Volume 38, Issue 7 | JULY 2021

DISCLOSURE

A MONTHLY COMPLIANCE REVIEW PUBLISHED BY THE IOWA BANKERS ASSOCIATION

CYBERATTACKS

THE RISK IS REAL

ALSO IN THIS ISSUE:

HMDA 2022: REPORTING OPEN-END LINES OF CREDIT

IOWA BANKERS ASSOCIATION

PUBLISHER
John K. Sorensen
President & CEO
Iowa Bankers Association, Johnston

EDITORS
Ronette Schlatter, CRCM
Senior Compliance Analyst III

Julie Gliha, MBA, CRCM
Vice President, Compliance

IBA OFFICERS

Call our hotline 844-734-7411

or email us at

compliance@iowabankers.com

The Disclosure is an official monthly publication of the Iowa Bankers Association, 8800 NW 62nd Avenue, PO Box 6200, Johnston, Iowa, 50131-6200; (515) 286-4300, (800) 532-1423, fax (515) 280-4140. News items are invited. The editor reserves the right to revise or refuse any editorial copy deemed to be unsuitable for publication.

The Disclosure may contain summaries and analyses of state and federal laws and banking regulations. Every effort is made to accurately summarize and analyze these laws and regulations, however, transactions should not be undertaken on the basis of this information alone. Bankers planning transactions which will be affected by any of the laws analyzed or summarized herein should seek advice of experienced bank counsel and/or state and federal bank regulators.

Subscriptions: IBA members can subscribe to an electronic subscription, at no charge, via password at *www.iowabankers.com/aspx/iba/publications.aspx?snid=14*. The non-member subscription rate is $380 per year. All prices include applicable state and local taxes.

For information about your subscription or to order, write to Iowa Bankers Association, **The Disclosure** Subscriptions, PO Box 6200, Johnston, Iowa, 50131-6200 or call (515) 286-4300 or (800) 532-1423, or fax (515) 280-4140.

For an archive of past Disclosure's, visit the IBA website at **www.iowabankers.com**

Volume 38, Issue 7 | JULY 2021

DISCLOSURE

A MONTHLY COMPLIANCE REVIEW PUBLISHED BY THE IOWA BANKERS ASSOCIATION

HIGHLIGHTS

FEATURE

REGULATORY UPDATE

NOTES OF INTEREST

COMPLIANCE FORUM

HMDA 2022: REPORTING OPEN-END LINES OF CREDIT

Jan. 1, 2022 marks a significant day for HMDA reporters. Effective Jan. 1, 2022, when the temporary threshold of 500 open-end lines of credit expires, the 2020 final HMDA rule becomes effective and sets the permanent HMDA reporting threshold for open-end lines of credit at 200. The result: more financial institutions will have to begin collecting data and reporting that data for dwelling-secured, open-end lines of credit on their LAR (Loan Application Register).

BACKGROUND

HMDA requires certain institutions to collect, record, and report specified information about their mortgage lending activity. In the 2015 HMDA Rule, the Consumer Financial Protection Bureau established institutional and transactional coverage thresholds in Regulation C that determine whether financial institutions are required to collect, record, and report HMDA data on closed-end mortgage loans or open-end lines of credit. The 2015 HMDA Rule set the closed-end threshold at 25 closed-end mortgage loans in each of the two preceding calendar years, and the open-end threshold at 100 open-end lines of credit in each of the two preceding calendar years. In 2017, the CFPB temporarily increased the open-end threshold to 500 open-end lines of credit for two years (calendar years 2018 and 2019) and then later in 2019, extended the temporary threshold of 500 open-end lines of credit to Dec. 31, 2021.

In early 2020, the CFPB issued yet another final rule impacting HMDA reporting. That rule increased the closed-end threshold to 100 effective July 1, 2020 – welcome news for many low volume HMDA reporters. However, the same final rule included some unwelcome news for many financial institutions: it lowered the 500 open-end line of credit threshold to 200 effective Jan. 1, 2022.

OPEN-END REPORTING

So what does the 200 threshold mean? Beginning in calendar year 2022, federally-regulated financial institutions that meet Regulation C's institutional coverage criteria[1] *and* originated at least 200 open-end lines of credit in each of the two preceding calendar years, must collect, record, and report data on on dwelling-secured open-end lines of credit on their LAR. That data must be reported by March 1 of the following calendar year. As a result, institutions that originated at least 200 open-end lines of credit in both 2020 and 2021 will need to begin collecting and reporting data for open-end applications in which final action is taken on or after Jan. 1, 2022.

COUNTING YOUR OPEN-END LINES

In order to make a determination as to whether or not you must begin reporting dwelling-secured, open-end lines of credit, institutions will have to "look back" to their previous two calendar years mortgage lending activity and count the number of originated dwelling-secured, open-end lines of credit. Regulation C indicates only originated, *reportable* open-end lines of credit should be included in the count. Thus, a quick recap of what is reportable under the open-end rules is warranted.

Open-End vs. Closed-End

First and foremost, to be reportable, the transaction must be dwelling-secured, and open-end credit. Regulation C does not define "open-end credit" but refers back to Regulation Z's definition. Regulation Z defines "open-end credit" as "consumer credit extended by a creditor under a plan in which: (i) The creditor reasonably contemplates repeated transactions; (ii) The creditor may impose a finance charge from time to time on an outstanding unpaid balance; and (iii) The amount of credit that may be extended to the consumer

during the term of the plan (up to any limit set by the creditor) is generally made available to the extent that any outstanding balance is repaid."

Institutions often error and include multiple advance closed-end loans in their calculation. It is that last component of the definition of "open-end credit" – "credit being made available to the consumer when the outstanding balance is repaid" – that differentiates open-end and a multiple advance, closed-end credit transaction. Multiple advance closed-end loans, such as construction loans or some home improvement loans, in which advances can be made up to a maximum credit limit, should not be included in the count if the loan terms prohibit the consumer from paying down the balance and taking new advances to the extent the amount that has been paid down.

Consumer-Purpose Lines of Credit

Nearly, but not all, consumer purpose, dwelling-secured open-end lines should be included in the count as nearly all consumer-purpose, open-end lines are reportable. Loan purpose does not factor into whether or not a consumer-purpose open-end line is reportable. As a result, dwelling-secured, open-end lines used for home purchase, refinance, home improvement or any other consumer purpose are reportable and should be included in an institution's count. However, Regulation C provides a few exemptions from HMDA reporting including temporary financing,[2] credit transactions in an amount of $500 or less, or an open-end line of credit used primarily for agricultural purpose or secured by a dwelling that is located on real property used primarily for ag purpose. A consumer purpose open-end line that meets one of these exemptions should not be counted.

Business-Purpose Lines of Credit

Business-purpose lines of credit, on the other hand, are only reportable if the open-end line is used for the purpose of home purchase,[3] improving a home[4] or is a refinancing.[5] And here again the exemptions outlined above apply to open-end lines of credit. So for example, if the purpose of the loan is to refinance ag credit, or is secured by a dwelling a located on ag land, the line of credit is not reportable and should NOT be included in the institution's count.

Documenting the Count

It will be important for institutions to establish a process for identifying and counting their reportable, open-end lines of credit. The process is important because the annual count is not a "one and done" process. Each year going forward, institutions that hover around the 200 threshold will have to identify, track and count their reportable open-end lines of credit to determine if they must start or continue to report open-end lines. Just as important will be the documentation of the count, especially for those institutions just above or below the 200 open-end threshold. Since the reporting threshold is new, it's likely to be a focal point of HMDA compliance exams until regulators are confident HMDA reporters have a good understanding of the requirement and a compliance management program is in place to meet the regulatory requirement.

START PREPARING NOW

Institutions that are currently closed-end HMDA reporters may be lulled into complacency by the fact they have strong, closed-end reporting systems in place. After all, how much harder can it be to report open-end lines of credit? In a word, PLENTY! The reason? Actually, there are two reasons: systems and staff. Consumer purpose, open-end lines of credit are often created from different loan platforms than closed-end mortgage loans. Most HMDA support and software interfaces are built into closed-end consumer credit loan platforms but are often lacking in open-end systems, or are an additional add-on product. Loan platforms for business-purpose lines of credit have even fewer HMDA supports in place. Application processes will need to be enhanced to ensure demographic information and other HMDA data is collected at the time of application. Many institutions don't have application processes for business purpose lines of credit. As a result,

application process for covered business-purpose lines will need to be developed and implemented. It's also going to be a huge adjustment for staff who have been told for the last five-plus years to not report open-end lines of credit. Additional processes and training will be needed. Tools and compliance guides will need to be revamped to assist staff in identifying reportable open-end lines. Enhanced monitoring will be required at least initially. Audit programs will need to be adjusted. The list goes on and on.

Jan. 1 is six months away so institutions may not feel a sense of urgency in making a determination if it will have to start reporting its open-end line of credit. However, keep in mind applications are reportable in the year in which final action is taken. Thus, applications received in late third quarter and fourth quarter 2021 could be reportable in 2022 if they don't close until after Jan. 1, 2022, meaning the bank will be required to collect HMDA data for these applications even earlier. So the clock is ticking to conduct your open-end counts for 2020 and 2021 to determine if you must begin collection and reporting in 2022.

Footnotes:

[1]Regulation C's institutional coverage criteria includes all of the following: Has a branch or home office in a MSA, assets in excess of the designated regulatory threshold ($48 million for 2021), and originated at least one home purchase loan secured by a first lien on a dwelling in the preceding year.

[2]A line of credit is designed to be replaced by separate permanent financing extended by any financial institution to the same borrower at a later time. See § 1003.3(c)(3)

[3]A loan or line of credit, used in whole or part, for the purpose of purchasing a dwelling.

[4]A loan or an open-end line of credit that is for the purpose, in whole or in part, of repairing, rehabilitating, remodeling, or improving a dwelling or the real property on which the dwelling is located.

[5]A loan or an open-end line of credit in which a new, dwelling-secured debt obligation satisfies and replaces an existing, dwelling-secured debt obligation by the same borrower.

FEATURE

CYBERATTACKS THE RISK IS REAL

Cyberattacks are getting to be a daily occurrence. It seems each newscast has at least one story about a hacker successfully disrupting a business operation and holding it for ransom or a data breach of consumer information at a popular retail outlet. No one is immune from cyber threats — consumers, businesses — large and small, charitable organizations. Even government entities can fall prey to cyber criminals. The risk is real and seems to increase exponentially daily. Even the White House is warning corporate executives and business leaders to step up security measures after intrusions disrupted operations at a major meatpacking company and the largest U.S fuel pipeline.

INCREASED EXPECTATIONS

The federal banking regulators recognize the increased risk as well and appear to be poised to increase their regulatory expectations related to an institution's data security program. In December of 2020, the Office of the Comptroller of the Currency, Federal Reserve and Federal Deposit Insurance Corporation jointly **announced** a **proposed rule** that would require financial institutions to notify their regulators within 36 hours of a "computer-security incident" that rises to the level of a "notification incident." The proposed rule would also affect companies that provide certain services to financial institutions, including data processing. Those service providers would be required to notify at least two individuals at affected financial institution immediately after the financial institution service provider experiences a computer-security incident that it believes in good faith could disrupt, degrade, or impair services provided for four or more hours.

The proposed rule recommends adding a definition of "computer security incident" to each agency's regulations. The definition would not be limited to unauthorized access to customer personal information. Under the proposal, not all "computer security incidents" require notification to financial institution regulators. The term "notification incident" would mean that a financial institution believes in good faith a "computer security incident" could materially disrupt, degrade, or impair:

- The ability of the financial institution to carry banking operations, activities, or processes, or deliver banking products and services to a material portion of its customer base, in the ordinary course of business;
- Any business line of a financial institution, including associated operations, services, functions and support, and would result in a material loss of revenue, profit or franchise value; or
- Those operations of a financial institution, including associated services, functions and support, as applicable, the failure or discontinuance of which would pose a threat to the financial stability of the United States.

The proposed regulation specifically includes as an example of a notification incident a "ransom malware attack that encrypts a core banking system or backup data." Service providers would be required to notify two individuals at each affected financial institution.

At the time of this article's publication, this rule has not been finalized.[1] However, there is existing guidance and rules for financial institutions related to information and data security. Originally issued in 2001, and last updated in 2014, the **Interagency Guidelines** Establishing Information Security Standards requires each financial institution to develop and

FEATURE

maintain an effective information security program tailored to the complexity of its operations, and to require, by contract, service providers that have access to its customer information to take appropriate steps to protect the security and confidentiality of this information. Issued in March 2005, the **Interagency Guidance** on Response Programs for Unauthorized Access to Customer Information and Customer Notice requires financial institutions to establish a security breach response program and, in general, to notify affected customers when a breach occurs. In addition, financial institutions are responsible for ensuring that third party service providers take appropriate measures designed to meet the objectives of the guidelines and comply with Section 501(b) of GLBA.

Given the increased incidents and risks posed by frequent hacker attempts, coupled with the possibility of increased regulatory requirements, financial institutions may be well advised to reassess the effectiveness of their information security program.

BACK TO THE BASICS

To evaluate the effectiveness of an existing information security program, institutions will likely need to review their risk assessment. According to the Interagency Guidelines Establishing Information Security Standards,[2] a risk assessment must include the following four steps:

- Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems;
- Assess the likelihood and potential damage of identified threats, taking into consideration the sensitivity of the customer information;
- Assess the sufficiency of the policies, procedures, customer information systems, and other arrangements in place to control the identified risks; and
- Apply each of the foregoing steps in connection with the disposal of customer information.

Threats continue to evolve, both internally and externally. As a result, the risk assessment process needs to be an ongoing activity. Financial institutions need to be cognizant of emerging risks and continually review their current policies and procedures to make certain they have adequate controls in place to safeguard customer information and other information systems. Institutions must also update the risk assessment, as necessary, to account for system changes before they are implemented or new products or services before they are offered.

In addition to identifying reasonably foreseeable threats, a risk assessment must evaluate the potential damage from these threats and the sufficiency of policies and procedures to identify and mitigate the threats. The evaluation process includes identifying weaknesses or other deficiencies in existing security controls and assessing the extent to which customer information and other information systems are at risk as a result of those weaknesses.

Finally, a financial institution should adjust its information security program to reflect the results of its ongoing risk assessment and the key controls necessary to safeguard customer information as well as other data and systems. The adjustments should take into account changes in technology, the sensitivity of its customer information, internal or external threats to information, and the institution's own changing business arrangement such as mergers, acquisitions, alliances and joint ventures, outsourcing arrangements, and changes in customer information systems.

EMERGING RISKS

According to a recent survey of financial institutions conducted by CSI[3] and detailed in a March 2021 blog,[4] the overwhelming majority (81%) of respondents view social engineering, either in general or in specific forms, as the greatest cybersecurity threat in 2021:

- **Customer-targeted phishing:** The topmost cybersecurity threat identified by financial institutions was social engineering aimed at customers via phishing (34%). In "phishing" attempts an attacker sends a fraudulent ("spoofed") message to an individual designed to trick the individual into revealing sensitive information to the attacker

or to deploy malicious software on the victim's infrastructure like ransomware by tricking the individual to click on a link or open an attachment. This coincides with recent reports of large-scale email impersonation attacks, including those that target employees of large corporations pretending to be from the recipient's personal financial institution and trying to trick them into providing sensitive information about their accounts.

- **Employee-targeted phishing:** Almost as many institutions (32%) are most worried about phishing aimed at internal targets that let attackers into internal systems. This concern is well founded. Employees working from home and burdened by new financial and family challenges due to the pandemic are ripe targets for cybercriminals.
- **Social engineering:** Rounding out the top three cybersecurity threats at 14% was social engineering in all its forms, which includes baiting, phishing, vishing, spear phishing, tailgating and contact spamming.

CSI suggests emerging cyber threats include:

- **Supply Chain Attacks:** This attack occurs when a bad actor targets a software or hardware vendor to deliver malicious code through seemingly legitimate products or updates. The recent **SolarWinds breach** is an example of a supply chain attack, which is becoming an increasingly popular method to distribute malware.
- **Virtual Private Network (VPN) Attacks:** As remote work becomes the norm for many organizations, cybercriminals will likely continue VPN attacks in attempt to gain access to corporate networks and data. Many home networks do not have proper passwords setup or lack proper security protocols, presenting vulnerabilities for criminals to target.
- **Cloud-Based Attacks:** Many organizations are migrating more of their infrastructure to the cloud, prompting cybercriminals to shift more of their efforts to cloud-based attacks. Institutions must ensure their cloud infrastructure is securely configured to prevent harmful breaches.

STRENGTHENING CYBERSECURITY EFFORTS

The same CSI survey[5] also asked participating financial institutions what tactics they planned to use in 2021 to strengthen their cybersecurity efforts. Over 85% of institutions plan to conduct some form of cybersecurity training. The vast majority of them (62%) plan to educate both employees and customers. A smaller group (23%) plans to focus on internal training among employees and board members. Proactive measures, such as penetration testing, conducting routine social engineering exercises, recurring vulnerability scans and cyber security audits were frequently noted as planned events for 2021 as well.

A June 2021 article[6] in Bank Business News details additional steps financial institutions can take to assess and mitigate data security risks. Several of the steps relate to reviewing and updating the institution's risk assessment and controls as discussed earlier, as well as enhanced training for both employees and customers. Additional steps suggested by the author of this article include:

- **Review user access.** It is important to understand how and where employees access data. Do they perform all work onsite? Do some employees access your network remotely? Do they use individual computers and other devices to perform some of their work? Are they transporting laptops to and from a branch to a home office? Knowing the answers to these questions will establish whether employees are accessing sensitive information in a secure environment. This knowledge can also help prevent data breaches arising from lost or stolen devices. When reviewing access privileges, make sure you have a complete list of all users for every system that stores or transmits customer data. Suspend or terminate any inactive accounts and evaluate whether each user requires their existing level of access to perform their assigned duties. A best practice is to limit access privileges to the minimum

necessary to perform assigned job duties using the least amount of privilege.

- **Audit third-party service providers.** Institutions that employ third-party service providers for document processing, billing, and distribution, should audit their security program as thoroughly as its own. One of the best ways to validate a third-party service provider's security program is to check whether they hold an industry-recognized certification or attestation.
- **Implement multiple levels of security.** If your risk assessment identified any gaps in your facility security, access controls, or technical safeguards, now is the time to correct any oversights.
- **Establish secure methods of data disposal.** Evaluate the methods in place at your institution for disposing of redundant and obsolete data that may contain sensitive data. Digitally overwriting electronic data and shredding hard copy records are best practices that will protect sensitive financial information.

The White House is also urging businesses to take a more proactive stance in protecting their systems. In a June 3 memo issued by Ann Neuberger, the deputy national security advisor for cyber and emerging technology, urges corporate executives to adopt the best practices President Biden laid out in an executive order[7] signed in May aimed at addressing the country's vulnerability to cyberattacks, such as multifactor authentication and encryption. Neuberger also urged companies to backup data and keep back-ups offline so that they are not vulnerable to ransomware variants; to update and patch systems regularly; and to build and test an incident response plan so that businesses can sustain operations in the event of an attack.

PLAN AHEAD

It is critical to have a plan in place for responding to security incidents, data breaches and other emergencies. Incident response plans should include an identified chain of command and contact information for team members. Also include procedures for responding to data breaches and notifying regulatory agencies, law enforcement, and customers. If a natural disaster or cybersecurity incident occurs, institutions also need to restore the integrity and availability of any lost or damaged data. Comprehensive disaster recovery and business continuity plans detail procedures for restoring access to the network, data and facilities. Testing the disaster recovery plan at least annually to ensure team members understand their role and how to respond to different scenarios is also crucial.

When information security is compromised, the consequences can be dire. Possible consequences include reputation risk, loss of customer confidence in your institution, financial losses, regulatory scrutiny, etc. Re-evaluating your risk assessment and mitigating identified vulnerabilities can help prevent an incident from becoming a compliance nightmare.

Footnotes:

[1]While the comment period has closed, the IBA participated in the American Bankers Association's comment letter submission on the proposal. The ABA comment letter can be found **here** and the joint trade letter can be found **here**.

[2]**https://www.federalreserve.gov/supervisionreg/interagencyguidelines.htm**

[3]CSI is a national provider of fintech and regtech solutions. **www.csiweb.com**

[4]**https://www.csiweb.com/what-to-know/content-hub/blog/banks-brace-for-cybersecurity-threats-in-2021**

[5]Detailed in CSI's 2021 Banking Priorities Executive report, found at **https://www.csiweb.com/2021-banking-priorities-executive-report**

[6]**https://www.bankbusiness.us/10-steps-retail-banks-can-take-to-assess-and-mitigate-data-security-risk**

[7]**https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity**

REGULATORY UPDATE

NEW FEDERAL HOLIDAY: JUNETEENTH NATIONAL INDEPENDENCE DAY

On June 17, 2021, President Joe Biden signed into law S.475 — known as the Juneteenth National Independence Act — making June 19 a federal holiday. This act amended section 6103(a) of title 5 USC adding Juneteenth as the newest federal holiday since Martin Luther King Day. This is significant for financial institutions because several compliance regulations contain timing provisions which prohibit federal holidays from being counted as a "business day."

Because of the short two-day notice of an additional federal holiday, and lack of regulatory guidance, creditors were left to make risk-based decisions on how to handle pending loan closings that included Saturday, June 19 in their rescission period or three-day waiting period between delivery of the Closing Disclosure and consummation. To date, the Consumer Financial Protection Bureau has not issued formal guidance but instead released a statement stating "the CFPB recognizes that some lenders did not have sufficient time after the Federal holiday declaration to consider whether and how to adjust closing timeline." The same statement implied the CFPB may be coordinating with other regulatory agencies in providing further guidance, "Any guidance ultimately issued by the CFPB would take into account the limited implementation period before the holiday and would be issued after consultation with the other FIRREA regulators and the Conference of State Bank Supervisors to ensure consistency of interpretation for all regulated entities." At the time of this publication, the CFPB has not issued further guidance.

CFPB ISSUES CORRECTION TO NEW HPML ESCROW EXEMPTION

The Consumer Financial Protection Bureau issued a notice in the **June 3, 2021 Federal Register** adding a comment to its Official Staff Commentary that it included in a recent higher-priced mortgage loan escrow exemption final rule but that was not incorporated into the Code of Federal Regulations due to an omission in an amendatory instruction. The CFPB is also revising a comment that it included in the same recent final rule, but that inadvertently did not appear in a subsequently effective final rule.

Specifically, the following comment was added to the CFR, explaining the threshold differences in the new HPML escrow exemption and the existing "small creditor" exemption:

Paragraph 35(b)(2)(vi)(B).

1. The transaction threshold in § 1026.35(b)(2)(vi)(B) differs from the transaction threshold in § 1026.35(b)(2)(iii)(B) in two ways. First, the threshold in § 1026.35(b)(2)(vi)(B) is 1,000 loans secured by first liens on a principal dwelling, while the threshold in § 1026.35(b)(2)(iii)(B) is 2,000 loans secured by first liens on a dwelling. Second, all loans made by the creditor and its affiliates secured by a first lien on a principal dwelling count toward the 1,000-loan threshold in § 1026.35(b)(2)(vi)(B), whether or not such loans are held in portfolio. By contrast, under § 1026.35(b)(2)(iii)(B), only loans secured by first liens on a dwelling that were sold, assigned, or otherwise transferred to another person, or that were subject at the time of consummation to a commitment to be acquired by another person, are counted toward the 2,000-loan threshold.

RESPA ESCROW FAQ

The Consumer Financial Protection Bureau released a set of 23 frequently asked questions that provide an overview of the escrow account provisions under Regulation X. The FAQs address a variety of topics including key definitions, account analysis, deficiencies, shortages, surpluses, HUD's public guidance documents and more. **Read the FAQs.**

REGULATORY UPDATE

BSA/AML EXAM UPDATES

The Federal Financial Institutions Examination Council released updates to four sections of the Bank Secrecy Act/ Anti-Money Laundering Examination Manual, including:

- **International Transportation of Currency or Monetary Instruments Reporting** (PDF)
- **Purchase and Sale of Monetary Instruments Recordkeeping** (PDF)
- **Reports of Foreign Financial** (PDF)
- **Special Measures** (PDF)

The updates should not be interpreted as new instructions or increased focus on certain areas; instead, they offer further transparency into the examination process and support risk-focused examination work. The manual provides instructions to examiners for assessing the adequacy of a bank's BSA/AML compliance program and its compliance with BSA regulatory requirements.

NEW REG. E FAQ

The Consumer Financial Protection Bureau released a set of frequently asked questions that address the unauthorized transfer and error resolution provisions under the Electronic Fund Transfer Act and Regulation E. The FAQs also address situations when a consumer is fraudulently induced by a third party to provide their account information or private network rules conflict with the regulation. **Read the FAQs.**

CRA WEBSITE UPDATE

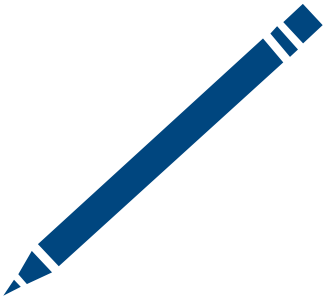
The FFIEC has updated its CRA website by adding the 2021 Distressed or Underserved Nonmetropolitan Middle-income Geographies list. These are geographic areas where revitalization or stabilization activities are eligible to receive Community Reinvestment Act consideration under the community development definition.

The CRA applies a one-year lag period for geographies that were listed in 2020 but are no longer designated as distressed or underserved in the current release. Revitalization or stabilization activities in these geographies are eligible to receive CRA consideration under the community development definition for 12 months after publication of the current list. The current and previous years' lists can be found **here**.

CFPB TO RESUME MLA EXAMS

The Consumer Financial Protection Bureau issued an **interpretive rule** that explains the basis for its authority to examine supervised financial institutions for risks to active duty servicemembers and their dependents (i.e. military borrowers) from conduct that violates the Military Lending Act (MLA). As a bit of history, in September 2013, the CFPB amended its supervisory procedures so that examiners could review lenders' records regarding MLA violations. From that time until 2018, no companies disputed the CFPB's authority to review their MLA lending practices. In 2018, the CFPB's leadership discontinued MLA-related examination activities, based on its stated belief that Congress did not specifically confer examination authority on the CFPB with respect to the MLA. The current CFPB leadership does not find those prior beliefs persuasive and the CFPB will now resume MLA-related examination activities.

NOTES OF INTEREST



REVISED IRA DISTRIBUTION FORM

The IRS has issued a revised **2020 Publication 590-B**, *Distributions from Individual Retirement Arrangements* (IRAs), intended to clarify the application of required minimum distribution rules under the Setting Every Community Up for Retirement Enhancement Act.

The explanation of the 10-year rule has been expanded to indicate that, if applicable, the entire balance of the IRA must be withdrawn by Dec. 31 of the year containing the 10th anniversary of the owner's death, and the beneficiary is allowed, but not required, to take a distribution before that date. The publication notes that the 10-year rule applies if:

- The beneficiary is an eligible designated beneficiary who elects the 10-year rule if the owner died before reaching his required beginning date, or
- The beneficiary is a designated beneficiary who is not an eligible designated beneficiary, regardless of whether the owner died before reaching his required beginning date.

CHILD TAX CREDIT PAYMENTS START JULY 15

Financial institutions will start seeing additional payments to nearly 36 million families starting July 15. The American Rescue Plan raised the maximum Child Tax Credit in 2021 to $3,600 for qualifying children under the age of 6 and to $3,000 per child for qualifying children between ages 6 and 17. Eligible families will begin receiving advance payments, either by direct deposit or check. The IRS will issue advance Child Tax Credit payments on July 15, Aug. 13, Sept. 15, Oct. 15, Nov. 15 and Dec. 15.

Payments sent via ACH will likely use a one-day settlement process. The files received before 5 p.m. on the day before settlement must be made available to consumers by 9 a.m. on the settlement date. The entries will include the Company Name "IRS TREAS 310" and the Company Entry Description "CHILDCTC."

A few reminders:

- Payments sent to closed accounts should be returned using code R02;
- Bank is only required to validate the account number in the ACH file matches the account number on record. Under Nacha rules, banks are not required to validate the Receiver name matches the accountholder name;
- Since these are tax credits, they are not subject to reclamation.

The IRS has created a special Advance Child Tax Credit 2021 page at **IRS.gov/childtaxcredit2021**, designed to provide the most up-to-date information about the credit and the advance payments. The page also features other useful new online tools, including an interactive Child Tax Credit eligibility tool to help families determine whether they qualify for the advance Child Tax Credit payments. For more information on the Child Tax Credit payments, see IRS release **IR-2021-124**.

DOJ CONTACT FOR REPORTING UNEMPLOYMENT FRAUD FUNDS

The Department of Justice Unemployment Insurance Fraud Task Force has announced a new contact method for financial institutions to use if they suspect that frozen funds are proceeds from unemployment insurance fraud. Financial institutions can email **uifraud@oig.dol.gov** if they have frozen funds thought to be from unemployment fraud that cannot be returned to the defrauded state workforce agencies through ACH reversal or other return processes. Financial institutions should include in the email, the name, phone number and email address of the employee that law enforcement can contact for more information.

NOTES OF INTEREST

ADDITIONAL 2020 HMDA DATA

The Federal Financial Institutions Examination Council has made available additional data on 2020 mortgage lending transactions at 4,475 U.S. financial institutions reported under the Home Mortgage Disclosure Act. The HMDA **Dynamic National Loan-Level Dataset** is updated on a weekly basis to reflect late submissions and resubmissions.

The **Aggregate and Disclosure Reports** provide summary information on individual financial institutions and geographies. The **HMDA Data Browser** allows users to create custom tables and download datasets that can be further analyzed.

EMPLOYER VACCINATION GUIDANCE

The Equal Employment Opportunity Commission updated its coronavirus-related question-and-answer document with 21 new or modified Q&A related to employer vaccination policies. The full text of the EEOC guidance can be found **here**. Key points included in the Q&A:

- Under the ADA, an employer may offer an incentive to employees to voluntarily provide documentation or other confirmation that they received a vaccination on their own (Q&A K.16).
- An employer also may offer an incentive to employees for voluntarily receiving a vaccination administered by the employer or its agent if the incentive "is not so substantial as to be coercive." The EEOC explained that "because vaccinations require employees to answer pre-vaccination disability-related screening questions, a very large incentive could make employees feel pressured to disclose protected medical information" to their employer (Q&A K.17).
- Under the ADA, it is not a "disability-related inquiry" for an employer to inquire about or request documentation or other confirmation that an employee obtained the COVID-19 vaccine (Q&A K.9). (For background, the ADA permits a "disability-related inquiry" only if the employer demonstrates the inquiry is job-related and consistent with business necessity.)
- Information about an employee's COVID-19 vaccination is confidential medical information under the ADA and therefore must be kept confidential and stored separately from the employee's personnel files (Q&A K.4 & K.9).
- The EEOC affirmed that an employer may require all employees physically entering the workplace to be vaccinated for COVID-19, subject to the reasonable accommodation provisions of Title VII and the ADA (Q&A K.1). If an employee cannot receive the vaccine because of a disability, "the employer may not require compliance for that employee unless it can demonstrate that the individual would pose a 'direct threat' to the health or safety of the employee or others in the workplace." If the employer determines that the individual would pose a direct threat, the employer must assess whether a reasonable accommodation would reduce or eliminate the threat. (Q&A K.5 & K.6.)
- Similarly, the EEOC affirmed that, if an employee's sincerely held religious belief, practice or observance prevents the employee from obtaining a COVID-19 vaccine, the employer must provide a reasonable accommodation unless it would pose an undue hardship (Q&A K.12). The EEOC provided examples of reasonable accommodations that may be offered to employees who do not get vaccinated due to a disability or sincerely held religious belief: a requirement to wear a face mask, work at a social distance from coworkers or non-employees, work a modified shift, get periodic tests for COVID-19, be given the opportunity to telework, or accept a reassignment (Q&A K.2).

COMPLIANCE FORUM

The Compliance Forum is not intended to be a definitive analysis of the subjects discussed or a substitute for personal legal advice.

Q. Our bank has an application for a TRID covered loan that will be secured by multiple properties. What property costs should be included in the "estimated taxes, insurance and assessments" section on page one of the Loan Estimate and Closing Disclosure? Only the property costs for the primary property or the property costs for ALL of the collateral properties?

A. The "estimated taxes, insurance and assessments" on both the Loan Estimate and Closing Disclosure should include all property costs for ALL real property that will secure the loan. Property costs include items such as hazard insurance, flood insurance, taxes, homeowners association and condominium fees, ground rent, and leasehold payments.

Q. If multiple properties will secure a TRID loan, but the bank is only escrowing for the taxes and insurance of one of the properties, how should the "In escrow?" field be completed in the "Estimated Taxes, Insurance & Assessments" section on page one of the TRID disclosures?

A. If the bank is escrowing for only portion of the property costs when there are multiple properties securing the loan, the "In escrow?" field may indicate "some" instead of "yes" per the commentary to 1026.37(c)(4)(iv) - #2:

> *2. Amounts paid by the creditor using escrow account funds. Section 1026.37(c)(4)(iv) requires the creditor to disclose an indication of whether the amounts disclosed under § 1026.37(c)(4)(ii) will be paid by the creditor using escrow account funds. If only a portion of the amounts disclosed under § 1026.37(c)(4)(ii), including, without limitation, property taxes, homeowner's insurance, and assessments, will be paid by the creditor using escrow account funds, the creditor may indicate that only a portion of the amounts disclosed will be paid using escrow account funds, such as by using the word "some."*

Q. If we do an annual escrow analysis for a borrower and that account has a shortage equal to or more than one month's escrow account payment, we understand our options in Reg. X are to allow the shortage to exist and do nothing or require the borrower to repay the shortage in equal monthly payments over a 12-month period. But may we accept a lump sum payment if the borrower wishes to cover the shortage at the time of the annual analysis instead of paying over a 12-month period? Also, can we communicate to the borrower paying the shortage in a lump sum is an additional, voluntary option?

A. Yes, if there is a shortage that is equal to or more than one month's escrow account payment, the servicer may accept an **unsolicited** lump sum payment to resolve the shortage. However, the servicer cannot require or provide the option of a lump sum payment on the annual escrow account statement. The annual escrow statement, which reflects the escrow account analysis, may only indicate that a shortage can exist or that the borrower can repay the shortage in equal monthly payments over at least a 12-month period.

The servicer may communicate to the borrower paying the shortage in a lump sum is an option, provided that the communication is not in the annual escrow account statement itself and does not appear to indicate that a lump sum payment is something that the servicer requires but rather is an entirely voluntary option. Regulation X does not prohibit a servicer from including other statements or materials in the same envelope as the annual escrow statement or in an entirely separate communication that provides general information regarding the operation of a borrower's escrow account or additional guidance on ways in which a borrower may manage or make voluntary payments into their escrow account.

Q. Our borrower has a mortgage loan secured by their principal dwelling that had an original loan balance of $200,000, secured by a $200,000 open-end mortgage. The borrower has paid down the loan balance to $120,000. They are now requesting a new loan to refinance the balance of this existing loan and with cash out funds up to the original $200,000 loan balance, still secured by our existing open-end mortgage for $200,000. Regulation Z has an exemption from rescission for closed-end loans if no new money is advanced.

Since the new loan amount is the same as the original loan amount, and we are using our existing open-end mortgage as collateral, does rescission apply?

A. Yes, the loan is rescindable. Rescission applies to this loan because the "no new money exemption" you reference in the closed-end credit rules compares the new loan amount to the unpaid balance and earned unpaid finance charge of the existing loan being refinanced. The difference between the new loan amount and the unpaid principal and interest of the existing loan is subject to rescission. Loan costs attributed to the new loan are not included in the rescindable amount. The exemption found in §1026.23(f)(2) states the following: … *The right of rescission shall apply, however, to the extent the new amount financed exceeds the unpaid principal balance (emphasis added), any earned unpaid finance charge on the existing debt, and amounts attributed solely to the costs of the refinancing or consolidation.* It is important to note, this "no new money exemption" only applies only to closed-end credit transactions. It cannot be used for open-end transactions.

An example may help illustrate: current loan balance is $120,000 with unpaid earned interest of $1,000 and $1,000 in loan costs attributed to the refinance. The new loan request amount is $200,000. The rescindable amount is calculated as follows:

New loan balance	$200,000
Minus loan costs	$1,000
Minus existing loan balance	$120,000
Minus earned interest	– $1,000
Rescindable amount	$78,000

Q. We currently allow our ACH Originators to opt-out of dual control when submitting ACH files (I.e. one employee generate the ACH file, a second employee confirm via e-mail, fax, or telephone call to the ODFI confirming the number and dollar amount of the file). Many of our Originators are small businesses with few employees and they don't always have two employees available to initiate and verify files. Is this an acceptable practice?

A. Dual control is a best practice but not a Nacha requirement. Dual control does reduce an institution's risk. A recent embezzlement case illustrates this risk: an Originating Depository Financial Institution (ODFI) allowed Originators to opt-out of dual control. One of the Originator's employees, who was an authorized user to initiate ACH files on behalf of the Originator, added an extra ACH entry to the ACH file to credit her account at another financial institution. The extra ACH entries occurred over a period of time. The amount of unauthorized entries totaled over $24,000 before the Originator discovered the fraud. From the ODFI's perspective, the employee was listed as an authorized user and had full authority to debit or credit accounts owned by the Originator; therefore, the loss rested with the Originator.

Not requiring dual control when Originators submit ACH files increases fraud risk. Some ODFI's allow Originators to opt-out of dual control by acknowledging (via signature) an opt-out section within the Originator/ODFI Agreement or by having the owner of the business or person in control of the business sign a separate dual control waiver. Dual control is certainly a best practice and is extremely effective in deterring fraud, but there may be circumstances where the practice is not feasible.