



June 21, 2024

*Via Electronic Mail*

Julia R. Gordon  
Assistant Secretary for Housing, FHA Commissioner  
Federal Housing Administration  
U.S. Department of Housing and Urban Development  
451 7<sup>th</sup> Street SW  
Washington, DC  
20410

**Re: Significant Cybersecurity Incident (Cyber Incident) Reporting Requirements**

Dear Ms. Gordon,

The American Bankers Association,<sup>1</sup> Bank Policy Institute,<sup>2</sup> and the Housing Policy Council<sup>3</sup> (collectively, the Associations) write to provide feedback on the Federal Housing Administration's (FHA) Mortgagee Letter 2024-10 establishing cyber incident reporting requirements for FHA-approved mortgagees. The Mortgagee Letter, effective immediately, contains wide-ranging and rapid requirements for cyber incident reporting that are simply not achievable and will present considerable compliance challenges for FHA-approved mortgagees. Therefore, the Associations request that FHA withdraw the current Mortgagee Letter and reconsider the terms set forth. An immediate suspension would allow the agency additional time to consider other existing cyber regulatory reporting requirements and to develop an

---

<sup>1</sup> The ABA is the voice of the nation's \$23.4 trillion banking industry, which is composed of small, regional, and large banks that together employ approximately 2.1 million people, safeguard \$18.6 trillion in deposits, and extend \$12.3 trillion in loans.

<sup>2</sup> The Bank Policy Institute is a nonpartisan public policy, research and advocacy group that represents universal banks, regional banks, and the major foreign banks doing business in the United States. The Institute produces academic research and analysis on regulatory and monetary policy topics, analyzes and comments on proposed regulations, and represents the financial services industry with respect to cybersecurity, fraud, and other information security issues. Business, Innovation, Technology and Security ("BITS"), BPI's technology policy division, provides an executive-level forum to discuss and promote current and emerging technology, foster innovation, reduce fraud, and improve cybersecurity and risk management practices for the financial sector.

<sup>3</sup> The Housing Policy Council is a trade association comprised of the leading national mortgage lenders and servicers; mortgage, hazard, and title insurers; and technology and data companies. Our interest is in the safety and soundness of the housing finance system, the equitable and consistent regulatory treatment of all market participants, and the promotion of lending practices that create sustainable homeownership opportunities in support of vibrant communities and long-term wealth building for families. For more information, visit [www.housingpolycouncil.org](http://www.housingpolycouncil.org).

approach that satisfies FHA’s goals without introducing unique new standards that will create adverse operational impacts for firms and customers during the critical stages of incident response.

As currently drafted, the Mortgagee Letter has an impractical “significant cybersecurity incident” definition, combined with an insufficient reporting timeframe. The definition covers events that “potentially jeopardize” information or information systems or pose an “imminent threat of violation” to security policies, both ambiguous standards to meet.<sup>4</sup> On top of that, FHA-approved mortgagees must report incidents “within 12 hours of detection”<sup>5</sup> which is extraordinarily challenging in part due to dependence on reporting from third party service providers. Taken together, those thresholds for reporting extend beyond any existing Federal or state reporting requirement.

The breadth and speed of the Mortgagee Letter’s current requirements are also inconsistent with several ongoing government cyber regulatory harmonization efforts. This includes the Cyber Incident Reporting Council’s (“CIRC”) work to coordinate, deconflict, and harmonize Federal incident reporting requirements.<sup>6</sup> Moreover, the requirements are at odds with the National Cybersecurity Strategy’s objective “to harmonize not only regulations and rules, but also assessments and audits of regulated entities” to “minimize the burden of unique requirements.”<sup>7</sup>

As last year’s CIRC report identified, there are at least eight separate incident reporting requirements applicable to financial institutions.<sup>8</sup> Among others, these include the prudential banking regulators’ Computer-Security Incident Notification Rule<sup>9</sup> and the Cyber Incident Reporting for Critical Infrastructure Act.<sup>10</sup> Introducing a new requirement with a distinct threshold and timeframe for reporting threatens to further complicate an already complex regulatory landscape. In fact, according to a recent survey of large financial institutions, firm cyber teams now spend as much as 70 percent of their time on regulatory compliance matters. Therefore, an uncoordinated approach to regulatory reporting requirements is not without consequence and leaves cyber professionals with less time for the core security activities that are essential to effectively managing the organization’s cyber risk.

---

<sup>4</sup> U.S. DEP’T OF HOUSING & URBAN DEVELOPMENT, FED. HOUSING ADMIN, MORTGAGEE LETTER 2024-10, SIGNIFICANT CYBERSECURITY INCIDENT (CYBER INCIDENT) REPORTING REQUIREMENTS 2 (2024).

<sup>5</sup> *Id.*

<sup>6</sup> DEP’T OF HOMELAND SEC., HARMONIZATION OF CYBER INCIDENT REPORTING TO THE FEDERAL GOVERNMENT 2 (2023), <https://www.dhs.gov/sites/default/files/2023-09/Harmonization%20of%20Cyber%20Incident%20Reporting%20to%20the%20Federal%20Government.pdf>.

<sup>7</sup> OFFICE OF THE NAT. CYBER DIR., NATIONAL CYBERSECURITY STRATEGY 9 (2023), <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>.

<sup>8</sup> DEP’T OF HOMELAND SEC., HARMONIZATION OF CYBER INCIDENT REPORTING TO THE FEDERAL GOVERNMENT 9 (2023), <https://www.dhs.gov/sites/default/files/2023-09/Harmonization%20of%20Cyber%20Incident%20Reporting%20to%20the%20Federal%20Government.pdf>.

<sup>9</sup> Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 86 Fed. Reg. 66424 (Nov. 23, 2021).

<sup>10</sup> 6 U.S.C. § 681.

The Associations are committed to working with FHA to better understand the intent behind the Mortgage Letter and explore ways to accomplish those goals without diverting critical incident response resources. If you have any questions or would like to discuss these comments further, please contact Heather Hogsett at [heather.hogsett@bpi.com](mailto:heather.hogsett@bpi.com), John Carlson at [jcarlson@aba.com](mailto:jcarlson@aba.com), or Meg Burns at [meg.burns@housingpolicycouncil.org](mailto:meg.burns@housingpolicycouncil.org).

Sincerely,

/s/ Heather Hogsett  
Heather Hogsett  
SVP, Technology & Risk Strategy, BITS  
Bank Policy Institute

/s/ John Carlson  
John Carlson  
VP, Cybersecurity Regulation & Resilience  
American Bankers Association

/s/ Meg Burns  
Meg Burns  
Executive Vice President  
Housing Policy Council

cc: Harry Coker, Jr.  
Director  
Office of the National Cyber Director  
Executive Office of the President

Robert Silvers  
Under Secretary  
Office of Policy  
Department of Homeland Security