Federal Housing Finance Agency
Office of Inspector General

Enterprise Monitoring of Cloud Computing Service Providers

White Paper • WPR-2020-005 • August 12, 2020

WPR-2020-005

August 12, 2020

Executive Summary

Fannie Mae and Freddie Mac (the Enterprises) rely heavily on counterparties and third-parties to originate and service the mortgages the Enterprises purchase and on third-parties to provide the operational support for a wide array of professional services. As the Enterprises and the Federal Housing Finance Agency (FHFA or Agency) recognize, that reliance exposes the Enterprises to a number of risks. Risks include counterparty, operational, cyber, and reputational risks.

We explained in our fiscal year 2020 Management and Performance Challenges for FHFA that FHFA is challenged to effectively oversee the Enterprises' management of risks related to their counterparties and third-parties.

Earlier this year, we published a white paper entitled *Enterprise Third-Party Relationships: Risk Assessment and Due Diligence in Vendor Selection*, which described the Enterprises' third-party risk management programs as they pertain to assessing and selecting one particular type of third-party: financial technology companies (fintechs).

We also recently issued a white paper that provided a high-level overview of cloud computing at the Enterprises and discussed benefits and risks, particularly with third-party cloud service providers. According to lists provided to us by the Enterprises, each Enterprise has relationships with dozens of third-party cloud service providers and considers about half of its cloud providers to be inherently high-risk third-parties. FHFA lacks authority to supervise third-party cloud service providers under contract to the Enterprises. This white paper looks at the Enterprises' monitoring procedures for third-party cloud service providers, pursuant to FHFA Advisory Bulletin 2018-08, *Oversight of Third-Party Provider Relationships*.

TABLE OF CONTENTS .....

ABBREVIATIONS

AB 2018-04	Advisory Bulletin 2018-04, *Cloud Computing Risk Management*
AB 2018-08	Advisory Bulletin 2018-08, *Oversight of Third-Party Provider Relationships*
Enterprises	Fannie Mae and Freddie Mac
FHFA or Agency	Federal Housing Finance Agency
OIG	Federal Housing Finance Agency Office of Inspector General
TPRM Standard	Fannie Mae Third-Party Risk Management Standard

BACKGROUND

The Enterprises rely heavily on counterparties and third-party providers (collectively third-parties) to originate and service the mortgages the Enterprises purchase and to provide the operational support for a wide array of professional services. As the Enterprises and FHFA recognize, that reliance exposes the Enterprises to a number of risks, including the risk that a third-party will not meet its contractual obligations and the risk that a third-party will engage in fraudulent conduct. Risks to the Enterprises from reliance on third-parties also include counterparty, operational, cyber, and reputational risks. Both Enterprises maintain that they have established controls to mitigate these risks. The Enterprises manage their relationships with third-parties through their contracts with those third-parties.

We explained in our fiscal year 2020 Management and Performance Challenges for FHFA that in light of the financial, governance, and reputational risks arising from the Enterprises' relationships with counterparties and third-parties, FHFA is challenged to effectively oversee the Enterprises' management of risks related to their counterparties and third-parties.[1] This has been a long-standing challenge and will remain so for the foreseeable future.

In light of the risks related to third-parties, we recently published a white paper entitled *Enterprise Third-Party Relationships: Risk Assessment and Due Diligence in Vendor Selection*, which described the Enterprises' third-party risk management programs as they pertain to assessing and selecting one particular type of third-party: fintechs.[2] This white paper looks at the Enterprises' monitoring procedures for third-party cloud service providers, pursuant to Advisory Bulletin 2018-08, *Oversight of Third-Party Provider Relationships* (AB 2018-08). We did not evaluate the adequacy of their processes.

ENTERPRISE MONITORING OF THIRD-PARTY CLOUD SERVICE PROVIDERS

Earlier this year, we issued a white paper that provided a high-level overview of cloud computing at the Enterprises and discussed benefits and risks, particularly with third-party

[1] *See* OIG, *FHFA Fiscal Year 2020 Management and Performance Challenges* (Oct. 22, 2019) (online at www.fhfaoig.gov/sites/default/files/Fiscal%20Year%202020%20Management%20and%20Performance%20Challenges.pdf).

[2] *See* OIG, *Enterprise Third-Party Relationships: Risk Assessment and Due Diligence in Vendor Selection* (Mar. 12, 2020) (online at www.fhfaoig.gov/sites/default/files/WPR-2020-003.pdf).

cloud service providers.[3] According to lists provided to us by the Enterprises, each Enterprise has relationships with dozens of third-party cloud service providers and considers about half of its cloud providers to be inherently high-risk third-parties. An internal FHFA assessment from 2019 named a cloud service provider as Fannie Mae's most critical third-party.[4]

FHFA lacks authority to supervise third-party cloud service providers under contract to the Enterprises.[5] FHFA has issued several advisory bulletins in which it announced its supervisory expectations for Enterprise oversight of these third-parties.[6] In 2018, FHFA issued Advisory Bulletin 2018-04, *Cloud Computing Risk Management* (AB 2018-04), in which it announced its specific supervisory expectations for Enterprise oversight of third-party cloud service providers. FHFA recognized, in AB 2018-04, that cloud computing presents notable information security risks and counsels the Enterprises to "assess each cloud provider's quality and performance in providing information security to protect data."

According to an FHFA official, AB 2018-08 is a "companion" to AB 2018-04, and the expectations in both advisory bulletins should be implemented in tandem. AB 2018-08 counsels that the nature and extent of monitoring the performance of third-party providers should be commensurate with the level of risk and the Enterprises' monitoring procedures should adapt to the changing risk landscape during the life of a third-party provider relationship. Pursuant to AB 2018-08, for concerns identified during monitoring, the Enterprises should ensure they are resolved in a timely manner and procedures exist to escalate issues as necessary. FHFA also expects each Enterprise to ensure it "retains

---

[3] *See* OIG, *An Overview of Enterprise Use of Cloud Computing* (Mar. 11, 2020) (online at www.fhfaoig.gov/sites/default/files/WPR-2020-002.pdf).

[4] Freddie Mac also works with the cloud provider, but FHFA's assessment of Freddie Mac did not include this statement.

[5] In FHFA's most recent annual report to Congress, the Agency explained that it "must rely on provisions in the regulated entities' third-party contracts to obtain access to information about service providers [including mortgage servicers] that is necessary to fulfill FHFA's statutory safety and soundness responsibilities." FHFA has asked Congress to authorize FHFA to "examine the records, operations, and facilities of each material service provider to a regulated entity for the limited purpose of identifying practices that could pose a safety and soundness risk to the regulated entity" (endorsing recommendations from the Financial Stability Oversight Council and the Government Accountability Office that Congress grant the Agency authority to examine third parties that do business with its regulated entities). *See* FHFA, *2019 FHFA Report to Congress*, at 14-15 (June 15, 2020) (online at www.fhfa.gov/AboutUs/Reports/Pages/Annual-Report-to-Congress-2019.aspx).

[6] For example: Advisory Bulletin 2017-02, *Information Security Management*, in which FHFA articulated its expectations that the Enterprises select a cloud provider that is consistent with their established risk limits and consider the provider's "abilities to identify and mitigate cyber threats to data and operational infrastructure" (online at www.fhfa.gov/SupervisionRegulation/AdvisoryBulletins/Pages/Information-Security-Management.aspx); AB 2018-08, in which FHFA set forth its expectations that the Enterprises monitor their relationships with third parties and, among other things, to "consider whether the third party is complying with applicable legal and regulatory requirements, including documenting such compliance when necessary."

sufficient staff with the necessary expertise, authority, and accountability to oversee and monitor the third-party provider relationship."

Fannie Mae

Fannie Mae's internal Third-Party Risk Management Standard (TPRM Standard) establishes the framework for the Enterprise's approach to managing third-party risk. It includes the minimum monitoring requirements and roles and responsibilities, among other things. The Enterprise's Third-Party Risk Committee maintains the TPRM Standard.

Monitoring Procedures

Fannie Mae creates a risk profile that assesses third-parties against ten "inherent risk triggers" as high, medium, low, or not applicable.[7] The TPRM Standard describes how the assessment against the triggers is used to determine a third-party's risk category and the level and frequency of monitoring activities. The highest-risk third-parties are assigned to risk category one, and the lowest-risk third-parties are assigned to risk category five. According to the TRPM Standard, Fannie Mae focuses most of its risk management activities, including ongoing monitoring, in the top two risk categories. About half of Fannie Mae's cloud providers fall into one of the top two risk categories.

Fannie Mae told us there are two groups responsible for monitoring its cloud service providers: Procurement monitors the risk and controls, and the business unit that procures the cloud services monitors performance and Service Level Agreements.[8] Procurement establishes monitoring processes to align with the Enterprise's risk management policies and standards and engages directly with third-party cloud service providers. Procurement and the business units also have regular meetings with higher risk third-parties.

The risk profile directs monitoring activities specific to the cloud service provider. A monitoring activity may involve reviews and tests to verify the cloud service provider's operational controls. For such cases, Procurement may request verification of a current independent audit and that no significant operational deficiencies were noted in that audit. Certain cloud providers may also be referred to Fannie Mae's information security group for re-assessments of whether the appropriate cloud and security controls are maintained. The

[7] For more information, see OIG, *Enterprise Third-Party Relationships: Risk Assessment and Due Diligence in Vendor Selection* (Mar. 12, 2020) (online at www.fhfaoig.gov/sites/default/files/WPR-2020-003.pdf).

[8] The Enterprises manage risk using an industry standard "Three Lines of Defense" model. The first line of defense is the business unit that generates a particular risk. The second line of defense includes groups that are responsible for independent oversight and monitoring of risk management. The third line of defense for each Enterprise is its Internal Audit function. *See* Fannie Mae, *2019 Form 10-K*, at 116 (online at www.fanniemae.com/resources/file/ir/pdf/quarterly-annual-results/2019/q42019.pdf); Freddie Mac, *2019 Form 10-K*, at 67-68 (online at www.freddiemac.com/investors/financials/pdf/10k_021320.pdf).

information security group is an example of one of the "Domain Experts" that the first line business unit engages when specialized issues arise with monitoring cloud providers. Under the TPRM Standard, the above monitoring activities must be performed at least every two years for high risk providers and annually for critical third-parties.

Procurement is also responsible for documenting findings identified during monitoring, action plans to remediate the findings, status of remediation, and evidence of remediation. According to the TPRM Standard, a finding is a determination that the third-party has failed to demonstrate that it is effectively managing the risks associated with its services. Procurement or the Domain Expert rates how significant the finding is, which determines the timeline for remediation. If the finding is rated high and not remediated within nine months, it is escalated to the Third-Party Risk Committee, according to an Enterprise official. Information from documented findings help to determine which providers should be added to Fannie Mae's "Heightened Monitoring List."

Fannie Mae policy requires periodic updates of both the TPRM Standard and third-party monitoring procedures. Under the TPRM Standard, risk profiles and monitoring procedures for cloud providers in the top two risk categories are required to be updated on at least an annual basis. The TPRM Standard also includes a requirement that the standard be reviewed and approved on an annual basis. The Third-Party Risk Committee is responsible for approving the TPRM Standard. One of the purposes of the annual review, according to the TPRM Standard, is to assess whether it aligns with changes in business, risk, and control conditions.

Freddie Mac

Freddie Mac's Enterprise Operations and Technology Risk team manages the Vendor Risk Standard, which establishes high-level, minimum requirements for how Enterprise divisions should manage risk with third-party suppliers, including cloud providers.

Freddie Mac reported to us in July 2020 that it is currently undergoing an enterprise-wide transition of its third-party program. As publicly reported by FHFA, Freddie Mac's implementation of a third-party risk management framework is still in the early stages.

Monitoring Procedures

The Information Technology division serves as the first line for managing cloud service provider relationships. Currently, specific monitoring procedures for cloud providers follow a decentralized model in which a designated "contract owner" establishes procedures at a contract level. As part of the Enterprise's third-party program transformation, Freddie Mac is transitioning its monitoring procedures from contract-based to division level. An FHFA

official described to us that the Enterprise is centralizing its approach to help provide a comprehensive view of risks.

Freddie Mac also assesses risk with cloud providers on a high, medium, or low basis. In general, the contract owner establishes and monitors the cloud provider's service-level agreements based on the assessed risk. The Enterprise reported to us that its cloud providers are "reassessed on a periodic basis." A common assessment tool is the review of an independent audit report to provide Freddie Mac "assurances regarding their operating practices." This audit is submitted by the cloud provider on a periodic basis and, according to the Federal Financial Institutions Examination Council, it can be used to assure that the cloud provider's controls are effective.

The contract owner is also responsible for identifying, remediating, monitoring, and reporting "issues" concerning the cloud service provider. According to an internal policy document, the contract owner must execute these activities in accordance with Freddie Mac's Issue Management Standard. Enterprise Operations and Technology Risk is responsible for escalating issues that exceed the Enterprise's risk limits.

Enterprise officials described a two-fold approach to ensure that Freddie Mac has staff with the expertise to monitor cloud providers. In addition to internal training, Freddie Mac continues to recruit and hire cloud talent.

CONCLUSION

Each Enterprise has relationships with dozens of third-party cloud service providers and considers about half of its cloud providers to be inherently high-risk third-parties. FHFA lacks authority to supervise third-party cloud service providers under contract to the Enterprises. This white paper looks at the Enterprises' monitoring procedures for third-party cloud service providers, pursuant to FHFA Advisory Bulletin 2018-08.

OBJECTIVE, SCOPE, AND METHODOLOGY .....

The objective of this white paper was to provide an overview of the Enterprises' monitoring procedures of third-party cloud service providers, pursuant to AB 2018-08. To achieve this objective, we reviewed internal and publicly available FHFA and Enterprise documents. We also interviewed FHFA and Enterprise officials. We did not evaluate the adequacy of their processes.

We provided FHFA with the opportunity to respond to a draft of this white paper. We appreciate the cooperation of FHFA staff, as well as the assistance of all those who contributed to the preparation of this white paper.

ADDITIONAL INFORMATION AND COPIES.....

For additional copies of this report:

- Call: 202-730-0880
- Fax: 202-318-0239
- Visit: www.fhfaoig.gov

To report potential fraud, waste, abuse, mismanagement, or any other kind of criminal or noncriminal misconduct relative to FHFA's programs or operations:

- Call: 1-800-793-7724
- Fax: 202-318-0358
- Visit: www.fhfaoig.gov/ReportFraud
- Write:

  FHFA Office of Inspector General
  Attn: Office of Investigations – Hotline
  400 Seventh Street SW
  Washington, DC 20219