as a small business.

- **Liability.** It is imperative that legislation provide protections against legal liability for covered incident reports and the contents of those reports. ICBA also strongly supports provisions that prevent cyber incident notifications from being used as evidence in criminal or civil actions. Community banks should not be penalized for being in compliance with the law.

- **Penalties.** Community banks should not be penalized for missed deadlines or for a misdiagnosis of their cyber incident either from CISA or financial sector regulators, if all parties operated in good faith. It is very likely, given a small community bank's limited access to information on other cyber incidents happening around the nation, that they would know that their minor cyber incident may be part of a larger incident, or is part a group of related cybersecurity incidents that together satisfy the definition of a significant cyber incident. Additionally, the legislation should take into account that financial regulatory agencies can currently impose penalties, leading to potential duplicative penalties for community banks. We urge the legislation to include a safe harbor for small covered entities operating in good faith.

ICBA appreciates the opportunity to provide comments on this important legislation. We respectfully ask that you consider our feedback to ensure this legislation strikes the right balance of ensuring timely cyber incident information is reported to CISA while not imposing significant burdens on community banks.

Sincerely,

/s/

Rebeca Romero Rainey
President & CEO

CC: Members of the Senate Committee on Homeland Security and Governmental Affairs