Commonwealth of Massachusetts
Office of the State Auditor
Suzanne M. Bump
Making government work better

Official Audit Report – Issued November 18, 2021

Division of Banks

For the period July 1, 2017 through June 30, 2019

Commonwealth of Massachusetts
Office of the State Auditor
Suzanne M. Bump
Making government work better

November 18, 2021

Ms. Mary Gallagher, Commissioner of Banks
Division of Banks
1000 Washington Street, 10th Floor
Boston, MA 02118

Dear Commissioner Gallagher:

I am pleased to provide this performance audit of the Division of Banks. This report details the audit objectives, scope, methodology, findings, and recommendations for the audit period, July 1, 2017 through June 30, 2019. My audit staff discussed the contents of this report with management of the division, whose comments are reflected in this report.

I would also like to express my appreciation to the Division of Banks for the cooperation and assistance provided to my staff during the audit.

Sincerely,

Suzanne M. Bump
Auditor of the Commonwealth

cc: Mike Kennealy, Secretary of the Executive Office of Housing and Economic Development
Edward Palleschi, Undersecretary of the Office of Consumer Affairs and Business Regulation

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

DOB	Division of Banks
EOHED	Executive Office of Housing and Economic Development
EOTSS	Executive Office of Technology Services and Security
FinCEN	Financial Crimes Enforcement Network
FTA	foreign transmittal agency
NDRS	Non-Depository Regulatory System
NMLS	Nationwide Mortgage Licensing System
OCABR	Office of Consumer Affairs and Business Regulation
RMS	Regulatory Management System

EXECUTIVE SUMMARY

In accordance with Section 12 of Chapter 11 of the Massachusetts General Laws, the Office of the State Auditor has conducted a performance audit of the Division of Banks (DOB) for the period July 1, 2017 through June 30, 2019.

In this performance audit, we determined whether DOB (1) ensured that foreign transmittal agencies maintained three years of records in accordance with Section 10 of Chapter 169 of the General Laws; (2) collected, and acted on, information on mortgage lenders or brokers that may have had their licenses suspended or revoked by the licensing authority of any other state, as required by Sections 42.04(2)(b)(4) and 42.06(2)(b)(4) of Title 209 of the Code of Massachusetts Regulations; and (3) shared its information regarding Massachusetts-licensed lenders and brokers that had been subjected to formal enforcement action from other states, as required by Section 5107 of Title 12 of the United States Code and Section 1508(d)(3) of Title V of Public Law 110-289 (the Secure and Fair Enforcement for Mortgage Licensing Act of 2008). In addition, as part of our data reliability assessment, we determined whether DOB ensured that its employees had the cybersecurity awareness training required by the Executive Office of Technology Services and Security (EOTSS).

Below is a summary of our findings and recommendations, with links to each page listed.

Finding 1 **Page 8**	DOB did not ensure that all of its employees promptly completed cybersecurity awareness training.
Recommendations **Page 9**	1. DOB should develop and implement policies and procedures, in accordance with EOTSS policies, that require all current employees to receive annual cybersecurity awareness training. 2. DOB should develop and implement policies and procedures, in accordance with EOTSS policies, that require newly hired employees to receive cybersecurity awareness training during orientation or within a prescribed timeline before they have access to DOB's systems.

OVERVIEW OF AUDITED ENTITY

The Division of Banks (DOB) was established under Section 1 of Chapter 26 of the Massachusetts General Laws and operates under the direction of a commissioner of banks who is appointed by the Governor. DOB is a division of the Office of Consumer Affairs and Business Regulation (OCABR) within the Executive Office of Housing and Economic Development (EOHED). According to DOB's website,

> *[DOB] is the chartering authority and primary regulator for financial service providers in Massachusetts. DOB's primary mission is to ensure a sound, competitive, and accessible financial services environment throughout the Commonwealth.*

DOB is responsible for the supervision and regulation of non-depository institutions, which included 8,725 licensees and 4,793 branches and agent locations as of January 1, 2019. Non-depository institutions include mortgage lenders, brokers, loan originators, consumer finance companies, money-service businesses (i.e., foreign transmittal agencies, check sellers, and check cashers), debt collectors, and loan servicers. DOB also oversees depository institutions, which include state-chartered banks (cooperative banks, savings banks, and various types of trust companies) and credit unions. As of January 1, 2019, according to DOB's "Division at a Glance" report, there were 176 depository institutions with 1,313 depository branch office locations holding $399.2 billion in total assets as of December 31, 2018.

DOB has four units: Non-depository Institution Supervision, Depository Institution Supervision, Enforcement and Investigation, and Administration. A policy group chaired by the commissioner of banks and consisting of DOB senior management oversees all regulatory matters, conducts strategic planning, and directs day-to-day operations. OCABR's Administrative Services Unit performs most of the financial and accounting functions for DOB. DOB's information technology is managed and maintained by the EOHED Information Technology Department.

DOB received state appropriations of $18,111,512 and $18,507,880 for fiscal years 2018 and 2019, respectively. During our audit period, DOB had approximately 183 employees, including bank examiners, managers, and support employees. It is headquartered at 1000 Washington Street in Boston and has field offices in Woburn, Lakeville, and Springfield.

Secure and Fair Enforcement for Mortgage Licensing Act of 2008

The Secure and Fair Enforcement for Mortgage Licensing Act of 2008 required the establishment of a nationwide licensing and registration system for residential mortgage loan originators. A federal registry called the Nationwide Mortgage Licensing System (NMLS) was created accordingly. NMLS is a Web-based platform that state regulatory agencies use to perform a variety of tasks, such as administering initial license applications and monitoring ongoing compliance with licensing requirements. Licensees (individuals and companies) can use NMLS to apply for, renew, surrender, or amend licenses; register for license examinations in one or more states; and make payments for licenses and examinations. Consumers can use NMLS for such things as determining whether a mortgage loan originator is authorized to conduct business in a particular state.

DOB receives notifications from NMLS regarding any enforcement actions by other states against residential mortgage lenders and brokers that have, or have applied for, active licenses in Massachusetts. DOB updates NMLS when it takes formal enforcement action against any Massachusetts-licensed mortgage lender or broker.

Foreign Transmittal Agencies Overseen by the Non-depository Institution Supervision Unit

According to Section 45.02 of Title 209 of the Code of Massachusetts Regulations, a foreign transmittal agency (FTA) is "a person who engages or is financially interested in the business of receiving deposits of money for the purpose of transmitting the same or equivalents thereof to foreign countries." The United States Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) requires FTAs to file reports on certain transactions in NMLS and maintain supporting documentation. FinCEN analyzes these reports to support law enforcement efforts and identify money laundering and related trends and patterns.

FTAs must be licensed by DOB to operate in Massachusetts. DOB management told us that the division reviews FTA record retention policies during the initial licensing process and during examinations. DOB management also stated that DOB examines FTAs every three years, unless it identifies an increased risk (e.g., consumer complaints, notifications from other states), in which case it performs an examination sooner. During an examination, DOB analyzes samples of transaction records to assess an FTA's compliance with federal and state regulations. DOB requires FTAs to take appropriate and timely corrective action on any reporting or recordkeeping issues. Serious violations could cause an FTA to lose

its operating license. As of January 1, 2019, there were 68 licensed FTAs operating 2,497 branches in the Commonwealth.

Examination Process

DOB performs its examinations on a rotating schedule, every three years for mortgage lenders and brokers and every two years for check cashers and FTAs. When following up on prior examination issues, DOB conducts examinations every two years or less for mortgage lenders and brokers and more often for check cashers and FTAs. DOB uses a standard examination template to perform its examinations. DOB determines an entity's overall consumer protection compliance rating[1] by considering the entity's adherence to consumer protection laws and regulations and the effectiveness of its compliance with those laws and regulations. If an examination ends with a public enforcement action, DOB publishes information about the action on its website in addition to reporting it in NMLS. DOB's annual report is also published on the website and includes formal and informal enforcement actions DOB has taken.

DOB stores all information about its ongoing and completed examinations on a shared drive that it calls its M drive. Agency staff members can access the drive either through DOB's internal network or remotely using a drive access process established by DOB. DOB management gives employees access and other privileges, such as the ability to edit information on the drive, based on the employees' business needs.

Regulatory Management System

DOB uses a software application it calls the Regulatory Management System (RMS) to oversee and manage certain activities of state financial licensees and state-chartered banks and credit unions. RMS includes an integrated complaint tracking system, an education management system, and an examination management system. RMS also includes a subsystem called the Non-Depository Regulatory System, which is a repository and DOB's system of record to track and record the results of its licensee examinations.

1. According to DOB's Regulatory Bulletin 1.1-101 (Examination Policy), the consumer protection compliance rating "reflects the [entity's] record of helping to meet the credit needs of its entire community, including low- and moderate-income neighborhoods and individuals consistent with safe and sound operations."

AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY

In accordance with Section 12 of Chapter 11 of the Massachusetts General Laws, the Office of the State Auditor has conducted a performance audit of certain activities of the Division of Banks (DOB) for the period July 1, 2017 through June 30, 2019.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Below is a list of our audit objectives, indicating each question we intended our audit to answer and the conclusion we reached regarding each objective.

Objective	Conclusion
1. Does DOB ensure that foreign transmittal agency (FTA) licensees maintain three years of records in accordance with Section 10 of Chapter 169 of the General Laws?	**Yes**
2. Does DOB collect, and act on, information from other states in compliance with Sections 42.04(2)(b)(4) and 42.06(2)(b)(4) of Title 209 of the Code of Massachusetts Regulations?	**Yes**
3. Does DOB share its information regarding Massachusetts enforcement actions for licensed mortgage lenders and brokers with other states, as required by Section 5107 of Title 12 of the United States Code and Section 1508(d)(3) of Title V of Public Law 110-289?	**Yes**

In performing our audit work, we found that not all DOB employees promptly received cybersecurity awareness training, as discussed in Finding 1.

To achieve our audit objectives, we gained an understanding of DOB's internal control environment related to the objectives by reviewing agency policies and procedures, as well as conducting inquiries with DOB's staff and management. We evaluated the design, and tested the effectiveness, of controls DOB had established over monitoring FTA recordkeeping and notifying other states of public enforcement actions.

We performed the following procedures to obtain sufficient, appropriate audit evidence to address the audit objectives.

To determine whether DOB ensured that FTAs maintained three years of records in accordance with Section 10 of Chapter 169 of the General Laws, we selected a nonstatistical, random sample of 10 of the 44 FTA examinations DOB completed during our audit period. We inspected records of the detailed daily revenue and/or expense transactions, data reports, and money transfers DOB maintained for these examinations and confirmed that these 10 FTAs retained their records for at least three years.

To determine whether DOB collected, and acted on, information about mortgage lenders and brokers that may have had their licenses suspended or revoked by the licensing authority of any other state, we asked DOB for a report from the Nationwide Mortgage License System (NMLS) that showed the mortgage lenders and brokers that had had their licenses suspended or revoked by any state other than Massachusetts during the audit period. By reviewing examination schedules, completed examination folders, and file notations, we confirmed that DOB investigated and obtained actions due from other states regarding all 13 license suspensions or revocations in the report to ensure that it acted on notifications from NMLS.

We extracted all 213 examinations of licensed mortgage lenders and brokers that DOB completed during our audit period from the Non-Depository Regulatory System (NDRS) and separated them into two strata: examinations without formal enforcement action and examinations with formal enforcement action. For the first stratum, we inspected a nonstatistical, random sample of 20 of 207 examination folders to verify that there were no formal enforcement actions that resulted in reporting in NMLS. For the second stratum, we inspected all 6 examination folders to verify that DOB had reported the formal enforcement actions in NMLS so that notice of the action would be available to other states.

We used nonstatistical sampling methods and therefore could not project the results of our testing to the population.

Data Reliability

We determined the reliability of the data we received from NDRS by testing for accuracy and completeness. We randomly selected 10 of 257 examinations of FTAs and mortgage lenders and brokers from our audit period from NDRS and traced them to the source documentation (the final examination

report, a sheet signed by different levels of reviewers, and the commissioner of banks' letter to the licensee) to determine the accuracy of the data. We then compared DOB's published annual report, which showed a total of 257 examination reports during our audit period, to reports generated from NDRS to determine the completeness of the population of examinations.

In addition, we determined the reliability of the data we received from NDRS by conducting interviews with DOB officials about access rights and privileges for the Regulatory Management System (RMS), NDRS, and the M drive. We also tested certain information system general controls regarding access and security management.

From the 196 employees who had access to NDRS and the M drive for the audit period, we randomly selected 10 of the 19 who were hired during the audit period, and 20 of the 177 who were hired before the audit period, and reviewed cybersecurity awareness training certificates to determine whether they received the required annual cybersecurity awareness training (see Finding 1). In addition, we randomly selected 20 of the 196 employees and reviewed the email requests from DOB's Human Resources Department to verify that those employees' system access rights and editing privileges were authorized.

For all 33 employees terminated during our audit period, we compared the termination dates from DOB's Human Resources Department to the access termination dates in RMS, NDRS, and the M drive to determine whether employees were removed from all three systems within 24 hours after termination.

Based on the results of our data reliability assessments, we determined that the information obtained for our audit period was sufficiently reliable for the purposes of our audit work.

DETAILED AUDIT FINDINGS WITH AUDITEE'S RESPONSE

1. The Division of Banks did not ensure that all of its employees promptly completed cybersecurity awareness training.

The Division of Banks (DOB) did not ensure that all new employees received cybersecurity awareness training when they began working at DOB or that all current employees received annual cybersecurity awareness training in a timely manner. Specifically, of the 196 DOB employees who were active users of the Regulatory Management System and Non-Depository Regulatory System during our audit period, 3 received their annual cybersecurity awareness training 18 to 39 days late, and 7 newly hired employees did not receive cybersecurity awareness training until 39 to 235 days after they began work.

Untimely cybersecurity awareness training may lead to user error and compromise the integrity and security of protected information in DOB's information technology systems.

Authoritative Guidance

Section 5.1.1 of the Executive Office of Technology Services and Security's (EOTSS's) Acceptable Use of Information Technology Policy IS.002, which was in effect January 10, 2017, states, "All new hires must complete security awareness training within the established new hire training timeline and regularly thereafter."

Section 6.2.4 of EOTSS's Information Security Risk Management Standard IS.010, which went into effect October 15, 2018, states, "All personnel will be required to complete Annual Security Awareness Training."

Section 6 of state Executive Order 504, which was in effect January 1, 2009 through October 25, 2019, states,

> *All agency heads, managers, supervisors, and employees (including contract employees) shall attend mandatory information security training within one year of the effective date of this Order. For future employees, such training shall be part of the standardized orientation provided at the time they commence work. Such training shall include, without limitation, guidance to employees regarding how to identify, maintain and safeguard records and data that contain personal information.*

Reason for Issue

DOB does not have policies and procedures that require all current employees to receive annual cybersecurity awareness training. It also does not have policies and procedures that require newly hired employees to receive cybersecurity awareness training during orientation or within a prescribed timeline before they have access to DOB's systems.

Recommendations

1. DOB should develop and implement policies and procedures, in accordance with EOTSS policies, that require all current employees to receive annual cybersecurity awareness training.
2. DOB should develop and implement policies and procedures, in accordance with EOTSS policies, that require newly hired employees to receive cybersecurity awareness training during orientation or within a prescribed timeline before they have access to DOB's systems.

Auditee's Response

The DOB reviewed the recommendations, and we are developing and implementing policies and procedures in accordance with EOTSS policies to ensure employees receive the training in a timely manner. Additionally, the DOB will engage with [the Executive Office of Housing and Economic Development's Information Technology Department] and human resources to ensure newly hired employees receive cybersecurity awareness training during orientation or within a prescribed timeline before they have access to DOB's systems. Our agency recognizes the critical role of cybersecurity training and preparedness in all organizations, and we will ensure our policies and procedures align with the EOTSS policies.

Auditor's Reply

Based on its response, DOB is taking steps to address these issues.