Federal Housing Finance Agency
Office of Inspector General

Enterprise Third-Party Relationships: Risk Assessment and Due Diligence in Vendor Selection

White Paper • WPR-2020-003 • March 12, 2020

WPR-2020-003

March 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. Currently, FHFA lacks the authority to regulate parties that provide services to the Enterprises.

We have also identified third-party oversight as a top risk, specifically that FHFA is challenged to effectively oversee the Enterprises' management of risks related to their counterparties and third-parties.

In light of the risks related to third-parties, we have commenced a white paper series focused on third-party risk management. In this white paper, we describe the Enterprises' third-party risk management programs for the first two phases of the risk management life cycle, Risk Assessment and Due Diligence in Third-Party Provider Selection, for financial technology companies (fintechs).

TABLE OF CONTENTS

EXECUTIVE SUMMARY 2

ABBREVIATIONS 4

BACKGROUND 5

Third-Party Risk Management Life Cycle 6

RISK ASSESSMENT AND DUE DILIGENCE IN SELECTION OF FINTECH PROVIDERS 6

Fannie Mae 7

Process 1: Risk Profile 7

Process 2: Supplier Risk Assessment 7

Process 3: Operational Control Risk Assessment 7

Freddie Mac 8

Step 1: Discovery 8

Step 2: Risk Assessment 8

Step 3: Data Analysis 9

FHFA Oversight 9

CONCLUSION 9

OBJECTIVE, SCOPE, AND METHODOLOGY 10

ADDITIONAL INFORMATION AND COPIES 11

ABBREVIATIONS

AB 2018-08	FHFA Advisory Bulletin 2018-08
Enterprises	Fannie Mae and Freddie Mac
FHFA or Agency	Federal Housing Finance Agency
Fintech	Financial Technology
OCRA	Operational Controls Risk Assessment
OIG	Federal Housing Finance Agency Office of Inspector General

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.

Currently, FHFA lacks the authority to regulate parties that provide services to the Enterprises. The Enterprises manage their relationships with third-parties through their contracts with those third-parties.

We have also identified third-party oversight as a top risk. As described in our fiscal year 2020 Management and Performance Challenges for FHFA, we explained 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 longstanding challenge and will remain so for the foreseeable future.[2]

In light of the risks related to third-parties, we have commenced a white paper series focused on third-party risk management. This white paper looks at the risks associated with one particular type of vendor, fintechs. For purposes of this white paper, fintechs are financial services companies that use technology to create efficiencies. As a recent OIG white paper explained, the Enterprises are expanding their use of fintech vendors in programs to automate verifications of borrower employment, income, and assets.[3] In this white paper, we describe the Enterprises' third-party risk management programs for the first two phases of the life

[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] Similarly, the Financial Stability Oversight Council cautioned: "Reliance by financial institutions on third-parties to provide important operational function has increased over the past several years. With the adoption of fintech innovations and the proliferation of large data sets, some financial institutions have outsourced portions of certain operational functions and data gathering requirements…. These services have information and cost benefits, but relying on outside firms for critical data and services also creates risks."

[3] *See* OIG, *Enterprise Use of Automated Verifications of Borrower Employment, Income, and Assets* (Sept. 26, 2019) (WPR-2019-005) (online at www.fhfaoig.gov/sites/default/files/WPR-2019-005.pdf).

cycle, Risk Assessment and Due Diligence in Third-Party Provider Selection, for fintechs.[4] We did not evaluate the adequacy of their processes.

Third-Party Risk Management Life Cycle

FHFA issued Advisory Bulletin 2018-08 (AB 2018-08) to Fannie Mae and Freddie Mac on Oversight of Third-Party Provider Relationships in September 2018.[5] The Agency explained that issuance of this Advisory Bulletin provided guidance to the Enterprises on management of risks associated with third-party provider relationships, and an FHFA official told us that it was issued to provide safety and soundness guidance.

AB 2018-08 states that FHFA expects the Enterprises to establish and maintain a third-party provider risk management program that includes five phases of the risk management life cycle: Risk Assessment, Due Diligence in Third-Party Provider Selection, Contract Negotiation, Ongoing Monitoring, and Termination.

RISK ASSESSMENT AND DUE DILIGENCE IN SELECTION OF FINTECH PROVIDERS .....

In September 2018, FHFA issued AB 2018-08 to the Enterprises on assessing and managing risk associated with third-party vendors. It states that the Enterprises should ensure that third-party risk management corresponds with the level of risk and complexity of the relationship.

According to the Advisory Bulletin, management of the first life cycle phase, Risk Assessment, should include processes to identify and assess the risks associated with engaging a third-party provider. Among other things, this risk assessment may include an evaluation of risks such as volume of activity, technology required, and potential security risks with granting access to an Enterprise's non-public information. The Enterprises' programs should provide for management of the risks identified through the risk assessment, and, as necessary, the risk assessment should include a strategy to mitigate the risks or justify the acceptance of identified risks. The risk assessment should be reviewed and updated when appropriate.

---

[4] Subsequent OIG white papers are planned to cover the remaining three phases of the life cycle.

[5] The advisory bulletin was also issued to the Federal Home Loan Banks and the Office of Finance. This white paper discusses only Fannie Mae and Freddie Mac. For more information, see Federal Housing Finance Agency, Advisory Bulletin 2018-08, *Oversight of Third-Party Provider Relationships* (Sept. 28, 2018) (online at www.fhfa.gov/SupervisionRegulation/AdvisoryBulletins/Pages/Oversight-of-Third-Party-Provider-Relationships.aspx).

In the second phase, Due Diligence in Third-Party Provider Selection, the Enterprises should conduct an objective assessment of the vendor's ability to supply a product or service in a safe and sound manner before entering into a contract. Due diligence should be commensurate with the level of risk and should include an evaluation of financial, operational, legal, compliance, and reputational risks of engaging the proposed third-party. The guidance lists factors to consider in these areas, such as operational and internal controls and reliance on subcontractors. It also requires the results, findings, and recommendations to be documented.

Fannie Mae

Fannie Mae officials described for us three processes the Enterprise uses to assess risk and conduct due diligence associated with engaging with a third-party fintech.[6]

Process 1: Risk Profile

Fannie Mae Third-Party Risk Management creates a risk profile for groups of similar vendors. Fintech vendors are part of the Digital Alliance group. This group risk profile assesses ten "inherent risk triggers" as high, medium, low, or not applicable and includes factors such as whether the vendors would be interacting directly with consumers or have access to nonpublic personal information. The risk profile determines due diligence and monitoring requirements collectively for the group.[7]

Process 2: Supplier Risk Assessment

Based on the due diligence requirements from the risk profile, Fannie Mae Procurement performs a supplier risk assessment for each prospective vendor. The process begins by issuing a questionnaire to the prospective vendor.[8] Supporting documentation is collected from the vendor and then due diligence is performed to review information such as information security, Non-Public Information, or privacy. When the review is completed, Procurement issues a final risk review summary to the applicable Fannie Mae business unit that includes findings, observations, or recommendations.

Process 3: Operational Control Risk Assessment

Following completion of the supplier risk assessment, Third-Party Risk Management conducts an Operational Control Risk Assessment (OCRA) to identify or analyze risks in the

[6] Although the process can be customized according to risks, Fannie Mae uses the same general risk assessment and due diligence process for fintech vendors as it does for other types of vendors.

[7] Risk profiles for the Digital Alliance group are updated on an annual basis.

[8] Prior to engaging directly with a vendor, the scope of work and services is validated with the business unit requesting the services.

vendor's operational infrastructure associated with the service to be provided. The OCRA is based on weighting and scoring different functional areas, such as data management, quality assurance, quality control, audit, and talent management.

The Third-Party Risk Management group obtains supporting information for the vendor's questionnaire responses and conducts a review to verify responses and perform any applicable tests. Vendors receive a report summarizing findings and opportunities for improvement, and they submit an action plan to Fannie Mae responding to those issues. The vendor collaborates with Fannie Mae to remediate matters from the review. The Vice President of Single-Family Credit Risk Counterparty reviews the OCRA and associated findings and provides the business area approval.

Freddie Mac

Freddie Mac officials told us that the Enterprise created an eight-step process to manage risks associated with fintech vendors.[9] Freddie Mac officials explained to us that steps one through three correlate to assessing risk and conducting due diligence.

Step 1: Discovery

The Business Partner Integration group coordinates with the prospective vendor and completes a Discovery Documentation and Partner Profile, which is a "snapshot" that analyzes information such as the vendor's business model, companies the vendor has integrated with, their loan origination system, and their mortgage point of sale system. Freddie Mac then reviews a product demonstration to determine overall fit and confirm that the services provided match its needs.

Step 2: Risk Assessment

After the Discovery step, Vendor Risk Management conducts a risk assessment to determine the level of risk. The risk assessment considers areas such as information security, consumer compliance, and financial risk, and it identifies the associated due diligence activities to be performed by applicable Freddie Mac groups, such as Privacy, Legal, and Information Security.

The Counterparty Operational Risk Evaluation group conducts an onsite visit if requested by the business unit group. Their review includes an assessment of operational and internal

[9] Freddie Mac's Asset and Income Modeler program is its primary program utilizing fintech vendors. The risk assessment and due diligence processes described in this section apply to those fintech vendors, but not other types of Freddie Mac third-party vendors.

controls, covering corporate governance, business continuity/disaster recovery, information security, and quality control.

Step 3: Data Analysis

Following the risk assessment, the Credit Innovation and Analytics group obtains a data sample from the prospective vendor as a "pre-pilot" and reviews it to ensure that the data meets Freddie Mac standards. The group performs checks to confirm that required fields are populated, including how often and whether data is transcribed accurately; through this iterative process, a comfort level with the data quality is gained. At the conclusion of the data phase, the results of the data analysis, risk assessment, and discovery collectively are reviewed by multiple Freddie Mac groups.

FHFA Oversight

Since issuance of AB 2018-08, FHFA examination teams have performed ongoing monitoring of Enterprise practices to comply with the guidance, however, FHFA has not focused examination activities on fintech vendors.

CONCLUSION

Enterprise reliance on third-parties exposes them to a number of risks, including counterparty, operational, cyber, and reputational risks. Currently, FHFA lacks the authority to regulate parties that provide services to the Enterprises. This white paper describes the Enterprises' third-party risk management programs for the first two phases of the risk management life cycle, Risk Assessment and Due Diligence in Third-Party Provider Selection, for fintechs.

OBJECTIVE, SCOPE, AND METHODOLOGY .....

The objective of this white paper was to provide an overview of the Enterprises' third-party risk management programs for the first two phases of the life cycle, Risk Assessment and Due Diligence in Third-Party Provider Selection. To achieve this objective, we reviewed internal and publicly available FHFA and Enterprise documents. We also interviewed FHFA and Enterprise officials.

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