MORTGAGE BANKERS ASSOCIATION

June 26, 2024

The Honorable Julia Gordon
Assistant Secretary for Housing and Federal Housing Commissioner
Office of Housing – Federal Housing Administration
U.S. Department of Housing and Urban Development
451 7th Street, SW
Washington, DC 20410

Re: Significant Cybersecurity Incident (Cyber Incident) Reporting Requirements

Dear Commissioner Gordon,

The Mortgage Bankers Association (MBA)[1] appreciates the opportunity to provide feedback in response to the recent Mortgagee Letter (ML) concerning Significant Cybersecurity Incident reporting requirements.[2] Given the evolving landscape of cybersecurity threats, it is crucial to establish clear, consistent, and practical policies to navigate potential cyber-attacks effectively. By doing so, lenders can better safeguard their systems while protecting customers, employees, vendors, counterparties, and agency partners.

As part of that effort, it is also important that governmental authorities provide clear, aligned, and practical requirements and guidance. MBA's members share FHA's concerns about cyber threats and commitment to appropriately address cyber incidents. It is our hope that the clarifications we request here will help further that goal.

Incident Reporting Timeline

MBA has been a proponent of uniform cybersecurity incident reporting requirements. We encourage FHA to follow the efforts of other agencies to create a uniform reporting requirement. Currently, the Cybersecurity and Infrastructure Security Agency (CISA) is proposing a standard that would require a entities to report a significant cybersecurity

[1] The Mortgage Bankers Association (MBA) is the national association representing the real estate finance industry, an industry that employs more than 275,000 people in virtually every community in the country. Headquartered in Washington, D.C., the association works to ensure the continued strength of the nation's residential and commercial real estate markets, to expand homeownership, and to extend access to affordable housing to all Americans. MBA promotes fair and ethical lending practices and fosters professional excellence among real estate finance employees through a wide range of educational programs and a variety of publications. Its membership of more than 2,000 companies includes all elements of real estate finance: independent mortgage banks, mortgage brokers, commercial banks, thrifts, REITs, Wall Street conduits, life insurance companies, credit unions, and others in the mortgage lending field. For additional information, visit MBA's website: www.mba.org.

[2] Mortgagee Letter 2024-10: Significant Cybersecurity Incident (Cyber Incident) Reporting Requirements.

incident within a 72-hour reporting timeframe for multiple industries.[3] Last year, the Office of the National Cyber Director released a request for information seeking information on how to harmonize cybersecurity requirements.[4] Additionally, the Department of Homeland Security recommended that federal agencies "streamline and harmonize reporting requirements for critical infrastructure, including by clearly defining a reportable cyber incident and establishing the timeline for reporting."[5] These efforts reflect the Administration's goal of harmonizing cybersecurity standards across agencies. Unfortunately, ML 2024-10 is significantly out of alignment with both the CISA proposal and recent guidance from its own sister agency, Ginnie Mae.

Effective upon the release of the ML, lenders must report "Significant Cybersecurity Incidents" to HUD within 12 hours of the detection of any suspected incident. This timeframe is both unreasonable and impracticable. In the initial 12 hours of a cybersecurity incident, lenders are typically just beginning to assess system impacts, may still be actively defending against the intrusion, and might have an impaired ability to communicate with external parties due to compromised systems. In addition, details about an incident can change quickly during those initial hours. It is also unclear what FHA will be able to do with the additional lead time, as a 12-hour standard creates a high likelihood that it will be informed outside of regular business hours, with information that is incomplete, speculative and/or unhelpful.

As stated above, MBA has maintained that the timeline for reporting incidents should be consistent.[6] FHA's 12-hour policy is both considerably shorter than, and inconsistent with, any of the other federal agencies with which MBA members regularly interact. For example, in March Ginnie Mae introduced a 48-hour reporting mandate for cyber incidents.[7] MBA has concerns that even a 48-hour reporting period is unreasonable and presents many of the same issues described above. However, in the absence of broad interagency coordination to develop a more appropriate standard, MBA encourages HUD to at least align the FHA timeline with other federal agencies under the HUD umbrella – namely, Ginnie Mae. FHA should also consider tying its reporting requirement to a determination that an incident *impacting FHA* has occurred, rather than the mere "detection" of *any* incident.

Together, these changes will afford mortgagees the time necessary to determine if there is actually a breach as well as decrease the number of ultimately harmless and/or irrelevant reports that FHA will receive.

---

[3] Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements (Docket No. CISA-2022-0010).
[4] Office of the National Cyber Director, Request for Information: Opportunities For and Obstacles To Harmonizing Cybersecurity, August 16, 2023.
[5] DHS Issues Recommendations to Harmonize Cyber Incident Reporting for Critical Infrastructure Entities, September 19, 2023.
[6] Mortgage Bankers Association, RE: Request for Information on Cyber Regulatory Harmonization (Oct. 31, 2023), available at https://www.regulations.gov/comment/ONCD-2023-0001-0029.
[7] APM 24-02: Cybersecurity Incident Notification Requirement.

Significant Cybersecurity Incident Definition

FHA must also narrow the scope of its reporting requirements. The ML defines a Significant Cybersecurity Incident as:

> *"an event that actually or potentially jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies and has the potential to directly or indirectly impact the FHA-approved mortgagee's ability to meet its obligations under applicable FHA program requirements."*

As written, HUD requires FHA lenders to report any incidents "potentially" affecting "information," regardless of its relevance to FHA mortgage lending or the mortgagee's ability to comply with FHA program requirements. For example, this could mean a bank is required to report an incident where a bank employee mistakenly emails Client A's checking account statement to Client B, even if neither client has a mortgage loan with the bank, let alone an FHA loan. While this incident involves "information," it is unrelated to mortgage lending and does not impact the bank's ability to meet FHA program requirements. Likewise, phishing attempts, even if detected, have the potential to affect information or an information system. Under the current definition, lenders arguably must report unsuccessful phishing attempts. This will further result in an influx of reports that have nothing to do with the FHA program. MBA recommends HUD redefine its definition of a Significant Cybersecurity Incident to read as follows:

> *A Significant Cybersecurity Incident (Cyber Incident) is an event that directly or indirectly impacts the FHA-approved mortgagee's ability to meet its obligations under applicable FHA program requirements, and jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system.*

Adopting the proposed definition would ensure that FHA is not overwhelmed with non-actionable information.

Use and Disclosure of Information Received Through Incident Reporting

MBA members have significant concerns over protecting and keeping confidential the sensitive information contained in reports required by the ML. This is of particular concern given that law enforcement may still be in the early stages of investigation at that point and release of the information could jeopardize the investigation. Further, even if HUD does not proactively publish the reports, it seems possible that the information may be subject to Freedom of Information Act (FOIA) requests.

HUD should clarify what it intends to do with the sensitive information it obtains through this required reporting and for what purpose. It should also confirm that it will keep the information confidential and will release the information, if at all, only in redacted form to avoid identifying lenders, vendors, and/or affected individuals by name.

Application Only to Single-Family Approved Mortgagee

The ML introduces changes to the FHA Single-Family Housing Policy Handbook (Handbook), mandating that "all FHA-approved mortgagees" report any Significant Cybersecurity Incident. MBA requests that HUD clarify that this Mortgagee Letter applies specifically to Single-Family Approved Mortgagees.

Incident Reporting Portal

The ML requires Significant Cyber Incidents to be reported through the FHA Resource Center, which is primarily designed to address compliance inquiries rather than accept and process formal reports. In contrast, the Lender Electronic Assessment Portal (LEAP) system, which HUD utilizes for other significant reporting obligations such as Material Events and operational changes, would be a more appropriate platform for these cybersecurity reports. The LEAP system is already governed by the "Doing Business As" section of the Handbook and is well-suited to handle major reporting events like sanctions, changes in control, and changes in address. We strongly recommend that HUD leverage the existing LEAP system to ensure a more efficient and coherent reporting process.

* * *

MBA appreciates HUD's ongoing willingness to engage with the industry and explore potential process improvements. Should you have questions or wish to discuss these issues further, please contact Darnell Peterson, at (202) 557-2922 or Gabriel Acosta at (202) 557-2811.

Sincerely,

Pete Mills
Senior Vice President
Residential Policy and Strategic Industry Engagement
Mortgage Bankers Association