REDACTED

Federal Housing Finance Agency
Office of Inspector General

FHFA is Addressing Inadequate Cybersecurity Incident Reports by the Enterprises

This report contains redactions of information that is privileged or otherwise protected from disclosure under applicable law.

Compliance Review • COM-2022-009 • September 22, 2022

COM-2022-009

September 22, 2022

Executive Summary

As part of their housing finance operations, Fannie Mae and Freddie Mac (the Enterprises) receive, store, and transmit significant and confidential information about borrowers, including financial data and personally identifiable information. Cyberattacks against the Enterprises could result in the theft of such data, as well as proprietary and trade secret information. Given the Enterprises' $7.2 trillion combined balance sheets as of year-end 2021, disruptions to their businesses from cyberattacks could result in widespread harm to the housing finance system.

In a 2019 evaluation, we found that the Federal Housing Finance Agency (FHFA) Division of Enterprise Regulation (DER) did not collect consistent cybersecurity incident data from the Enterprises. Consequently, DER lacked useful data that could assist in its efforts to oversee the Enterprises' controls to protect against cyberattacks and associated risks.

In response to our 2019 evaluation's recommendations, DER issued Advisory Bulletin 2020-05: *Enterprise Cybersecurity Incident Reporting* (AB 2020-05) in August 2020 that, among other things, requests that the Enterprises: (1) report to FHFA monthly regarding cybersecurity incidents; (2) immediately notify the Agency of any "major" cybersecurity incidents, which are those that interrupt one or more mission-critical functions or that result in the inability to achieve one or more mission-critical objectives, and (3) notify the Agency of any "significant" cybersecurity incidents, which interrupt or result in a degradation to one or more mission-critical functions or core services, within 24 hours of identifying such incidents. We closed our recommendations on October 26, 2020, based upon DER's issuance of AB 2020-05.

We initiated this compliance review to determine whether the Enterprises followed AB 2020-05 during the review period. We found that the Enterprises' monthly reports to DER generally met AB 2020-05's format and timeliness requirements. However, DER learned that Freddie Mac did not identify a "[redacted] cyberattack at a third party which potentially [redacted]. As a result of that incident, DER learned that Freddie Mac was not familiar with AB 2020-05's requirements for classifying and reporting cybersecurity incidents to the Agency. DER also found related shortcomings in the accuracy of Fannie Mae's cybersecurity incident reporting.

DER is taking several steps to remediate the identified shortcomings in the Enterprises' cybersecurity incident reporting. These steps include revising AB 2020-05's reporting template to provide additional instructions to the

COM-2022-009

September 22, 2022

Enterprises on how to report cybersecurity incidents in accordance with the template.

Given DER's independent detection of – and timely, unprompted corrective actions taken in response to – the reporting shortcomings referenced above, we are not reopening the 2019 evaluation's recommendations. However, we may revisit this topic after an appropriate interval to determine whether DER's actions have successfully addressed the Enterprises' cybersecurity incident reporting shortcomings.

This report was prepared by Wesley M. Phillips, Senior Policy Advisor, and Karen Berry, Senior Investigative Counsel. We appreciate the cooperation of FHFA staff, as well as the assistance of all those who contributed to the preparation of this report.

This report has been distributed to Congress, the Office of Management and Budget, and others and will be posted on our website, www.fhfaoig.gov.

/s/

Brian W. Baker
Deputy Inspector General,
Office of Compliance

TABLE OF CONTENTS

ABBREVIATIONS

AB 2020-05	Advisory Bulletin 2020-05: *Enterprise Cybersecurity Incident Reporting*, effective October 1, 2020
Agency or FHFA	Federal Housing Finance Agency
DCOR	FHFA Division of Conservatorship Oversight and Readiness
DER	FHFA Division of Enterprise Regulation
EIC	Examiner-in-Charge
Enterprises	Fannie Mae and Freddie Mac
Fannie Mae	Federal National Mortgage Association
Freddie Mac	Federal Home Loan Mortgage Corporation
NIST	National Institute of Standards and Technology
OIG	FHFA Office of Inspector General

BACKGROUND

Cyberattacks Pose Significant Risks to the Enterprises

As part of the Enterprises' processes to guarantee or purchase mortgage loans, they receive, store, and transmit significant information about borrowers, including financial data and personally identifiable information. Cyberattacks—such as malware attacks, password attacks, and distributed denial of service attacks—against the Enterprises could result in, or lead to, the theft of such confidential consumer data, as well as proprietary or trade secret information.[1] If an Enterprise were to suffer a significant cyberattack, the tangible costs of responding could be significant, including rebuilding compromised computer systems, purchasing credit monitoring for customers, and designing and implementing additional controls. Given the Enterprises' $7.2 trillion combined balance sheets,[2] disruptions to their businesses from cyberattacks could result in widespread harm to the housing finance system.

OIG's 2019 Evaluation Found Significant Disparities in the Enterprises' Cybersecurity Incident Reporting to FHFA

DER is responsible for examining the Enterprises to ensure their safety and soundness, including the adequacy of their controls to protect against cyberattacks. In a 2019 evaluation,[3] we observed that the Enterprises submitted their internal management reports to DER to provide information on certain cybersecurity incidents, including cyberattacks.[4]

Among other issues, we found that the Enterprises utilized different definitions for key cybersecurity-related terms related to their internal reports.[5] For example, Freddie Mac broadly defined a cybersecurity "event" as an "observable occurrence in a system or network that may

---

[1] Malware, or malicious software, is computer code that includes viruses, worms, and Trojan horses aimed at gaining control of systems. Password attacks involve the use of software to crack a user's password so that the attacker may obtain access to a secured system. The software systematically checks all possible keys or passwords until the correct one is found. A denial of service attack is intended to compromise the availability of networks and systems by overloading the network, thereby limiting legitimate traffic or communication. This type of attack can be done in a distributed fashion from many sources at once.

[2] Balance sheet total is as of year-end 2021.

[3] OIG, *FHFA Should Enhance Supervision of its Regulated Entities' Cybersecurity Risk Management by Obtaining Consistent Cybersecurity Incident Data* (EVL-2019-004) (September 23, 2019).

[4] Although no supervisory guidance required it, each Enterprise prepared monthly internal reports of cybersecurity matters for its management team. DER requested those reports in 2016 and 2017 and the Enterprises continued to provide them subsequently.

[5] The National Institute of Standards and Technology (NIST), a scientific standard-setting organization with the U.S. Department of Commerce, defines a "cybersecurity event" as a "cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation)." NIST defines a "cybersecurity incident" as a "cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery."

potentially be harmful and requires analysis." In contrast, Fannie Mae defined an "event" more narrowly to mean a "suspicious or anomalous event that has the potential to adversely affect Fannie Mae systems, data, or assets."

The differences in the Enterprises' definitions explained, at least in part, the disparities between their internal reports in terms of the volume and type of cybersecurity events captured therein. The Enterprises' definitional differences contributed to Freddie Mac reporting a significantly higher number of such incidents than did Fannie Mae during the same time period. This hindered DER's ability to compare and analyze the reported information.

We recommended that FHFA:

- Conduct the necessary inquiries and analyses to explain the large disparities in reported cybersecurity events and incidents between the Enterprises, and make use of that information in conjunction with [DER's] data collection initiatives.

- Evaluate the cybersecurity data it obtains from the [Enterprises] and revise, as appropriate, the Agency's existing cybersecurity reporting requirements to promote standardization of data, including the use of common definitions.

FHFA agreed with these recommendations. The Agency committed to evaluate cybersecurity data received from the Enterprises and to review its own reporting requirements in order to promote data standardization, including the use of common definitions. To those ends, the Agency stated that it would revise data collection formats, as appropriate, and "document a comparison of the definitions and data elements used in" the Enterprises' respective reporting requirements.

FHFA Issued an Advisory Bulletin in August 2020 to Ensure the Enterprises Report Cybersecurity Incidents Consistently

On August 21, 2020, FHFA issued AB 2020-05, effective October 1, 2020. AB 2020-05 requests that each Enterprise submit monthly reports to DER regarding its cybersecurity incidents,[6] using a standard, DER-provided reporting template. The template requires various pieces of specific information to be provided to DER, such as the date on which a particular cybersecurity incident began, the date on which it was detected, the incident's severity, its source, and a written description of the incident. The report is due within 15 calendar days of the end of each month (e.g., the July 2022 report for each Enterprise was due by August 15, 2022).

[6] AB-2020-05 defines a "reportable cybersecurity incident" as an occurrence that:

- occurs at the Enterprise or at a third party that actually or potentially jeopardizes the confidentiality, integrity, or availability of an Enterprise system or Enterprise information the system processes, stores, or transmits, or;

- constitutes a violation or imminent threat of violation of the Enterprise's security policies, security procedures, or acceptable use policies.

In addition to their monthly reports, AB 2020-05 also requests the Enterprises to report "major" cybersecurity incidents to the Examiner-in Charge (EIC) immediately, while "significant" incidents should be reported to the EIC within 24 hours of the Enterprise's significance determination.[7] AB 2020-05 defines a major cybersecurity incident as one that "interrupt(s) one or more mission critical functions or result(s) in the inability to achieve one or more mission critical objectives. Major incidents are likely to have a substantial negative impact on customers and/or counterparties and may pose reputational risk to the Enterprise. Cybersecurity incidents that include personally identifiable information may also be considered a major incident." A significant incident is one that "interrupt(s) or result(s) in a degradation to one or more mission critical functions or core services. Significant incidents may have a negative impact on customers and/or counterparties and may pose reputational risk to the Enterprise. Cybersecurity incidents that include substantial non-public information may also be considered significant incidents." Unlike the Enterprises' monthly reports, DER advised that no standard template has been provided to the Enterprises for reporting major or significant cybersecurity incidents.[8]

Based on AB 2020-05's requirements, we closed the two recommendations on October 26, 2020.

FINDINGS

We initiated this compliance review to determine whether, for the 18-month period of November 1, 2020, through April 30, 2022 (the review period), the Enterprises adhered to AB 2020-05's expectations for all monthly, major, or significant cybersecurity incident reports they submitted to DER.[9]

[7] Enterprise notifications to the EIC regarding major and significant incidents can occur via email, telephone, or in person so long as the Enterprise confirms that DER received the notifications. In addition to contacting the EIC, the Enterprise should send a report describing the major or significant incident to DER using secure methods established by FHFA.

[8] The Enterprises' monthly reports should include the details of any major or significant cybersecurity incidents separately reported to FHFA during the reporting period.

[9] OIG understands that on March 24, 2021, FHFA's Division of Conservatorship Oversight and Readiness (DCOR) issued revised guidance entitled *Conservator Guidance: Information Security and Business Disruption Incident Reporting* which directed the Enterprises to provide certain cybersecurity information to DCOR. This DCOR guidance was outside the scope of this compliance review as it did not serve as the basis for our closure of the recommendations in our 2019 report. For this reason, this report focuses only on the Enterprises' adherence to AB 2020-05 during the review period.

Although The Enterprises' Monthly Reports Generally Met AB 2020-05's Format and Timeliness Requirements, the Enterprises Incorrectly Classified Various Cybersecurity Incidents

Each Enterprise satisfied AB 2020-05's direction to submit monthly cybersecurity incident reports to DER for each of the 18 months in our review period using DER's specified template. Further, each Enterprise submitted 16 of these 18 monthly reports (89%) within 15 calendar days of the end of the reporting month per AB 2020-05.[10]

Each Enterprise used DER's template for all of its monthly reports, and all but one of the reports utilized the required terminology and classifications in DER's monthly reporting template.[11]

Freddie Mac Failed to Properly Classify a [redacted] Cybersecurity Incident

Although DER notes that the Enterprises did not submit any major cybersecurity incident reports during our review period, DER separately learned that Freddie Mac had failed to identify and properly classify a [redacted] cybersecurity incident. Consequently, it requested that Freddie Mac review three monthly reports and make any necessary changes in accordance with AB 2020-05. Freddie Mac complied with the request, reviewing the reports and changing the severity classification of a particular reported incident from "[redacted]" to "[redacted]."

DER learned that Freddie Mac had initially failed to recognize the cybersecurity incident's potential severity because the Enterprise was uncertain regarding AB 2020-05's reporting requirements for [redacted] at third parties associated with the Enterprises.[12] DER also found that Freddie Mac was not assigning to cybersecurity incidents [redacted]

[10] Fannie Mae submitted one report seven days late and one report two days late; Freddie Mac submitted one report four days late and one report three days late.

[11] In one report, Freddie Mac did not initially use the DER-specified terms to report cybersecurity incidents. DER requested Freddie Mac to correct and re-submit the report, which it did.

[12] The Enterprises rely on numerous third parties to provide services that are critical to their business such as mortgage servicing, mortgage insurance, single-family mortgage-backed security issuance and administration, and technology functions. DER learned that Freddie Mac "was unaware that a reportable cybersecurity incident is defined in the AB as an occurrence that 'occurs at the Enterprise or at a third party that actually or potentially jeopardizes the confidentiality, integrity, or availability of … Enterprise information the system processes, stores, or transmits'[.]" In March 2022, Fannie Mae reported to DER a [redacted] at one of its [redacted], which was also a [redacted] for Freddie Mac. This report prompted DER to seek additional information from Freddie Mac on its own cybersecurity incident reporting regarding this [redacted]. Based on this incident, DER initiated a review of both Enterprises' cybersecurity incident reporting under AB 2020-05.

[redacted] consistent with AB 2020-05. DER stated that this is a concern, noting that the [redacted] carries implications for timely reporting to FHFA and other stakeholders.[13]

As a consequence of these issues, DER [redacted] Freddie Mac's cybersecurity incident conservatorship scorecard rating for the first quarter of 2022 from "[redacted]" to "[redacted]," which may impact the compensation of Freddie Mac's executives.[14] DER also reports that it is revising the monthly reporting template to provide better guidance to the Enterprises in reporting cybersecurity incidents as described below.

Fannie Mae Did Not Notify DER Promptly When It Re-Classified a Cybersecurity Incident's Severity Level

DER expects the Enterprises to report changes in a particular cybersecurity incident's severity level when such changes occur, rather than when the incident closes (potentially, months later).[15] Notwithstanding this expectation, DER found that, on multiple occasions, Fannie Mae classified an incident at a specific severity level and continued to report that same level to FHFA over the life of the incident, even after the Enterprise had decided to re-classify the incident's severity. In those cases, Fannie Mae did not report the severity classification change until it eventually reported the incident as "closed" in a final monthly report to the Agency.

As a consequence of Fannie Mae's failures to report its severity re-classifications in a timely manner, DER [redacted] the Enterprise's cybersecurity incident conservatorship scorecard rating for the first quarter of 2022 from "[redacted]" to "[redacted]."

DER is Revising Its Monthly Reporting Template to Provide Better Guidance to the Enterprises

DER officials said they took a "fresh look" at the monthly cybersecurity incident reporting template because of its review of the Enterprises' handling of the [redacted] at the [redacted] to

[13] When an Enterprise fails to recognize that an incident is significant, it is unlikely [redacted] to meet AB 2020-05's 24-hour notification requirement.

[14] Each year since 2012, FHFA has published a conservatorship scorecard tied to the conservatorship strategic plan in place at the time. The scorecard serves as an "essential tool" for communicating the Agency's priorities and expectations to the Enterprises and holding them accountable for implementation of the conservatorship strategic plan. FHFA rates the Enterprises' performance with the scorecard using classifications such as "[redacted]," meaning the Enterprise is on schedule to meet quarterly milestones, or "[redacted]," meaning the Enterprise is on schedule but "with significant issues and concerns." Executive compensation at an Enterprise is based, in part, on the Enterprise's performance in meeting conservatorship scorecard goals.

[15] As noted in a prior footnote, Fannie Mae reported its [redacted] to DER. While this prompted DER's review of both Enterprises' cybersecurity incident reporting under AB 2020-05, it was not part of the shortcoming that DER identified at Fannie Mae.

identify areas of improvement. The officials also said they were trying to ensure that the Enterprises understand FHFA's expectations and will provide additional clarity through enhanced reporting examples.

To accomplish this, DER is adding fields to the template and providing clarifying examples of what could fall into the specific reporting categories. DER anticipates issuing a revised reporting template to the Enterprises in September 2022.

CONCLUSIONS

The Enterprises generally adhered to AB 2020-05's format and timeliness requirements for their monthly reporting of cybersecurity incidents. However, DER has found substantial shortcomings in their classifications of the severity levels of multiple incidents, and for one Enterprise, in notifying the Agency in a timely manner that it had subsequently re-classified the severity of certain incidents.

Given DER's independent detection of – and timely, unprompted corrective actions taken in response to – the shortcomings referenced above, we are not reopening the 2019 evaluation's recommendations. However, we may revisit this topic after an appropriate interval to determine whether DER's actions have successfully addressed the Enterprises' cybersecurity incident reporting shortcomings.

OBJECTIVE, SCOPE, AND METHODOLOGY

We initiated this compliance review to determine whether the Enterprises adhered to certain of AB 2020-05's directions for reporting cybersecurity incidents for the period November 1, 2020, through April 30, 2022.

To conduct our work, we reviewed the Enterprises' monthly reports and other Agency documentation. We also interviewed DER officials.

We conducted our compliance review from May 2022 through July 2022 under the authority of the Inspector General Act of 1978, as amended, and in accordance with the *Quality Standards for Inspection and Evaluation* (December 2020), which were promulgated by the Council of the Inspectors General on Integrity and Efficiency.

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