IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CHOOSE AN EFFECTIVE HMDA REPORTING TOOL

Rafique Ahmed Mohammad

Director, Compliance Data Management, LoanDepot LLC, Department of Information Technology,
University of the Cumberlands
6561 Irvine Center Drive, Irvine, CA, 92618

Abstract: Consumer Financial Protection Bureau Implemented the Regulation C, 12 CFR Part 1003 (Regulation C) in October 2015. The Reg C requirements were developed by federal financial institutions examination council (FFIEC), the Board of Governors of the Federal Reserve System (Board), the Consumer Financial Protection Bureau (CFPB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the State Liaison Committee (SLC) — and the U.S. Department of Housing and Urban Development (HUD). The 2015 HMDA rule guided the types of institutions that qualify for data reporting and transactions subject to Reg C. The bank, savings association or credit union meets or exceeds either the closed-end mortgage loan or the open-end line of credit loan volume threshold in each of the two preceding calendar years. Beginning July 1, 2020, a bank, savings organization, or credit union that generated at least 100 closed-end home loans or 500 open-end lines of credit in each of the previous two calendar years meets or exceeds the loan-volume requirement. To determine if a transaction is subject to Regulation C, a financial institution should first determine whether the loan or line of credit is a closed-end mortgage or an open-end line of credit. Currently, the institutions subject to Reg C collect the data and report to the CFPB quarterly. To collect the data and report to the CFPB, the institutions utilize third-party vendors who provide regulatory reporting software services.

Keywords: CFPB, Reg C, Closed-end mortgage, open-end line of credit

Introduction

The home mortgage disclosure act was effective January 1, 2018. The data-related requirements serve three purposes, the first one is to validate that the institutions are serving the community housing needs, the second one is to provide support to the public officials in distributing public investment to attract private investments, and finally, the last one is to identify discriminatory lending patterns and enforce actions for the discriminatory lending practices. The institutions should collect the new data points in 2018 and report the data in the 2019 calendar year. Effective January 1, 2020, quarterly reporting is required for large-volume reporters. The HMDA rule requires the institutions to collect, record and report the data for covered loans and applications. Partially exempt institutions are not required to collect, record, and report the data. The new rule amends to collect the applicant’s ethnicity, race, and sex. With the new data requirements effective January 1, 2018, the institutions rely on third-party vendors to provide the required software for collecting, recording, and submitting the data to the CFPB. However, various risks are involved in using third-party vendor software, like data breaches, operational disruption, legal/compliance risks, and reputational damage. This article explores the various HMDA reporting tools available in the marketplace and explains various associated risks; thus, institutions can choose an effective HMDA reporting tool with minimal risk software.

I. LITERATURE REVIEW

Many vendors are available in the market to provide the institutions with the ability to gather data, record and submit the mortgage loan data to the CFPB. The solutions include desktop and web-based platforms. CFPB has defined numerous error validations as part of the data submission process [1]. The errors are classified into four categories syntactical, validity, quality, and macro edits. Syntactical errors are the checks to see if the loan/application registration is in the proper format and that the data covers the correct filing year. For example, a syntactical edit is made if none of the rows in the loan/application register begin with number two (2), indicating that the following data fields contain information about the reported loan or application. The filer must address all syntactical editing mistakes and re-upload the amended loan/application register to the HMDA Platform before submitting the loan/application register. Validity Edits verify whether each data field contains valid values. For example, a validity edit is performed if the contact person's phone number does not conform to the pattern "999-999-9999." The loan/application register can only be submitted once the filer is present. Corrects any validity edit mistakes and uploads the revised loan/application record to the HMDA Platform. Quality Edits verify that entries in individual data fields or combinations of data fields match the intended values. For example, a quality edit is performed if the provided Tax Identification Number differs from that supplied by the institution on the previous year's loan/application register. The filer can only submit the loan/application register if he or she either validates the accuracy of all values identified by quality edits on the HMDA Platform, corrects the flagged values, and re-uploads the amended loan/application register to HM Macro Edits, verify that the submitted loan/application. Registration is consistent with expected values. For example, a macro quality edit is performed if the reported proportion of multifamily loans surpasses 10% of the loan/application register entries. The loan/application register cannot be submitted until the filer either validates 95 percent of the correctness of all the values indicated by the HMDA Platform's macro quality modifications or corrects the flagged values and re-uploads the amended loan/application register to the HMDA Platform. Once the institutions are ready to submit the data, they must prepare the file in a specific file format and then upload it to the CFPB platform. Once the data is uploaded, the platform either successfully submits the data or throws edits for the institutions to fix and submit again. Inaccurate data submission leads to audits and could lead to potential fines by the CFPB. In the event of an audit, the institutions have to re-submit the data again for the current/prior years. Institutions usually license/independently develop the loan origination system for maintaining the loan life cycle. The loan origination system is the record system for the loan data, fed to the vendor software for the CFPB data submission. CFPB provides guidelines on the point at which the data should be collected within the loan origination system, and this data should only be submitted to the agency. The institutions follow these guidelines and implement the appropriate enhancements/functionality with the loan origination system to capture the HMDA data.

II. CHALLENGES IN COLLECTING HMDA DATA FROM THE LOS

Under the Home Mortgage Disclosure Act (HMDA), covered institutions must make loan information available to the public. These data are used by regulators, examiners, academics, industry leaders, and members of the general public to analyze mortgage lenders' performance in meeting the goals established by the Equal Credit Opportunity Act (ECOA), the Fair Housing Act (FHA), and the Community Reinvestment Act (CRA). Inaccurate HMDA data stymies attempt to discover potential discriminatory practices in home mortgage lending and to monitor other compliance issues. As the Consumer Finance Protection Bureau (CFPB) showed in 2013, compliance with HMDA is a central focal point for enforcement. This enforcement effort will only intensify as the CFPB considers adopting additional HMDA reporting standards. These modifications will increase the complexity and compliance risk of HMDA filings. Poor HMDA data integrity may also indicate issues that might negatively affect a lender's business intelligence (BI) system. Lenders rely on BI tools to inform critical business choices regarding the firm's marketing, operations, finance, and other strategic areas. Data incorporated in BI systems is frequently derived from the same loan origination systems utilized for HMDA reports. The conclusion is that inaccuracies in HMDA reportable data points jeopardize the information CEOs rely on in their decision-making framework. This might result in developing and implementing strategies and tactics based on incorrect data points. For covered mortgage lenders, HMDA reporting can be a considerable problem. The complexity of corporate systems and the collaboration necessary among many individuals and systems creates multiple potential for reporting mistakes. We address four frequent errors lenders make throughout the HMDA reporting process and how to reduce these errors in your HMDA compliance management system below. These four inaccuracies are the first in several HMDA reporting problems we will cover in forthcoming publications.

A. Failure to Capture All HMDA-Reportable Transactions

Accurate HMDA reporting requires the identification of all reportable transactions in a timely fashion. For some lenders, the complexity of their business models can lead to missing reportable applications. Properties with multiple purposes or multiple dwellings and applicants with serial investment properties present challenges. Loans related to manufactured home purchases, home improvements, and loans sold in secondary markets commonly present scenarios that complicate assessing an application should be reported. In addition, managing applications that become applications that were not eventually submitted to underwriting may result in the exclusion of reportable applications that should be coded as withdrawn or closed for incompleteness.

B. Incorrect Loan Amount

The loan amount is one of the HMDA variables that many lenders need help to report accurately in their HMDA LAR. Errors can be caused by simple data entry mistakes (e.g., typographical errors, transposed numbers, inaccurate rounding, etc.), recording the base loan amount instead of the note amount, and changes in the amount requested during the application process from appraisals, counteroffers, etc. Examiners have identified this as a standard reporting error to scrutinize during an audit of HMDA data, and lenders should be particularly mindful of the potential for errors in this field.

C. INACCURATE GEOCODING

The HMDA fields that are the product of geocoding (MSA et al.) are crucial for any geographic-based analysis of lending patterns, such as CRA and redlining analyses. Based on our experience, assigning the correct Census Tract presents the greatest geocoding challenge to lenders. The geocoding fields are unique among HMDA reporting requirements for many lenders because they depend on third-party software or services that can result in occasional or systemic errors. These errors can raise doubts about an entire HMDA submission. Whether you rely on a manual or automated process that integrates your system with a third-party geocoding provider, several factors can lead to reporting errors. These include failing to audit externally sourced geocoding results, using the wrong base geocoding year, and using the wrong address.

D. Incorrect Rate Spread Calculation

Calculating the rate spread for each HMDA-reported loan requires incorporating market interest rate data published by the FFIEC. While there are tools that help automate the calculation and recording of these data for HMDA, the underlying calculation relies on the accuracy of three variables: the rate lock date, the action date, and the amortization type. Errors in recording any of these three variables will yield incorrect calculations. In our experience, capturing the appropriate rate lock date is one field that presents challenges to some lenders due to the possibility of it changing during the application process from rate re-locking requests by the borrower. As they are implemented, loan origination systems may prevent lenders from changing the original rate lock date and from recording re-lock dates, resulting in miscalculations of the rate spread.

E. What You Can Do to Mitigate These Errors

Managing these errors requires a solid grasp of HMDA reporting requirements and how data points are identified, entered into your loan origination system, and preserved for eventual reporting. When assisting clients, ADI recommends several steps for assessing and correcting common HMDA errors, including Review automated systems to ensure they are accurately identifying HMDA-reportable applications and loans; Analyze excluded transactions, such as leads, to ensure they do not meet the definition of an application under HMDA; Establish controls to minimize data entry errors; Review and analyze processes that transfer data between systems to ensure transferred data are accurate and correctly mapped for the HMDA submission; Perform an audit on a sample of applications to determine the accuracy of the recorded data based on source documentation; and Conduct a full HMDA data scrub if error rates are above thresholds established by the CFPB [2]. With new reporting requirements on the horizon and increased regulatory use of HMDA data in supervisory and examination responsibilities, the risk of HMDA reporting errors will only grow. Moreover, HMDA data will increasingly reveal the broad characteristics of markets and customers each reporting lender serves. Then, lenders must implement solid controls and a culture of compliance with HMDA reporting requirements. This will help lenders overcome current and future compliance challenges and maximize internal data quality that can be leveraged to support their marketing and growth strategies.

III. Risks Identified in the vendor software

F. Cybersecurity

Today, third parties are frequently used as a vector for cyber-attacks. Attackers enter supply-chain linkages, infecting their systems and gadgets invisibly. The attacker then employs the third party as a "platform" to conduct assaults against more valuable targets.

G. Regulatory/Compliance

This sort of risk is frequently caused by a third-party security control failure that results in data loss, which leads to a data privacy breach that exposes the primary organization to accountability and penalties. This risk is a significant problem for modern businesses, as 80% of data breaches now involve a third party. Third-party violations of environmental or labor laws can potentially lead to regulatory/compliance risk.

H. Financial

A third-party activity that harms an organization's financial status is referred to as financial risk. This damage might result from poor vendor work or a faulty component that slows down the company and decreases income. Financial harm might also take the shape of penalties or legal bills.

I. Operational

The prospect of a third-party action causing an operational shutdown creates operational risk. A vendor victimizing a network attack or natural disaster may create a system lockdown, disrupting company operations momentarily.

J. Reputational

Negative public opinion generated by published security breaches, legal transgressions, or lousy customer interactions creates reputational risk. When you collaborate with a third party with terrible labor standards or treat its employees unjustly, you put your reputation at risk.

K. Strategic

Strategic risk refers to the issues that arise when third-party and organizational business plans are not in sync. This risk is frequently caused by a third party's bad business decision. Some third-party risks can have a wide range of consequences for enterprises. Data breaches are an example of a severe risk that spans numerous risk categories—they interrupt operations, pose a regulatory risk, and can result in financial and reputational harm.

IV. RISK MANAGEMENT

Third-party risk management is an organizational discipline that evaluates and mitigates the risks of interacting with suppliers and third-party service providers. Third-party risk management entails establishing strong governance over your vendor network and adhering to strict vendor selection, onboarding, performance monitoring, and offboarding processes. You must take the following actions to maintain good governance over your vendors: Recognize the risks of outsourcing specific tasks and services to third-party vendors.

- Sort your vendors and assets into categories; identify your significant vendors.
- Develop a vendor due diligence approach for your company based on your organization's internal vendor risk appetite.
- Specify the critical security, privacy, and business continuity rules suppliers must have before working with your firm.
- Assess suppliers' risk levels before onboarding them by sending questionnaires to vendors and utilizing publicly available data sources such as security ratings (we will show you questions to ask your vendors during the pre-contract due diligence process in a subsequent section).
- Only onboard suppliers once your risk management team has examined the risk assessment results of the vendor and concluded that the risks, they bring to your business are at an acceptable level.
- Reduce certain vendor risks by taking further actions, such as putting in place a contract that explains how the vendor will manage the risks you are concerned about.
- Continuously monitor and audit vendors.
- Make sure that correct risk management practices are followed throughout vendor offboarding.

V. CONCLUSION

Managing third-party risk is critical for organizations today but also tricky. Third-party risk is increasing as more businesses continue to outsource more and more of their business services. Today, organizations must urgently strengthen their third-party risk management skills. Vendor Risk Management solutions may simplify life for enterprises ready to take the lead in controlling third-party risk. This program will assist customers in tracking and managing their suppliers and creating, sending, and reviewing risk assessment questionnaires to detect vendor risk effectively.

REFERENCES

[1] Submitter, B. D. (2020). An updated review of the new and revised data points in HMDA: Further observations using the 2019 HMDA Data. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3786976

[2] Bar, M., & Kakar, V. (2022). Lender heterogeneity in Home Mortgage Lending Evidence from HMDA data in context of the COVID-19 pandemic. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4074749