Volume 40, Issue 4 | APRIL 2023

DISCLOSURE

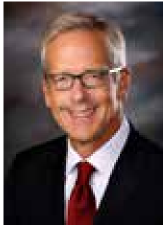
A MONTHLY COMPLIANCE REVIEW PUBLISHED BY THE IOWA BANKERS ASSOCIATION

Protect your customers by knowing how to spot red flags

ALSO IN THIS ISSUE:

A PRIMER ON FDIC INSURANCE

IOWA BANKERS ASSOCIATION

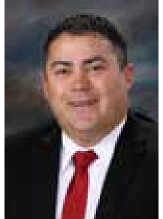


PUBLISHER
John K. Sorensen
President & CEO
Iowa Bankers Association, Johnston

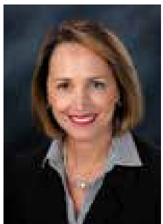
EDITORS
Ronette Schlatter, CRCM
Compliance Analyst III

Julie Gliha, MBA, CRCM
Vice President, Compliance

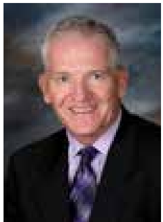
IBA OFFICERS



CHAIRMAN
Matt Lujano, President
Westside State Bank, Westside



CHAIRMAN-ELECT
Mary Kay Bates, President & CEO/CFO
Bank Midwest, Spirit Lake



TREASURER
Kim Greenland, Senior Vice President
City State Bank, Mount Ayr

PAST CHAIRMAN
Aaron Kness, President & CEO
Iowa State Bank & Trust, Fairfield

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, 8901 Northpark Drive, 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, by emailing editor@iowabankers.com. 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.

Copyright © 2023 Iowa Bankers Association

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

Volume 40, Issue 34 | APRIL 2023

DISCLOSURE

A MONTHLY COMPLIANCE REVIEW PUBLISHED BY THE IOWA BANKERS ASSOCIATION

HIGHLIGHTS

04 A PRIMER ON FDIC INSURANCE

COURT CASE EMPHASIZES IMPORTANCE OF CLEAR ACCOUNT DISCLOSURES

FEATURE

07 **CHECK FRAUD — IT'S IN THE MAIL**

In February, FinCEN issued an eight-page alert warning banks to be vigilant in identifying and reporting check fraud schemes related to U.S. mail theft. This article reviews the FinCEN red flags for mail theft-related check fraud as well as check fraud liability under the Uniform Commercial Code.

REGULATORY NEWS

11 IRS RELIEF FOR REPORTING 2023 RMDS

WARNING: LENDERS MAY BE LIABLE FOR DISCRIMINATORY APPRAISALS

FINCEN BOI REPORTING GUIDANCE

UPDATED CONTACT INFO ON CONSUMER DISCLOSURES

2022 BANK HMDA DATA AVAILABLE

HUD TO REINSTATE 2013 DISPARATE IMPACT RULE

CFPB SUPERVISORY HIGHLIGHTS FOCUSES ON FEES

COMPLIANCE FORUM

14 CRA PUBLIC FILE CONTENT REQUIREMENTS

PROVIDING CTR INFORMATION TO CUSTOMERS

CREDIT REPORTING AGENCY TRIGGER LEADS

REQUIRED DEPOSIT LOAN DISCLOSURE

CTR FILING ON DECEASED JOINT OWNER

A Primer on FDIC Insurance

Most customers don't give a second thought to FDIC deposit insurance ... until a bank fails. In early March, a run on deposits led to the closure of Silicon Valley Bank in California, making it the second-largest bank failure in U.S. history. Around the same time, Signature Bank in New York was closed by its state banking authority. These two recent events may have depositors — and perhaps some bank employees — thinking and asking questions about FDIC insurance.

It is important that consumers understand deposit insurance is one of the most significant benefits of having an account at an FDIC-insured bank, and bank employees are in the best position to communicate that message to consumers, instilling confidence in the U.S. banking system. The best source for information and resources related to deposit insurance is the FDIC. The FDIC has multiple resources for both consumers and banks on its **Deposit Insurance Resources webpage**.

DEPOSIT INSURANCE BASICS

FDIC deposit insurance protects bank customers in the unlikely event that an FDIC-insured depository institution fails. Bank customers don't need to purchase deposit insurance; it is automatic for any qualifying deposit account opened at an FDIC-insured bank. Depositors that qualify to receive FDIC deposit insurance coverage include natural persons, legal entities such as corporations, partnerships and unincorporated associations, and public units, such as cities and counties.

Deposits are insured up to $250,000 per depositor, per FDIC-insured bank, per ownership category. Deposits held in different ownership categories are separately insured, up to $250,000, even if held at the same bank. There are 14 FDIC deposit insurance categories with the most common categories including single accounts, joint accounts, revocable trust accounts, irrevocable trust accounts,[1] certain retirement accounts, employee benefit plan accounts, business/organization accounts, government accounts and more.[2]

All deposits owned by the same depositor (or depositors) in the same ownership category are added together for the purpose of calculating FDIC deposit insurance coverage. This aggregation is irrespective of whether the deposits are opened under the same product type (for example, all CDs) or a combination of different product types (for example, a CD and a savings account). In addition, the number of accounts a depositor establishes within an ownership category — three accounts owned under the single ownership category, for example — has no impact on the maximum amount of deposit insurance coverage provided. It is the total dollar amount of all deposit accounts within a specific ownership category that is considered when determining insurance coverage.

CALCULATING INSURANCE COVERAGE

To determine the amount of insurance coverage available, the following questions — at a minimum — should be answered:

1. **Who owns the deposits?** Identifying the particular individual, business or government entity that owns the deposits is an essential first step in analyzing the amount of deposit insurance coverage that may be available.
2. **What FDIC ownership category is the depositor attempting to qualify under?** Deposits made under each of the 14 FDIC ownership categories are insured separately provided the depositor meets the specific requirements for each of the ownership categories.
3. **Does the depositor meet all the requirements for coverage under the applicable ownership category?** Each ownership category has specific requirements that must be met to receive separate insurance coverage under that category. If an account fails to meet the requirements, the deposits will be insured in another ownership category (for an individual usually the single account category) and the deposits will be added together with any other funds that the depositor has in that same ownership category.

While frontline staff are essential in disseminating information about FDIC insurance, they should be cautious when providing an analysis of deposit insurance coverage amounts and advising depositors on how to restyle an account just to extend their FDIC insurance coverage as doing so could impact the

depositor's estate planning. Instead, the FDIC has a number of tools to assist depositors in determining if their deposits are fully insured, including:

- **Frequently Asked Questions About Deposit Insurance** — The FAQ reflects some of the most common questions about FDIC insurance.
- **Deposit Insurance Brochures and Videos** — The FDIC has videos and brochures — Deposit Insurance at a Glance and Your Insured Deposits[3] — that are available in English and Spanish to help consumers and employees understand how deposit insurance works, the accounts covered by deposit insurance and how to calculate insurance coverage.
- **The Electronic Deposit Insurance Estimator** (EDIE) — Allows consumers to calculate their coverage on a per-bank basis, determine how much is insured and what portion of their funds (if any) exceeds the coverage limits. Consumers can also learn how the insurance rules limits apply to specific deposit accounts. EDIE permits depositors to print a report of their calculations for their records.
- **FDIC Information and Support Center** — Should depositors have additional questions after reviewing the FDIC's online resources, they can call 1-877-ASK-FDIC or submit a question online.

IMPORTANCE OF ACCOUNT RECORDS

In the event of the failure of an insured bank, the FDIC relies upon deposit account records to determine the ownership of an account and the amount of deposit insurance coverage available to each depositor. The importance of clear account records that detail account owners by name, the ownership category, and the added requirements and information needed to satisfy separate insurance coverage under specific category cannot be overstated (such as beneficiaries on revocable trust account must be listed in bank records or all co-owners of a jointly owned account must personally sign the signature card[4]). Deposit account records include:

- Signature cards
- CDs and passbooks
- Account ledgers and computer records that relate to the insured bank's deposit-taking function
- Official items
- Corporate resolutions authorizing accounts in the possession of the insured bank
- Other books and records of the insured bank

The FDIC has also developed valuable information for bankers wanting to learn more about FDIC insurance, including:

- **Deposit Insurance Coverage Webinars for Bankers** — The FDIC offers a webinar series on FDIC insurance covering the fundamentals of deposit insurance, advanced insurance topics, and insurance coverage for specific products, like Revocable Trust Accounts. The FDIC expects information on the deposit insurance seminar series will be made available on the FDIC's homepage during the 2nd quarter of 2023.
- **Bank Employee's Guide to Deposit Insurance** —This comprehensive guide helps bank employees provide basic deposit insurance information, general principles of insurance coverage, and detailed information about each of the ownership categories addressing requirements for each ownership category, common misconceptions and questions, death of an account owner and additional deposit insurance coverage resources.

Utilizing the tools provided by the FDIC, bank staff can answer questions and provide depositors with the information needed to have confidence their deposits are safe and sound.

Footnotes:

[1]Effective April 1, 2024, revocable and irrevocable trust accounts will be combined into one ownership category for FDIC insurance purposes. To learn more about this upcoming change, see the FDIC's **Fact Sheet**, Final Rule on Simplification of Deposit Insurance Rules for Trust and Mortgage Servicing Accounts.

[2]See page 21 of the **FDIC Deposit Insurance Guide for Bankers** for a full listing of the deposit insurance ownership categories.

[3]Your Insured Deposits is also available in Simplified Chinese, Traditional Chinese, Korean, Tagalog, and Vietnamese.

[4]The FDIC waives the signature requirement in some cases. Negotiable instruments and CDs, for example, are exempt from the signature requirement.

HIGHLIGHTS

Court Case Emphasizes Importance of Clear and Accurate Disclosures

The Iowa Bankers Association was recently made aware of a 2021 lawsuit against an Iowa bank where a consumer asserted the bank breached their contract by charging overdraft fees for a debit card transaction that was authorized against the consumer's available balance but later settled against a balance insufficient to cover the item — referred to as Authorized Positive, Settle Negative (APSN).

While the parties agreed the bank contract allowed the bank to charge overdraft fees in general, they disagreed as to the timing of when an overdraft is determined. In general, the court ruled the bank clearly defined an "item" to include "all orders or instruction for payment, transfer or withdrawal or funds from your account; all deposits to your account, even if returned unpaid, any holds or restrictions we put on your account, and any other debits or credits to your account ..." allowing the bank to make an overdraft determination at the time the merchant seeks payment of funds on a transaction that has already been authorized.

The court determined the bank further clearly explained the process of authorizing transactions, the fact that other intervening transactions could post before the authorized transaction reducing the available balance, and that such transactions could result in an overdraft. Therefore, the court ruled the bank's disclosures clearly and unambiguously disclosed the overdraft determination will occur at a later point in time — meaning after the merchant submits the final request for payment. It is important to note the bank not only clearly disclosed this process at account opening but followed this process when processing such transactions.

The same consumer also claimed —among other things — a breach of contract when the bank, on two occasions, charged multiple fees when a merchant resubmitted a transaction that was previously rejected for insufficient funds. As with the situation above, the bank's account agreement explicitly authorized the bank to assess these representment fees.

Further, the account agreement clearly defined an "item" as stated above indicating each presentment may be subject to the NSF fee. Therefore, the court determined there was no breach of contract and the bank was not unjustly enriched. For the reason's stated in the court document, the court granted the dismissal of both counts.

This court case emphasizes the importance of clear and detailed disclosures and the importance of ensuring operational processes reflect the terms and conditions disclosed at account opening. It is important to note this court case may or may not impact a regulatory finding during an exam but may provide important precedence should a bank be subject to a similar legal challenge. **Read the court case.**

FEATURE

CHECK FRAUD — IT'S IN THE MAIL

Protect your customers by knowing how to spot red flags

On Feb. 27, FinCEN issued an **eight-page alert** warning banks to be vigilant in identifying and reporting check fraud schemes related to U.S. mail theft. Despite the declining use of checks in the U.S., it will come as no shock to most banks that check fraud is on the rise. What may be shocking, however, is the current conduit of choice for many criminals — check fraud resulting from mail theft through the U.S. Postal Service.

From March 2020 through February 2021, the U.S. Postal Inspection Service[1] received 299,020 mail theft complaints — an increase of 161% compared to the same period a year earlier. BSA reporting for check fraud has also increased in the past three years. In 2021, banks filed more than 350,000 SARs with FinCEN to report potential check fraud — a 23% increase over the number of check fraud-related SARs filed in 2020. This upward trend continued into 2022, when the number of SARs related to check fraud reached over 680,000, nearly double the previous year's amount of filings.

TYPOLOGIES OF MAIL THEFT-RELATED CHECK FRAUD

According to the FinCEN alert, criminals committing mail theft-related check fraud generally target the U.S. Mail in order to steal personal checks, business checks, tax refund checks, and checks related to government assistance programs, such as Social Security payments and unemployment benefits. Criminals will generally steal all types of checks in the U.S. Mail as part of a mail theft scheme, but business checks may be more valuable than personal checks because business accounts are often well-funded and it may take longer for the victim to notice the fraud.

The FinCEN alert indicates after stealing checks from the U.S. Mail, fraudsters and organized criminal groups may alter or "wash" the checks, replacing the payee information with their own or fraudulent identities or with business accounts that the criminals control. During check washing, these illicit actors also often increase the dollar amount on the check, sometimes by hundreds or thousands of dollars. Washed checks may also be copied, printed, and sold to third-party fraudsters on the dark web and encrypted social media platforms in exchange for convertible virtual currency.

In some cases, victim checks are also counterfeited using routing and account information from the original, stolen check. Criminals may cash or deposit checks in person at banks, make deposits through automated teller machines (ATMs), or via remote deposit into accounts they control. Frequently these accounts are opened specifically for the check fraud schemes. They may also rely on money mules and their pre-existing accounts to deposit fraudulent checks. Regardless, once the checks are deposited, the funds are typically rapidly withdrawn through ATMs or wired to other accounts the criminals control.

MAIL THEFT-RELATED CHECK FRAUD RED FLAGS

The alert outlined a number of "red flags" identified by USPIS, in coordination with FinCEN, to help banks detect, prevent, and report suspicious activity connected to mail theft-related check fraud. The alert warns, while no single

FEATURE

red flag is determinative of illicit or suspicious activity, banks should consider the surrounding facts and circumstances. For example, the bank should take into consideration the customer's historical financial activity, whether the transactions are in line with prevailing business practices, and whether the customer exhibits multiple red flags, before determining if a behavior or transaction is suspicious or otherwise indicative of mail theft-related check fraud. A few of the red flags outlined the alert include:

- Non-characteristic large withdrawals on a customer's account via check to a new payee.
- Customer complains of a check or checks stolen from the mail and then deposited into an unknown account.
- Customer complains that a check they mailed was never received by the intended recipient.
- Existing customer with no history of check deposits has new sudden check deposits and withdrawal or transfer of funds.
- Non-characteristic, sudden, abnormal deposit of checks, often electronically, followed by rapid withdrawal or transfer of funds.
- Examination of suspect check reveals faded handwriting underneath darker handwriting, giving the appearance that the original handwriting has been overwritten.
- New customer opens an account that is seemingly used only for the deposit of checks followed by frequent withdrawals and transfer of funds.

MAIL THEFT-RELATED CHECK FRAUD SAR GUIDANCE

A bank is required to file a SAR in the following circumstances:

- Insider abuse involving any amount;
- Transactions aggregating $5,000 or more where a suspect can be identified;
- Transactions aggregating $25,000 or more regardless of potential suspects; and
- Transactions aggregating $5,000 or more that involve potential money laundering or violations of the BSA.

While the dollar thresholds for filing may not always be met, banks are encouraged to file nonetheless in appropriate situations involving these matters, based on the potential harm that such crimes can produce. Even when the dollar thresholds of the regulations are not met, banks have the discretion to file a SAR and are protected by the safe harbor provided for in BSA.

When filing a SAR related to mail theft-related check fraud, FinCEN requests that banks indicate a connection between the suspicious activity being reported and the activities highlighted in Alert 2023-003 by including the key term "FIN-2023- MAILTHEFT" in SAR field 2 ("Filing Institution Note to FinCEN"), as well as in the narrative, and by selecting SAR Field 34(d) (check fraud). Banks should include any and all available information relating to the account and locations involved in the reported activity, identifying information and descriptions of any legal entities or arrangements involved and associated beneficial owners, and any information about related persons or entities involved in the activity. Banks may highlight additional advisory or alert keywords in the narrative, if applicable.

In addition to filing a SAR, as applicable, the alert also suggests banks should refer their customers who may be victims of mail theft-related check fraud to the USPIS at 1-877-876-2455 or **www.uspis.gov/report** to report the incident.

CHECK FRAUD LIABILITY

While the FinCEN alert provides helpful information to identify and report check fraud, it does not address liability for losses resulting from mail theft-related check fraud or check fraud in general. The increase in altered and counterfeit checks has led to confusion about the rules regarding check returns and who bears any loss associated with the defective check. The check handling rules are found in the Uniform Commercial Code (UCC), **chapter 554** in Iowa Code. The UCC rules are based on the reason the check is unpayable, the timely return of unpayable checks, and the party in the best position to prevent the fraud.

FEATURE

Under UCC 554.4401, a paying bank may only pay a check that is properly payable. The UCC requires paying bank deposit customers to exercise "reasonable promptness" in examining statements to determine all items presented for payment were properly authorized by the depositor. Iowa law provides customers up to one year to inspect their statements, however, this period may be (and often is) reduced in the account agreement. Typically account agreements require deposit customers 30 to 60 days to inspect their periodic statements and make a claim that a check was not properly payable.

The reason for the check not being payable determines deadlines for paying banks to take action and responsibility for any loss. The three main reasons a check may not be payable are the check is: (1) altered, (2) counterfeit — having a forged drawer (payor or maker) signature, or (3) forged endorsement. An alteration is an unauthorized change in a check that modifies the obligation of a party. This typically means an alteration of the payee or amount and sometimes involves "washing" the check to make such changes. Whereas, a counterfeit is a check with a forged or unauthorized drawer signature. Neither altered checks nor counterfeit (forged drawer signature) checks are properly payable.

Counterfeit checks — Paying banks have until the "midnight deadline" (midnight of the next banking day following the banking day of receipt) to pay or begin the return of the check. Under Regulation CC, if a paying bank decides to not pay a check, it must generally return the check to the depositary bank not later than 2 p.m. (local time of the depositary bank) on the second business day following the banking day on which the check was presented to the paying bank. The assumption is that the paying bank is in the best position to know whether the signature on the check is its customer's signature.

Altered checks or forged endorsements — The midnight deadline does **not**, however, apply to altered checks or checks containing a forged endorsement. Paying banks who discover that a paid check was altered or contained a forged endorsement may make a breach of warranty claim directly with the depositary bank. When a bank accepts an item for deposit, it warrants to the paying bank that:

- The check is not altered;
- Endorsements are not forged or unauthorized;
- The person being paid is entitled to enforce the check or authorized to obtain payment; and
- The depositary bank has no knowledge that the check contains a forged drawer signature.

The depositary bank is liable for any breaches of these warranties on the basis that it is in the best position to detect the irregularity and flaw and to recover any losses from the depositor. Under Iowa law, the paying bank generally has up to one year to make a breach of warranty claim. The reason paying banks have longer to make breach of warranty claims is that it often takes time for the paying bank and its customers to discover that an endorsement is forged or the check altered. Typically, the paying bank has no contact with the endorsing party and neither it nor its customer may be familiar with the endorsing party's signature. In contrast, the depositary bank is in the best position to detect a forged endorsement as it has the contact with the endorsing party—usually its own customer. Similarly, the depositary bank is in the best position to identify and stop an altered item from entering the system and causing a loss.

Conflicts often arise between the paying bank and bank of first deposit related to timely returns and whether a check was altered or considered counterfeit. The Federal Reserve Financial Services does not "settle" check liability conflicts; it merely processes and returns checks according its Operating Circulars. Liability is often worked out on a bank to bank basis. When the conflict cannot be resolved, the only recourse left may be a legal process. Because the check handling rules are grounded in the UCC, a legal proceeding reviewing the facts and circumstances of the particular situation may be needed to determine liability (if the amount of the check warrants the cost of the legal proceeding). It is also worth noting, Regulation CC does contain a "default rule" but it is only applicable to

substitute checks and electronic checks **where the original check is not available.** In these limited circumstances, a check is **presumed to be altered** in such conflicts where the original check is not available for inspection, however, even this presumption is rebuttable.

RESOURCES

Because the number of checks being written has declined, many banks no longer have team members with extensive knowledge of the UCC check provisions and Fed's check processing rules. Criminals may realize this and are exploiting it. Therefore, an institution's best defense against curbing check fraud losses is knowledge related to:

- Properly identifying why a check is unpayable;
- Differentiating between breach of warranty claims and payor bank responsibilities;
- Understanding the appropriate return timeframes and processes;
- Recognizing when the Fed's check return process can be utilized versus when returns need to be handled on a bank-to-bank basis; and
- Having knowledgeable legal counsel on standby, if needed.

To this end, the IBA does have several resources to assist members with check fraud and check handling matters, including:

- **The Check Handling Guide** — This free, members-only guide sets out the basics of Iowa's Uniform Commercial Code related to check issuance and acceptance.
- A series of **FAQs** on various check handling matters on the IBA website.
- **Payment Fraud on the Rise** — a January 2023 Disclosure article on payment fraud
- On-demand webinar offerings for purchase, including:
  - **Legal Liabilities when Check Fraud Occurs**
  - **Avoiding Check Fraud Liability**
  - **Check Fraud and SAR Filings**

Footnotes:

[1]The USPIS is the law enforcement, crime prevention, and security arm of the USPS.

[2]12 C.F.R. §229.31(b)(1)

[3]Found online at **Operating Circulars**. See **OC 3** for rules related to checks the Fed accepts for return.

REGULATORY NEWS

IRS RELIEF FOR REPORTING 2023 RMDS

The Internal Revenue Service issued **Notice 2023-23** to provide guidance to financial institutions on reporting required minimum distributions (RMDs) for 2023 due to the last minute signing of the SECURE 2.0 Act that moved the required beginning date for RMDs back to 73, impacting the RMD reminder notice due Jan. 1, 2023. This amendment is effective for distributions required to be made after Dec. 31, 2022, with respect to individuals who will attain age 72 after that date. This delay in the required beginning date means that these IRA owners (who, prior to enactment of the SECURE 2.0 Act, would have been required to take minimum distributions from their IRAs for 2023) will have no RMD due from their IRAs for 2023.

If an IRA owner has an RMD due for 2023, the financial institution that is the trustee, custodian, or issuer maintaining the IRA must file a 2022 Form 5498 (IRA Contribution Information) by May 31, 2023, and indicate by a check in Box 11 that an RMD is required for 2023. Additionally, if an IRA owner has an RMD due for 2023, the financial institution must furnish a statement to the IRA owner by Jan. 31, 2023, that informs the IRA owner of the date by which the RMD must be distributed, and either provides the amount of the RMD or offers to calculate that amount upon request (RMD statement).

For IRA owners who will attain age 72 in 2023, the RMD statement should not be sent, and the 2022 Form 5498 should not include a check in Box 11 or any entries in Box 12a or 12b. However, in recognition of the short amount of time financial institutions have had to change their systems for furnishing the RMD statement since the enactment of the SECURE 2.0 Act at the end of 2022, relief is being provided with respect to this reporting. Under this relief, the IRS will not consider an RMD statement provided to an IRA owner who will attain age 72 in 2023 to have been provided incorrectly if the IRA owner is notified by the financial institution no later than April 28, 2023, that no RMD is actually required for 2023. Notice 2023-23 informs the banks they will be granted relief of such reporting errors if they correct them no later than April 28, 2023.

The SECURE 2.0 Act did not change the required beginning date for IRA owners who attained age 72 prior to Jan. 1, 2023. To reduce misunderstanding among IRA owners, the IRS encourages all financial institutions, in communicating these RMD changes, to remind IRA owners who attained age 72 in 2022, and have not yet taken their 2022 RMDs, that they are still required to take those distributions by April 1, 2023.

WARNING: LENDERS MAY BE LIABLE FOR DISCRIMINATORY APPRAISALS

The Justice Department and the Consumer Financial Protection Bureau filed a statement of interest to explain the application of the Fair Housing Act and the Equal Credit Opportunity Act to lenders relying on discriminatory home appraisals. The statement of interest was filed in *Connolly, et al. v. Lanham, et al.,* a lawsuit currently pending in the U.S. District Court for the District of Maryland alleging that an appraiser and a lender violated the FHA and ECOA by lowering the valuation of a home because the owners were Black and by denying a mortgage refinancing application based on that appraisal.

The couple sued the appraiser who provided a lower appraisal for the home when the family's photographs were used, and the nonbank lender that denied a loan based on that appraisal.

Attorneys for the lender have argued the lender should not be held liable because it was relying on a third-party appraiser. In their court filing, the CPFB and DOJ said that lenders can be held liable under the FHA and ECOA for relying on discriminatory appraisals. The nonbank lender "wrongly insists that it could not comply with the FHA and ECOA's requirements because its hands were tied by other federal laws concerning appraisal independence," the agencies said. Rather, the agencies argue lenders are legally obligated **not** to rely on appraisals that are inaccurate or violate the law. "It is well-established that a lender is liable if it relies on an appraisal that it knows or should know to be discriminatory, and (the) defendant's arguments to the contrary are ill-founded," the DOJ and CFPB said. **Read the press release.**

REGULATORY NEWS

FINCEN BOI REPORTING GUIDANCE

FinCEN has started publishing guidance materials to assist the public and small businesses in understanding the upcoming beneficial ownership information (BOI) reporting requirements that become effective Jan. 1, 2024. The materials include **FAQs**, a one-page **key question guide**, as well as a one-page summary of **key filing dates**. In addition, FinCEN posted an **introductory video**, along with a more detailed **informational video** about the reporting requirement.

As a reminder, the Corporate Transparency Act (CTA) called for the establishment of uniform BOI reporting requirements on a central registry for certain types of corporations, limited liability companies, and other similar entities created in or registered to do business in the United States. The CTA authorized FinCEN to collect that information and disclose it to authorized government authorities and financial institutions, subject to effective safeguards and controls. The CTA and its implementing regulations will provide essential information to law enforcement, national security agencies, and others to help prevent criminals, terrorists, proliferators, and corrupt oligarchs from hiding illicit money or other property in the United States. At this point, financial institution requirements related to Beneficial Owners under the BSA has NOT changed.

UPDATED CONTACT INFO ON CONSUMER DISCLOSURES

The Consumer Financial Protection Bureau issued a final rule in the **March 20 Federal Register** that makes non-substantive corrections and updates to CFPB and other federal agency contact information found in various regulations, including the contact information that must be provided on the ECOA adverse action notices and the FCRA Summary of Consumer Rights. The final rule is effective April 19, 2023, but the mandatory compliance date for amendments that impact forms given to consumers, as indicated below, is March 20, 2024.

In Regulation B (ECOA), the CFPB is amending the federal agency contact information in appendix A for the CFPB, OCC, FDIC, NCUA, FTC, and other listed agencies. The contact information must be included in ECOA adverse action notices. The CFPB is also correcting its contact information in appendix D, which sets forth the process for requesting official CFPB interpretations of Regulation B. In Regulation V (FCRA), the CFPB is amending the model form in appendix K for the Summary of Consumer Rights to correct the contact information for various agencies. Again, the contact information changes must be made no later than March 20, 2024. The updated contact information impacting IBA members is:

- CFPB: Bureau of Consumer Financial Protection, 1700 G Street NW, Washington, DC 20552.
- FDIC: Division of Depositor and Consumer Protection, National Center for Consumer and Depositor Assistance, Federal Deposit Insurance Corporation, 1100 Walnut Street, Box #11, Kansas City, MO 64106.
- OCC: Office of the Comptroller of the Currency, Customer Assistance Group, P.O. Box 53570, Houston, TX 77052.

2022 BANK HMDA DATA AVAILABLE

The Consumer Financial Protection Bureau has made available Home Mortgage Disclosure Act modified loan application registers for each financial institution that filed HMDA data collected in 2022. The data from the CFPB is modified to protect applicant and borrower privacy. The 2022 modified HMDA data can be found **here**.

REGULATORY NEWS

HUD TO REINSTATE 2013 DISPARATE IMPACT RULE

The Department of Housing and Urban Development announced that it has submitted to the Federal Register for publication a final rule entitled Restoring HUD's Discriminatory Effects Standard. This final rule rescinds the Department's 2020 rule governing Fair Housing Act disparate impact claims and restores the 2013 discriminatory effects rule. In this final rule, HUD emphasizes that the 2013 rule is more consistent with how the Fair Housing Act has been applied in the courts and in front of the agency for more than 50 years.

HUD's 2020 final rule conformed the 2013 disparate impact rule with the U.S. Supreme Court's 2015 decision in *Texas Department of Housing and Community Affairs v. Inclusive Communities Project,* which recognized disparate impact analysis to demonstrate discrimination claims under the FHA but added key limitations to ensure the burden of proof in disparate impact cases is with the plaintiff. The 2020 final rule never took effect because a Massachusetts federal district court judge stayed the rule pending consideration of consumer advocates' challenge to the rule as arbitrary and capricious. In a statement, HUD said the 2013 rule provides a more straightforward framework for determining discriminatory effects than the 2020 rule.

This Final Rule will go into effect 30 days after it is published in the Federal Register. Due to a preliminary injunction staying the implementation of the 2020 Rule in Massachusetts Fair Housing Center v. HUD, the 2020 Rule never went into effect, and the 2013 Rule – which has been in place for nearly a decade – has been and is currently still in effect. Accordingly, regulated entities that were complying with the 2013 Rule have no need to change any practices they have in place to comply with this rule. Read HUD's **Final Rule** on Restoring HUD's Discriminatory Effects Standard.

CFPB SUPERVISORY HIGHLIGHTS FOCUSES ON FEES

The Consumer Financial Protection Bureau issued a special edition of **Supervisory Highlights** in early March focusing on the CFPB's recent supervisory work related to violations of law in connection with fees. The publication includes supervisory observations related to Deposits, Auto Servicing, Mortgage Servicing, Payday and Small-Dollar Lending and Student Loan Servicing.

The CFPB noted the following exam findings:

- Related to Deposit Accounts, the CFPB cited institutions for unfair unanticipated overdraft fees for transactions that authorized against a positive balance, but settled against a negative balance (i.e., APSN overdraft fees) as well as the practice of assessing multiple NSF fees for the same transaction when disclosures did not adequately explain multiple fees could be assessed if the same item was presented for payment more than once.
- Examiners found that auto servicers engaged in unfair acts or practice by assessing late fees in excess of the amounts allowed by consumers' contracts, charging unauthorized late fees after acceleration and/or repossession and charging repossession fees significantly higher than average repossession costs.
- In conducting mortgage servicing examinations, examiners identified a number of UDAAP and Regulation Z violations related to junk fees. Examiners found that servicers charged consumers late fee amounts in excess of amounts authorized by the contract — specifically servicers failed to implement maximum late fee amounts set by the contract and/or state law. Examiners also found that servicers engaged in deceptive acts or practices by sending monthly periodic statements and escrow disclosures that included monthly private mortgage insurance premiums that consumers did not owe. These consumers did not have borrower-paid PMI on their accounts; instead, the loans were originated with lender-paid PMI, which should not be billed directly to consumers.

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

Q What information needs to be updated in our CRA Public File each year and what is the deadline for completing the updates? Are all banks, regardless of their size, subject to the CRA public file requirements?

A The deadline for updating the public file is April 1 each year. So if your bank has not already completed this project, you need to complete the update ASAP. The public file requirements are found in Regulation BB, § 228.43. All banks must are subject to the public file requirements but the requirements vary a bit depending upon the size of your bank and whether or not your bank is subject to HMDA reporting. The IBA has developed a checklist to assist member banks in updating their public files, see 2023 CRA Public File Checklist.

Q If a customer asks why we are requesting their personal information for a Currency Transaction Report (CTR) reportable transaction, or the amount of cash deposit that triggers reporting, what should we say?

A To assist frontline staff in these situations, FinCEN developed a pamphlet containing information on the CTR requirements. This pamphlet can be provided directly to customers to address their questions. The bank is not required to provide consumers with the pamphlet, but it is a useful tool that helps customers understand when a CTR is triggered and why the bank is requesting their personal information. The pamphlet can be found here with more information about the pamphlet and its use found here.

Q We had a customer apply for a mortgage loan. As part of our underwriting process we obtained a tri-merge credit bureau report for each applicant. Within a couple hours of our credit report pull, our applicant was contacted by another lender with a sales pitch for a mortgage loan. The other lender told our customer they saw that they had applied for a mortgage loan at our bank. Of course, our customer contacted us immediately wanting to know why we shared their information with another lender. When we contacted our credit bureau provider to understand how another lender would know so quickly we had pulled a credit report on our customer, we learned the other lender subscribed to the bureau to receive "trigger leads." I know about pre-screened offers of credit but I had never heard of a trigger lead. Can you tell me more?

A A "trigger lead" is a marketing product that is sold by the three major credit bureaus — Experian, TransUnion and Equifax — to lenders who are looking for customers with certain specifications like loan types, ZIP codes or FICO scores. After a consumer applies for a loan, the lender will typically pull their credit report, signaling to the major credit bureaus the consumer is shopping for credit. The CRA then sells this information to product subscribers who often reach out to consumers via phone call or email within hours of the credit pull to provide their rate and product information to the consumer.

Triggers leads are legal under the Fair Credit Reporting Act and can even benefit consumer who are truly shopping for credit products. But trigger leads can be frustrating for consumers who do not want to be solicited and think their lender has shared their information with another lender without their permission. There are ways that a consumer can prevent ending up on a trigger list:

- Register at www.optoutprescreen.com. This will opt a consumer out of unwanted prescreened solicitations and trigger leads for five years and it costs nothing. It does usually take one to two weeks for it to take effect.
- Sign up at the Do Not Call Registry, www.donotcall.gov. This is also free and should take effect within 24 hours, however a borrower may have already ended up on a trigger lead list prior to registering so could still receive calls for up to 31 days. Being on the DNC list does not mean all calls will stop.

Lenders can help limit trigger lead contacts by not including the consumer's phone number or email address on the credit pull.

Q Since interest rates are rising, we have more customers interested in using their time certificates of deposit as collateral for loans in order to obtain a better

interest rate. Can you remind me when we should and should not be checking the "required deposit" box in the Fed Box disclosure?

A The "required deposit" disclosure is detailed in Regulation Z at **§ 1026.18(r)** and is triggered if the creditor requires the consumer to maintain a deposit account as a condition of the transaction – which would be the case when the creditor requires the deposit account as collateral as a condition for a favorable interest rate.

Section 1026.18(r) describes three types of deposits that are not considered required deposits: escrow accounts for items such as taxes, insurance and repairs; payments under a Morris plan; and a deposit that earns "not less than" 5 percent per year. The "not less than" language is a bit confusing. It means, if a deposit earns at least 5 percent per year (or more), no disclosure is required. This exception applies whether the deposit is held by the creditor or by a third party. Thankfully, the Official Staff Commentary to this section states, *"Use of the phrase "need not" permits creditors to include the disclosure even in cases where there is doubt as to whether the deposit constitutes a required deposit."* This means the required deposit box can be checked consistently when a deposit account is taken as collateral for a loan regardless of the interest rate earned on the deposit, ensuring compliance with regulation.

Q If a customer deposits over $10,000 into their joint account, we would normally file a CTR on both owners of the account. A Part 1 would be completed for the owner depositing the funds, checking box 2a — Person conducting transaction on own behalf. Another Part 1 would be completed for the second owner, checking box 2c — Person on whose behalf transaction was conducted. However, in our most current situation one of the joint owners recently passed away but is still listed as an owner on the account. So do we still complete a Part 1 on the deceased joint owner?

A If the account is owned jointly with survivorship, then upon the death of one owner, the funds pass directly to the surviving owner. As a result, a CTR Part 1 would only be completed for the surviving owner, checking box 2a — Person conducting transaction on own behalf.