Very Broad and Very Fast: The New Federal Housing Administration's 12-Hour Cyber Incident Notification Rule

May 28, 2024

On May 23, 2024, the U.S. Department of Housing and Urban Development ("HUD") announced that, effective immediately, Federal Housing Administration ("FHA")-approved Mortgagees are subject to a drastically heightened cybersecurity incident reporting regime. HUD issued this new requirement (the "HUD Notification Requirement") without the need for notice or comment in Mortgagee Letter 2024-10 (the "Letter"), which amends the Single Family Housing Policy Handbook 4000.1 (the "Handbook") to require FHA-approved Mortgagees to report "suspected" "Significant Cybersecurity Incidents" within 12 hours of detection.

Notable aspects of the HUD Notification Requirement include: (1) an extremely broad definition of a reportable Significant Cyber Incident; (2) a 12-hour reporting time frame; and (3) an unusually early reporting trigger that starts the notification clock at detection. In practice, the HUD Notification Requirement will require Mortgagees to report many more cyber incidents and report them much sooner than under any other widely applicable notification regime—presenting a significant compliance challenge that will pressure test even the most robust incident response plans ("IRPs").

Scope of Reporting Obligation

The HUD Notification Requirement applies to all FHA-approved Mortgagees, including Title I Lenders, Title II Mortgagees, and other FHA program participants, as defined in the Handbook.[1] FHA-approved Mortgagees include the following types of entities:

[1] Handbook, § I.A.1–2. The letter is addressed to: All FHA-Approved Mortgagees, All Direct Endorsement Underwriters, All Eligible Submission Sources for Condominium Project Approvals, All FHA Roster Appraisers, All FHA-Approved 203(k) Consultants, All HUD-Certified Housing Counselors, All HUD-Approved Nonprofit Organizations, All Governmental Entity Participants, All Real Estate Brokers, and All Closing Agents.

- Supervised Mortgagees, financial institutions that are members of the Federal Reserve System or whose accounts are insured by the Federal Deposit Insurance Corporation ("FDIC") or the National Credit Union Administration ("NCUA");

- Nonsupervised Mortgagees, lending institutions that have as their principal activity the lending or investing of funds in real estate mortgages, consumer installment notes or similar advances of credit, the purchase of consumer installment contracts, or from a directly related field; and

- Investing Mortgagees, organizations that invest funds under their own control.

Covered Mortgagees must report to HUD when they experience a "suspected" Significant Cyber Incident, which is defined as either an event that (1) "actually or potentially jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system" or (2) "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."

Events Jeopardizing Information

The first category of reportable event takes the traditional definition of a cyber incident (i.e., unlawful access that jeopardizes the confidentiality, integrity, or availability of information or an information system) and broadens it significantly by including "suspected" incidents that "potentially" jeopardize information or systems. In addition, the term "information" is not limited to nonpublic or sensitive information. Moreover, the definition of "information system" is not limited to a Mortgagee's own information systems. Accordingly, it appears that a suspected cyber incident at a third party that potentially jeopardizes the confidentiality, integrity, or availability of a Mortgagee's nonsensitive information could trigger the 12-hour notification obligation, starting from the time of "detection."

Events Violating Policies

The second category of reportable event is a violation (or imminent threat of a violation) of security policies, security procedures, or acceptable use policies that also has the potential to directly or indirectly impact the FHA-approved mortgagee's ability to meet its obligations under applicable FHA program requirements. Most importantly, this definition does not distinguish between (1) events that could impact the Mortgagee's ability to meet financial obligations and (2) events that could impact the Mortgagee's ability to meet operational requirements in the Handbook (including, e.g., performance, reporting, and confidentiality obligations). While the former are likely to

be relatively rare (given capital adequacy requirements), the latter may be more common, particularly considering the routine frequency of data theft, ransomware, and DDoS attacks.

As a result, depending on how the impact prong of this category is interpreted, this second category could also be very broad in practice, especially because of the presence of the words "potential" and "indirectly."

This definition also is not expressly limited to the policies of the Mortgagee, so it appears that the imminent threat of a violation of a security or acceptable use policy at a third party that has the potential to indirectly impact a Mortgagee's ability to meet its obligations under applicable FHA program requirements could be reportable within 12 hours of detection.

Reporting and Documentation Requirements

Mortgagees must report Significant Cyber Incidents by email to HUD's FHA Resource Center at <answers@hud.gov> and HUD's Security Operations Center at <cirt@hud.gov> within 12 hours. As noted above, this is an unusually short deadline, made even more demanding by the fact that the 12-hour clock starts running from the time of detection of the incident, not from the time the incident is determined to be notifiable, as is the case with most other cyber incident regulatory notification requirements (e.g., the Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers requires a material or potentially material cybersecurity event be reported 36 hours from determination that the event is notifiable).

In addition, the reporting obligation is extremely prescriptive, requiring very specific details, many of which almost certainly will not be known in the first 12 hours of an incident. The report to HUD must include the following information:

- Mortgagee name;
- Mortgagee ID;
- Name, email address, and phone number of Mortgagee's point of contact for Security Operations Center follow-up activities;
- Description of the Cyber Incident, including the following, if known:

- date of Cyber Incident;
- cause of Cyber Incident;
- impact to Personally Identifiable Information;
- impact to login credentials; and
- impact to Information Technology (IT) system architecture;

- List of any impacted subsidiary or parent companies; and
- Description of the current status of the Mortgagee's Cyber Incident response, including whether law enforcement has been notified.

Again, much of this information may not be known for weeks or even months after an incident. Presumably HUD anticipates that the initial report will contain what is reasonably known at the time of the reporting and that it will be supplemented as more information becomes available.

Takeaways

Compliance with the new HUD Notification Requirement will be difficult for most lenders to achieve. It will require almost immediate escalation of potential cyber incidents and available facts to individuals with the authority to make the notification determination. Compliance will thus likely require several updates to cyber incident response policies, procedures, and trainings, and lenders that are subject to the new requirement should consider taking the following measures:

- **Evaluate if Your Entity Is Covered**: The HUD Notification Requirement applies to a range of FHA program participants, as described above, effective immediately as of May 23, 2024. Financial institutions should promptly evaluate whether they are covered by the HUD Notification Requirement and determine whether any updates to their cyber incident response program are required.

- **Update IRP**: FHA-approved Mortgagees should ensure that their IRPs provide for timely investigation and escalation of potential Significant Cyber Incidents. The 12-hour notification window does not allow for any time lost between incident detection and escalation to persons responsible for reporting. The updated plans should include a template report that can be readily populated with the required

information to be reported to HUD. For lenders subject to other breach notification regimes, the updated plans should consider how HUD reporting should be sequenced in relation to other courtesy or required notifications.

- **Designate Responsible Personnel and Allocate Resources**: IRPs should also clearly identify the personnel responsible for making the decisions as to whether to report to HUD, when to report, and what should be included in the report. Ideally, several persons should be identified for this role in the likely event that one or more designated employees are unavailable. Additionally, given the significant increase in possible reporting obligations, consider allocating additional resources to support these functions.

- **Review Contracts with Third Parties for Incident Reporting**: Because third-party incidents could trigger reporting requirements, FHA-approved Mortgagees should review contracts with partners and vendors who have access to Mortgagee information or information systems, or who could affect the Mortgagee's obligations under the FHA, to ensure that such third parties are required to promptly notify Mortgagee of a qualifying incident. Additionally, Mortgagees should ensure that third-party incident notification is integrated into their HUD reporting procedures.

- **Test Incident Response**: To ensure that updated incident response procedures are effective, Mortgagees should test these procedures through simulated tabletop exercises. These exercises should involve the Mortgagee's incident response team and other key reporting decision-makers to troubleshoot any delays in communication, escalation, or notification.

The authors would like to thank Debevoise Summer Law Clerk Henry Maguire for his work on this Debevoise Data Blog.

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.

The cover art used in this blog post was generated by DALL-E.

* * *

Please do not hesitate to contact us with any questions.

Courtney M. Dankworth
Partner, New York
+1 212 909 6758
cmdankworth@debevoise.com

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

Satish M. Kini
Partner, Washington, D.C.
+1 202 383 8190
smkini@debevoise.com

Erez Liebermann
Partner, New York
+1 212 909 6224
eliebermann@debevoise.com

Gregory J. Lyons
Partner, New York
+1 212 909 6566
gjlyons@debevoise.com

Matt Kelly
Counsel, New York
+1 212 909 6990
makelly@debevoise.com

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

Jehan A. Patterson
Counsel, Washington, D.C.
+1 202 383 8246
jpatterson@debevoise.com

Michelle Huang
Associate, New York
+1 212 909 6553
mhuang1@debevoise.com

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

Alexandra N. Mogul
Associate, New York
+1 212 909 6444
anmogul@debevoise.com