Published on *The National Law Review* https://natlawreview.com

FHA's Releases 12-Hour Cyber Incident Notification Rule

Article By:

A.J. S. Dhaliwal

Mehul N. Madia

On May 23, the U.S. Department of Housing and Urban Development (HUD) announced that Federal Housing Administration-approved Mortgagees are subject to a heightened cybersecurity incident reporting regime. The new requirement, which amends the Single Family Housing Policy Handbook 4000.1, requires FHA-approved Mortgagees to report "suspected" "Significant Cybersecurity Incidents" within 12 hours of detection.

Under the new requirements, FHA-approved mortgagees must report to HUD when they experience a "suspected" Significant Cyber Incident, which HUD defines 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."

Mortgagees must report these Significant Cyber Incidents to HUD within *12 hours of detection*. The reporting obligation is very perspective and requires specific details concerning the cybersecurity incident including, for example, the date, cause, impact, cause of the cybersecurity incident, as well as the impact. It is not a stretch to say many of these details that may be difficult to know 12 hours after detection.

Putting It Into Practice: Beyond the very short reporting time frame, HUD has released an extremely broad definition of what constitutes a reportable Significant Cyber Incident. The second prong of HUD's definition is unusually broad in that it sweeps up "imminent threat" of a violation of security policies, that has the "potential to directly or indirectly" impact FHA-approved mortgagee's. This can sweep up the more common types of cyberattacks such as theft, ransomware, or DDoS attacks, as well as cyberattacks on third-party service providers where cybersecurity breaches may "indirectly" impact the mortgagee.

Compliance with HUD's notification requirement will be very difficult for most lenders to achieve. Lenders must have procedures in place to immediately escalate almost all potential cybersecurity incidents so that they can be appropriately assessed and reported.

Listen to this post

National Law Review, Volume XIV, Number 152