

HUD Proposes to Narrow Its Cyber Incident Notification Requirement

October 10, 2024

Earlier this year, the U.S. Department of Housing and Urban Development (“HUD”) released an unannounced and immediately effective Cyber Incident Reporting Requirement (the “Original Requirements”) in [Mortgagee Letter 2024-10](#), which imposed onerous requirements for Federal Housing Administration (“FHA”)-approved Mortgagees. These requirements included a 12-hour notification to HUD of even suspected incidents or incidents that violated policy. (We wrote about the Original Requirements [here](#).) Additionally, the 12-hour timeframe was to start from the incident detection, not from the determination of reportability. The Original Requirements received [sharp criticism](#) from the banking and housing industries for being unworkable. On September 30, 2024, HUD proposed amendments to the Original Requirements through a [draft Mortgagee Letter](#) (the “Proposed Amendments”).

The Proposed Amendments would bring the Original Requirements closer in line with the federal banking regulator computer-security incident [notification requirements](#). Such key changes include:

- **Extending the reporting timeline to 36 hours.** HUD proposes to extend the 12-hour notification requirement to 36 hours. Additionally, rather than the clock ticking from the start of the incident, the 36 hours would be from the moment the mortgagee determined the incident to be reportable. This aligns the reporting timeline to that of the federal banking regulator requirement.
- **Clarifying that a Cyber Incident must result in actual harm.** The Original Requirements defined reportable Cyber Incidents as events that potentially jeopardize information or information systems. The Proposed Amendments redefine Cyber Incidents as events resulting in actual harm, in line with the federal banking regulator definition of a “computer-security incident.” Neither the Original Requirements nor the Proposed Amendments define what constitutes “information” or “information systems.” This could be the subject of comment letters.
- **Raising the threshold for a “Reportable Cyber Incident.”** In addition to now requiring actual harm to be considered a Cyber Incident, the Proposed Amendments

would raise the threshold of a “Reportable Cyber Incident” to a Cyber Incident that has “materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade,” the mortgagee’s ability to meet its operational obligations for originating or servicing FHA-insured mortgages, partially in line with the federal banking regulator definition of a “notification incident.” This is a significant change from the Original Requirements, which included suspected Cyber Incidents and events that constitute a “violation or imminent threat of violation” of security policies and procedures with potential impact on the mortgagee’s ability to meet its FHA program requirements.

Mortgagees should be aware that the Proposed Amendments do not fully align with the other banking regulators’ notification requirements. An incident report to HUD still requires a long list of details about the incident, such as the names of the impacted subsidiary of parent companies, which may not feasibly be gathered within a matter of days. Additionally, while the Proposed Amendments add a materiality threshold as to what would be considered a “Reportable Cyber Incident,” this materiality analysis would not be two-tiered, as the other banking regulations require.¹ As is, the Proposed Amendments seemingly define material disruptions or degradations causing *any* deficiency in the mortgagee’s ability to meet its operational obligations to be reportable—as opposed to, for instance, *material* disruptions or degradations to the mortgagee’s ability to meet a *material portion* of its operational obligations.

These Proposed Amendments are not immediately effective; rather, the Original Requirements from earlier this year are [still in effect](#). In the meantime, covered entities are still required to report “Significant Cyber Incidents” within 12 hours from the time of detection. HUD is [accepting public feedback](#) on the Proposed Amendments through October 30, 2024. HUD has not published a target date to finalize the revisions.

If the Proposed Amendments go into effect, the tailored scope of reportable Cyber Incidents would provide more reasonable requirements for mortgagees to comply with and allow them to align HUD reporting processes to existing processes for the federal banking regulator notification requirement. Nevertheless, our [prior takeaways](#) on the importance of preparation and incident response testing still apply, as 36 hours from determination of a reportable incident is still not a long time—particularly in the midst of an incident.

¹ The [federal banking regulators](#) define a “notification incident” as a computer-security incident that has materially disrupted or degraded, or is reasonably likely to *materially* disrupt or degrade, a banking organization’s operations: (i) affecting a *material* portion of its customer base; (ii) resulting in a *material* loss of revenue, profit, or franchise value; or (iii) posing a threat to the financial stability of the United States.

To subscribe to the Data Blog, please [click here](#).

The [Debevoise Data Portal](#) is an online suite of tools that help our clients quickly assess their federal, state, and international breach notification and substantive cybersecurity obligations. Please contact us at dataportal@debevoise.com for more information.



Avi Gesser
Partner, New York
+1 212 909 6577
agesser@debevoise.com



Erez Liebermann
Partner, New York
+212 909 6224
eliebermann@debevoise.com



Anna Moody
Counsel, Washington, D.C.
+1 202 383 8017
amoody@debevoise.com



Karen Joo
Associate, New York
+1 212 909 6528
hjoo@debevoise.com



Stephanie D. Thomas
Associate, New York
+1 212 909 6535
sdthomas@debevoise.com

This publication is for general information purposes only. It is not intended to provide, nor is it to be used as, a substitute for legal advice. In some jurisdictions it may be considered attorney advertising.