Regulatory Update

Community Bankers for Compliance

Third Quarter 2024

Website

younginc.com

131 East Main Street • P.O. Box 711 • Kent, OH 44240 | P 330.678.0524 • F 330.678.6219

Instructors for the CBC Program

Bill Elliott, CRCM, Senior Consultant and Director of Compliance Education, Young & Associates, Inc.

Bill Elliott has over 45 years of banking experience. As a senior compliance consultant and manager of the compliance division with Young & Associates, Inc., Bill works on a variety of compliance-related issues, including leading compliance seminars, conducting compliance reviews, conducting in-house training, and writing compliance articles and training materials.

Bill's career includes 15 years as a compliance officer and CRA officer in a large community bank, as well as working at a large regional bank. He has experience with consumer, commercial, and mortgage loans, and has managed a variety of bank departments, including loan review, consumer/commercial loan processing, mortgage loan processing, loan administration, credit administration, collections, and commercial loan workout.

Dale Neiss, CRCM, Consultant, Young & Associates, Inc.

Dale Neiss is a compliance consultant with Young & Associates, Inc. With over 40 years of banking experience in Denver, CO, Dale has developed and implemented compliance management systems, loan review and community reinvestment act (CRA) programs, and enterprise risk management (ERM) framework for multiple banks. He has held the titles of Compliance and Loan Review Manager, BSA and CRA Officer, and Enterprise Risk Management Director. Prior to his Denver, CO banking experience, Dale began his banking career with the Office of the Comptroller of the Currency in Indianapolis, IN as an associate national bank examiner. At Young & Associates, Inc., he provides consulting and training, as well as writes articles and compliance manuals. He holds the designation of Certified Regulatory Compliance Manager (CRCM) by the Institute of Certified Bankers in Washington, D.C. Dale earned a Bachelor of Business Administration degree in Finance and Management from Kent State University.

Table of Contents

Agency News Items

CFPB: Financial and Privacy Risks to Consumers in Video Gaming Marketplaces (April 4, 2024)

Link

https://www.consumerfinance.gov/data-research/research-reports/issue-spotlight-video-games/

Text

The Consumer Financial Protection Bureau (CFPB) issued a report examining the growth of financial transactions in online video games and virtual worlds. These platforms increasingly resemble traditional banking and payment systems that facilitate the storage and exchange of billions of dollars in assets, including virtual currencies. However, consumers report being harmed by scams or theft on gaming platforms and not receiving the protections they would expect under federal law. The CFPB will be monitoring markets where financial products and services are offered, including video games and virtual worlds, to ensure compliance with federal consumer financial protection laws.

The report, Banking in Video Games and Virtual Worlds, looks at the growing use and scale of these assets across the gaming industry, the associated risks to consumers, and the evolution of games and virtual worlds into online marketplaces. American consumers spent nearly $57 billion on gaming in 2023, including on hardware, software, and in-game transactions such as converting dollars to virtual currencies or other gaming assets. These assets are often bought, sold, or traded in virtual markets that allow gaming companies to replicate everyday activities online, including financial payments.

The report identifies a number of trends and risks associated with gaming assets, including:

- **Gaming products and services resemble conventional financial products:** Games and virtual worlds enable players to store and transfer valuable assets, including in-game currencies and virtual items such as cosmetic skins or collectibles. For example, the largest reported sale of a cosmetic skin was for $500,000. Games and virtual worlds act as a real-world marketplace that enables players to store and transfer valuable assets. To leverage that value, gaming companies have begun incorporating financial products and services such as proprietary payment processors and money transmitters.
- **Gaming companies provide little customer support when consumers experience financial harm**: The increased value of in-game assets has fueled a rise in scams, phishing attempts, and account thefts. Attackers use phishing tactics or compromised user credentials to break into accounts and access game currency or virtual items, and then sell these assets off the platform for other currency. Consumers report having little recourse with gaming companies when they suffer losses, and game publishers claim to have no obligation to compensate the players for financial losses, including when service to a game

is suspended or a consumer's account is closed.

- **Gaming companies are assembling gamers' personal and behavioral data**: Publishers are collecting large amounts of data on players, including behavioral details such as financial data, purchasing history and spending thresholds. Gaming platforms can also track players' location data, which can generate an accurate portrait of a player's daily routines, such as their home address, places of employment or worship, and health and medical status. And with the advent of virtual- and mixed-reality gaming, the information gathered by headsets may include biometric data such as iris scans, eye movement, pupil response, and gait analysis, which may pose medical privacy risks.

The CFPB has received consumer complaints about hacking attempts, account theft, and lost access to gaming assets. In the complaints, most consumers report receiving limited support from the gaming companies, such as reimbursements or security improvements. Existing consumer protection laws apply to banking and payment systems that facilitate the storage and exchange of valuable assets. The CFPB is monitoring markets where financial products and services may be offered, including video games and virtual worlds.

What You Need to Do
Informational; please share with interested team members.

CFPB: Spring 2024 Supervisory Highlights (April 8, 2024)

Link

https://files.consumerfinance.gov/f/documents/cfpb_supervisory-highlights_issue-33_2024-04.pdf

Text - Introduction

The residential mortgage servicing market exceeds $13 trillion in current outstanding balances. When servicers do not comply with the law, they impose significant costs on consumers.

The CFPB is actively monitoring the market for emerging risks during a period of increasing default servicing activity since the end of the COVID-19 pandemic emergency. The mortgage industry has grappled with many challenges during this period, including increased requests for loss mitigation, changes to housing policies and programs, and staffing issues. Violations described in prior editions of *Supervisory Highlights* raised concerns about servicers' ability to appropriately respond to consumer requests for assistance, especially consumers at risk of foreclosure. While mortgage delinquencies and foreclosure rates remain near all-time lows, this may change in the future as consumers grapple with higher levels of debt and affordability challenges due to high rates and low housing supply. Foreclosure starts have risen in recent months, increasing the risks that vulnerable consumers face.

The CFPB also continues to prioritize scrutiny of exploitative illegal fees charged by banks and financial companies, commonly referred to as "junk fees." Examiners continue to find supervised mortgage servicers assessing junk fees, including unnecessary property inspection fees and improper late fees. Additionally, examiners found that mortgage servicers engaged in other unfair, deceptive, and abusive acts or practices (UDAAP) such as sending deceptive loss mitigation eligibility notices to consumers. Mortgage servicers also violated several of Regulation X's loss mitigation provisions.

The CFPB is currently reviewing Regulation X's existing framework to identify ways to simplify and streamline the mortgage servicing rules. The CFPB is considering a proposal to streamline the mortgage servicing rules, only if it would promote greater agility on the part of mortgage servicers in responding to future economic shocks while also continuing to ensure they meet their obligations for assisting borrowers promptly and fairly.

The findings in this report cover select examinations regarding mortgage servicing, that were completed from April 1, 2023 through December 31, 2023. To maintain the anonymity of the supervised institutions discussed in *Supervisory Highlights*, references to institutions generally are in the plural and related findings may pertain to one or more institutions.

Supervisory Observations

Mortgage Servicing

Examiners found that mortgage servicers engaged in UDAAPs and regulatory violations while processing payments by overcharging certain fees, failing to adequately describe fees in periodic statements, and not making timely escrow account disbursements. Additionally, as in prior editions of *Supervisory Highlights*, examiners identified persistent UDAAP and regulatory violations at mortgage servicers related to loss mitigation practices.

Unfair charges for property inspections prohibited by investor guidelines

Mortgage investors generally require servicers to perform property inspection visits for accounts that reach a specified level of delinquency. Investor guidelines stipulate when servicers should complete these property inspections. Servicers pass along the cost of property inspections to the consumers; the fees for this action generally range from $10 to $50.

Examiners found that servicers engaged in unfair acts or practices by charging property inspection fees on Fannie Mae loans where such inspections were prohibited by Fannie Mae guidelines. The CFPA defines an unfair act or practice as an act or practice that: (1) causes or is likely to cause substantial injury to consumers; (2) is not reasonably avoidable by consumers, and (3) is not outweighed by countervailing benefits to consumers or to competition.

Fannie Mae guidelines prohibit property inspections if the property is borrower-or tenant-occupied and one of the following applies: the servicer has established quality right party contact with the borrower within the last 30 days, the borrower made a full payment within the last 30 days, or the borrower is performing under a loss mitigation option or bankruptcy plan. Examiners found that in some instances a servicer would charge a property inspection fee on Fannie Mae loans even though the property was borrower-or tenant-occupied and the servicer had established quality right party contact within 30 days, the borrower had made a full payment within the last 30 days, or the borrower was performing under a loss mitigation option. In total, the servicers

charged hundreds of borrowers fees for property inspections that were prohibited by Fannie Mae's guidelines, causing consumers substantial injury. Consumers were unable to anticipate the property inspection fees or mitigate them because they have no influence over the servicer's practices. Charging improper fees has no benefit to consumers or competition. In response to these findings, the servicers corrected automation flaws behind some of the improper charges and implemented testing and monitoring to address the others. The servicers were also directed to identify and remediate borrowers who were charged fees contrary to investor guidelines.

Unfair late fee overcharges

Examiners found that servicers engaged in unfair acts or practices by assessing unauthorized late fees. These errors occurred for one of two reasons. First, in some instances servicers charged late fees that exceeded the amount allowed in the loan agreement. Second, in some instances servicers charged late fees even though consumers had entered into loss mitigation agreements that should have prevented late fees. Examiners found these practices constituted unfair acts or practices.

The servicers caused substantial injury to consumers when they imposed these unauthorized late fees. Consumers could not reasonably avoid the injury because they do not control how servicers calculate late fees and had no reason to anticipate that servicers would impose unauthorized late fees. Charging unauthorized late fees had no benefits to consumers or competition. In response to these findings, servicers refunded the fees and improved internal processes.

Failing to waive existing fees following acceptance of COVID-19 loan modifications

Regulation X generally allows certain servicers to offer streamlined loan modifications made available to borrowers experiencing a COVID-19 related hardship based on the evaluation of incomplete loss mitigation applications if the modifications meet certain requirements. One requirement is that the servicer "waives all existing late charges, penalties, stop payment fees, or similar charges that were incurred on or after March 1, 2020, promptly upon the borrower's acceptance of the loan modification."

Examiners found that servicers offered streamlined COVID-19 loan modifications but, in violation of Regulation X, failed to waive existing fees after borrowers accepted the modifications. In response to these findings, servicers are remediating consumers.

Failing to provide adequate description of fees in periodic statements

Regulation Z requires servicers to provide billing statements that include a list of all transaction activity that occurred since the last statement, including, among other things, "a brief description of the transaction." Examiners found that servicers failed to provide a brief description of certain fees and charges in violation of this provision when they used the general label "service fee" for 18 different fee types, without including any additional descriptive information. In response to these findings, the servicers implemented changes to provide more specific descriptions of each service fee.

Failing to make timely disbursements from escrow accounts

Regulation X requires servicers to make timely disbursements from escrow accounts if the borrower is not more than 30 days overdue. Timely disbursements are defined as payments made on or before the deadline to avoid a penalty. Examiners found servicers attempted to make timely escrow disbursements, but the payments did not reach the payees. The servicers did not resend the payments until months after the initial payment attempts. Some borrowers incurred penalties due to the late payments, which the servicers only reimbursed after the borrowers complained. Because the initial payments were unsuccessful, and the second payments were late, the servicers did not make timely disbursements and violated Regulation X. In response to these findings, the servicers were directed to comply with this regulation and remediate borrowers.

Deceptive loss mitigation eligibility notices

Examiners found that servicers engaged in deceptive acts or practices when they sent notices to consumers representing that the consumers had been approved for a streamlined loss mitigation option even though the servicers had not yet determined whether the consumers were eligible for the option.

In fact, some consumers were ultimately denied the option. An act or practice is deceptive when: (1) the representation, omission, act, or practice misleads or is likely to mislead the consumer; (2) the consumer's interpretation of the representation, omission, act, or practice is reasonable under the circumstances; and (3) the misleading representation, omission, act, or practice is material.

The notices were misleading because the servicers had not yet determined the consumers were eligible for the loss mitigation option. Consumers reasonably interpreted the representations to mean that the loss mitigation option was available to them. The representations were material because consumers could have made budgeting decisions on the false assumption that they were approved for a loss mitigation option or were discouraged from submitting complete loss mitigation applications or taking other steps to cure their delinquencies and avoid foreclosure. In response to these findings, the servicers reviewed affected borrowers who remained delinquent to ensure they were considered for appropriate loss mitigation options.

Deceptive delinquency notices

Examiners found that servicers engaged in deceptive acts or practices when they sent notices informing certain consumers that they had missed payments and should fill out loss mitigation applications. In fact, these consumers did not need to make a payment because they were current on their payments, in a trial modification plan, or had an inactive loan (e.g., loan was paid off or subject to short sale). These misrepresentations were likely to mislead consumers and it was reasonable for consumers under the circumstances to believe that the notices from their servicers were accurate. The representations were material because they were likely to influence consumers' course of conduct. For example, in response to the notice, a consumer may contact their servicer to correct the error or fill out unnecessary loss mitigation applications. In response to these findings, servicers are implementing additional policies and procedures to ensure accuracy of notices.

Loss mitigation violations

Regulation X generally requires servicers to send borrowers a written notice acknowledging receipt of their loss mitigation application and notifying the borrowers of the servicers' determination that the loss mitigation application is either complete or incomplete after receiving the application. Examiners found that servicers violated Regulation X by sending acknowledgment notices to borrowers that failed to specify whether the borrowers' applications were complete or incomplete.

Additionally, after receiving borrowers' complete loss mitigation applications, Regulation X generally requires servicers to provide borrowers with a written notice stating the servicers' determination of which loss mitigation options, if any, the servicers will offer to the borrower. Among other requirements, the written notice must include the amount of time the borrower has to accept or reject an offer of a loss mitigation option. Examiners found that servicers violated Regulation X because the servicers did not provide timely notices stating the servicers' determination regarding loss mitigation options. The servicers were directed to enhance policies and procedures to ensure timely loss mitigation determinations. One servicer also violated Regulation X because its written notices did not provide a deadline for accepting or rejecting loss mitigation offers. In response to the finding, the servicers updated the offer letter templates to include a deadline to accept or reject the loss mitigation offer.

Finally, Regulation X requires servicers to maintain policies and procedures that are reasonably designed to ensure that they can properly evaluate borrowers who submit applications for all available loss mitigation options for which they may be eligible. Examiners found that servicers violated Regulation X because they failed to maintain policies and procedures reasonably designed to achieve this objective. Specifically, the servicers did not follow investor guidelines for evaluating loss mitigation applications when they automatically denied certain consumers a payment deferral option rather than submitting the consumers' applications to the investor for review. In response to these findings, the servicers updated their policies and procedures and refunded or waived late charges and corrected negative credit reporting for impacted consumers.

Live contact and early intervention violations

Regulation X requires servicers to make good faith efforts to establish live contact with delinquent borrowers no later than the 36th day of delinquency. Examiners found that servicers violated this provision when they failed to make good faith efforts to establish live contact with hundreds of delinquent borrowers. The servicers took corrective action which included providing remediation to harmed borrowers including refunding or waiving late fees.

Regulation X also requires servicers to provide written early intervention notices to delinquent borrowers no later than the 45th day of delinquency and again every 180 days thereafter. Examiners found that servicers violated this provision when they failed to send written early intervention notices to thousands of delinquent borrowers. In response to these findings, the servicers identified and provided remediation to affected borrowers who were assessed late fees for missed payments after the 45th day of delinquency

Failing to retain records documenting actions taken on mortgage loan accounts

Regulation X requires servicers to retain records documenting actions taken with respect to a borrower's mortgage loan account until one year after the date the loan was discharged or servicing of the loan was transferred to another servicer. Examiners found that servicers failed to

document certain actions in their servicing systems, such as establishing live contact with borrowers, in violation of this provision. In response to these findings, the servicers were directed to enhance training and monitoring to ensure compliance with this requirement.

What You Need to Do

Informational; please share with affected team members.

CFPB: Action to Stop Illegal Junk Fees in Mortgage Servicing (April 24, 2024)

Link

https://files.consumerfinance.gov/f/documents/cfpb_supervisory-highlights_issue-33_2024-04.pdf

Text

The Consumer Financial Protection Bureau (CFPB) published an edition of *Supervisory Highlights* describing the agency's actions to combat junk fees charged by mortgage servicers, as well as other illegal practices. CFPB examinations found servicers charging illegal junk fees, such as prohibited property inspection fees; sending deceptive notices to homeowners; and violating loss mitigation rules that help struggling borrowers stay in their homes. In response to the CFPB's findings, financial institutions refunded junk fees to borrowers and stopped their illegal practices.

The mortgage servicing examination work announced today builds on prior CFPB exam work combatting junk fees in the mortgage servicing and other consumer financial markets. In October of last year, the CFPB announced that its examination work from February to August of 2023 resulted in $140 million refunded to consumers for unlawful junk fees in the areas of bank account deposits, auto loan servicing, and international money transfers. Since that time, the CFPB's supervision junk fee work has resulted in more than $120 million in additional junk fee refunds in the area of bank account deposits.

Mortgage servicers are the companies responsible for, among other things, processing mortgage payments and managing mortgage accounts. They play a critical role in assisting homeowners with repayment, including by helping mortgage borrowers access repayment options when they face financial difficulties. A mortgage servicer is chosen by the lender or investor that owns the mortgage, and not by the homeowner. Residential mortgage servicers currently handle more than $13 trillion in mortgage balances.

Over the last few years, the CFPB has prioritized combatting illegal junk fees in a wide range of consumer financial markets. Most recently, the CFPB announced a final rule that, when it goes into effect, would reduce credit card late fees by more than $10 billion every year. The CFPB has also proposed a rule that would save consumers more than $3.5 billion in overdraft fees every

year, and has addressed junk fees charged on international money transfers. Overdraft and non-sufficient funds fees have declined by more than $6.1 billion since the CFPB began scrutinizing junk fees.

The CFPB has also announced that it is working to address other anticompetitive mortgage fees, including those charged in connection with closing costs.

Some key findings from today's edition of *Supervisory Highlight* include mortgage servicers:

- **Illegally charging and obscuring fees:** Mortgage servicers charged homeowners prohibited and unauthorized fees. These included prohibited fees for property inspections and late fees that exceeded amounts allowed by their mortgage loan agreements. Mortgage servicers also failed to explain the reasons for fees by not describing them adequately on statements.
- **Keeping homeowners on the hook for fees during COVID-19:** During COVID-19, many servicers used a streamlined process to determine repayment options for struggling homeowners. Some servicers failed to waive late fees and penalties, as required.
- **Missing deadlines to pay property tax and home insurance:** Mortgage servicers that accepted or required money from borrowers to pay taxes and insurance failed to make those payments in a timely manner, which caused some borrowers to incur penalties. Servicers only took responsibility for those penalties for missed on-time payments if homeowners submitted complaints.
- **Deceiving homeowners and failing to properly evaluate them for repayment options:** Some servicers sent notices to homeowners in financial distress that stated they had been approved for a repayment option. In fact, no final decisions had been made, and some of the homeowners were ultimately rejected. Examiners also found servicers sent some homeowners false notices saying that they had missed payments and should apply for repayment options. Servicers also improperly denied requests for help and failed to evaluate struggling borrowers for repayment options as required under the CFPB's mortgage servicing rules.

In response to the CFPB's findings, mortgage servicers are taking corrective actions, including changes to their policies and procedures. For the fee-related findings, servicers are remediating homeowners, including providing refunds.

The CFPB has been looking at ways to streamline mortgage servicing rules, while making sure mortgage servicers fulfill their obligations to treat homeowners fairly. Findings from this edition of *Supervisory Highlights* will help inform any proposed changes.

What You Need to Do

Informational; please share with affected team members.

FRB: Consumer Compliance Outlook (April 30, 2024)

Link

https://www.consumercomplianceoutlook.org/

Text

Editor's Note: The material in the *Consumer Compliance Outlook* (*CCO*) is the intellectual property of the 12 Federal Reserve Banks and cannot be copied without permission.

In addition to regular articles on federal consumer compliance laws and regulations, the *CCO* will include data-driven articles that leverage the Federal Reserve System's supervisory data and observations from conducting consumer compliance examinations of state member banks. To that end, the *CCO* will be publishing articles on the top-cited violations in the prior year, including the nature of the violations, common mistakes, and risk mitigants. Financial institutions can use this information to help manage compliance risk.

The latest issue of *Consumer Compliance Outlook* is available for download. This issue includes the following articles and features:

- Overview of Private Flood Insurance Compliance Requirements
- Consumer Compliance Requirements for Commercial Products and Services
- Compliance Spotlight: Resources to Combat Increased Check Fraud

What You Need to Do
Informational; please share with affected team members.

Joint Agencies: Guide to Assist Community Banks to Develop and Implement Third-Party Risk Management Practices (May 3, 2024)

Link

https://www.federalreserve.gov/publications/2024-may-third-party-risk-management.htm

Text

Federal bank regulatory agencies released a guide to support community banks in managing risks presented by third-party relationships.

Community banks engage with third parties to help compete in and respond to an evolving financial services landscape. Third-party relationships present varied risks that community banks are expected to appropriately identify, assess, monitor, and control to ensure that their activities are performed in a safe and sound manner and in compliance with applicable laws and regulations. These laws and regulations include, but are not limited to, those designed to protect consumers and those addressing financial crimes.

The guide offers potential considerations, resources, and examples through each stage of the third-party relationship and may be a helpful resource for community banks. While the guide illustrates the principles discussed in the third-party risk management guidance issued by the agencies in June 2023 (https://www.federalregister.gov/documents/2023/06/09/2023-12340/interagency-guidance-on-third-party-relationships-risk-management), it is not a substitute for that guidance.

What You Need to Do

Informational; please share with affected team members.

CFPB: Statement on Supreme Court Decision in CFPB v CFSA (May 16, 2024)

Link

https://www.consumerfinance.gov/about-us/newsroom/statement-on-supreme-court-decision-in-cfpb-v-cfsa/

Text

The Consumer Financial Protection Bureau issued a statement regarding the Supreme Court's decision in CFPB v. Community Financial Services Association of America:

"For years, lawbreaking companies and Wall Street lobbyists have been scheming to defund essential consumer protection enforcement. The Supreme Court has rejected their radical theory that would have devastated the American financial markets. The Court repudiated the arguments of the payday loan lobby and made it clear that the CFPB is here to stay."

"Congress created the CFPB to be the primary federal watchdog protecting consumers from predatory and abusive practices in the financial sector. Since the CFPB opened its doors in 2011, it has delivered more than $20 billion in consumer relief to hundreds of millions of consumers and has handled more than 4 million consumer complaints."

"Today's decision is a resounding victory for American families and honest businesses alike, ensuring that consumers are protected from predatory corporations and that markets are fair, transparent, and competitive."

"This ruling upholds the fact that the CFPB's funding structure is not novel or unusual, but in fact an essential part of the nation's financial regulatory system, providing stability and continuity for the agencies and the system as a whole. As we have done since our inception, the CFPB will continue carrying out the vital consumer protection work Congress charged us to perform for the American people."

What You Need to Do

Informational; please share with interested team members.

Joint Agencies: Host State Loan-to-Deposit Ratios (May 31, 2024)

Link

https://www.fdic.gov/system/files/2024-05/final-section-109-ratios-june-2023-data-04-29-24.pdf

Text

The Board of Governors of the Federal Reserve System (Board), the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC) (collectively, the agencies) are making public the host state loan-to-deposit ratios that the agencies will use to determine compliance with section 109 of the Riegle-Neal Interstate Banking and Branching Efficiency Act of 1994 (Interstate Act). In general, section 109 prohibits a bank from establishing or acquiring a branch or branches outside of its home state primarily for the purpose of deposit production. Section 106 of the Gramm-Leach-Bliley Act of 1999 amended coverage of section 109 of the Interstate Act to include any branch of a bank controlled by an out-of-state bank holding company.

To determine compliance with section 109, the appropriate agency first compares a bank's estimated statewide loan-to-deposit ratio to the estimated host state loan-to-deposit ratio for a particular state. If the bank's statewide loan-to-deposit ratio is at least one-half of the published host state loan-to-deposit ratio, the bank has complied with section 109. A second step is conducted if a bank's estimated statewide loan-to-deposit ratio is less than one-half of the published ratio for that state or if data are not available at the bank to conduct the first step. The second step requires the appropriate agency to determine whether the bank is reasonably helping to meet the credit needs of the communities served by the bank's interstate branches. A bank that fails both steps is in violation of section 109 and subject to sanctions by the appropriate agency.

Section 109 of the Interstate Banking and Branching Efficiency Act	
Host State Loan-to-Deposit Ratios Using Data as of June 30, 2023 (Excludes wholesale or limited purpose Community Reinvestment Act-designated banks, credit card banks, and special purpose banks)	
State of U.S. Territory	**Host State Loan-to-Deposit Ratio**
Illinois	80%
Indiana	85%
Kansas	80%
Michigan	88%
Missouri	78%
Montana	77%
North Dakota	85%
Ohio	75%
Wisconsin	90%

Due to the legislative intent against imposing regulatory burden, no additional data were collected from institutions to implement section 109. However, since insufficient lending data were available on a geographic basis to calculate the host state loan-to-deposit ratios directly, the agencies used a proxy to estimate the ratios. Accordingly, the agencies calculated the host state loan-to-deposit ratios using data obtained from the Consolidated Reports of Condition and Income (call reports) and Summary of Deposits Surveys (summary of deposits), as of June 30, 2023. For each home state bank, the agencies calculated the percentage of the bank's total deposits attributable to branches located in its home state (determined from the summary of deposits), and applied this percentage to the bank's total domestic loans (determined from the call reports) to estimate the amount of loans attributable to the home state. The host state loan-to-deposit ratio was then calculated by separately totaling the loans and deposits for the home state banks, and then dividing the sum of the loans by the sum of the deposits.

Section 109 directs the agencies to determine, from relevant sources, the host state loan-to-deposit ratios. As discussed in the preamble to the joint final rule, Prohibition Against Use of Interstate Branches Primarily for Deposit Production (62 FR 47728, 47731, September 10, 1997), implementing section 109, banks designated as wholesale or limited purpose banks under the Community Reinvestment Act (CRA) were excluded from the host state loan-to-deposit calculation, recognizing that these banks could have very large loan portfolios, but few, if any, deposits. Likewise, credit card banks, which typically have large loan portfolios but few deposits, were also excluded, regardless of whether they had a limited purpose designation for CRA purposes. Beginning in 2001, special purpose banks, including bankers' banks, were excluded because these banks do not engage in traditional deposit taking or lending. The estimated host state loan-to-deposit ratios, and any changes in the way the ratios are calculated, will be

publicized on an annual basis.

What You Need to Do
If applicable; please share with associated team members.

OCC: Prohibition Against Interstate Deposits: Annual Host State Loan-to-Deposit Ratios (June 13, 2024)

Link

https://occ.gov/news-issuances/bulletins/2024/bulletin-2024-14.html

Text

The Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation (collectively, the agencies) issued on May 31, 2024, the host state loan-to-deposit (LTD) ratios. The OCC is issuing this bulletin to inform banks about how these ratios are used to determine compliance with section 109 of the Riegle—Neal Interstate Banking and Branching Efficiency Act of 1994 (IBBEA).

This bulletin rescinds OCC Bulletin 2023-14, "Prohibition Against Interstate Deposits: Annual Host State Loan-to-Deposit Ratios," published May 19, 2023.

These ratios

- use data as of June 30, 2023. The data excludes banks designated for Community Reinvestment Act (CRA) purposes as wholesale, limited purpose, or special purpose banks.
- are used to compare a bank's statewide LTD ratio with the host state LTD ratio for banks in a particular state.
- update data last released on May 19, 2023.

Section 109 of the IBBEA prohibits the use of interstate branches primarily for deposit production. The OCC's CRA regulation, specifically 12 CFR 25, subpart E, "Prohibition Against Use of Interstate Branches Primarily for Deposit Production," implements the requirements of IBBEA, section 109. The regulation includes specific tests for determining whether an interstate bank is lending appropriately in host states where it has branches.

Section 109 of the IBBEA and 12 CFR 25, subpart E, provide a process to test compliance with the statutory requirements. The first step in the process is an LTD ratio test that compares a bank's statewide LTD ratio with the host state LTD ratio for banks in a particular state. The second step is conducted if a bank's statewide LTD ratio is less than 50 percent of the published host state LTD for that state or if data are insufficient to complete step one. The second step requires the OCC to determine whether the bank is reasonably helping to meet the credit needs of the communities served by the bank's interstate branches. A bank that fails both steps is subject

to sanctions by the OCC.

The LTD ratios are published annually and comply with the requirements of IBBEA section 109.

What You Need to Do

If applicable; please share with associated team members.

Lending Issues

CFPB: Paying Upfront Fees to Lower Interest Rates on Mortgages (April 5, 2024)

Link

https://www.consumerfinance.gov/data-research/research-reports/data-spotlight-trends-in-discount-points-amid-rising-interest-rates/

Text

The Consumer Financial Protection Bureau (CFPB) issued a new report finding that more borrowers paid "discount points" upfront as overall interest rates rose. The percentage of homebuyers paying discount points roughly doubled from 2021 to 2023. The increase was even greater among borrowers with lower credit scores. While discount points may provide advantages to some borrowers, the financial tradeoffs are complex. The CFPB is monitoring these increases and potential risks to consumers.

Discount points are a one-time fee paid at closing to a lender in exchange for a lower interest rate. Paying one discount point is the equivalent of paying a fee of one percent of the loan amount, but discount points have no fixed value in terms of the change in interest rate. Most borrowers only benefit from discount points if they keep their mortgage long enough that the cumulative monthly savings from the reduced interest rate outweigh the upfront costs.

The report used quarterly Home Mortgage Disclosure Act (HMDA) data from 2019 through the first three quarters of 2023. The report found that borrowers with lower credit scores were more likely to pay discount points, and that discount points were especially prevalent among Federal Housing Administration (FHA) borrowers with low credit scores. This indicates that lenders may be using discount points to lower borrowers' monthly payments and debt-to-income ratio, which is one of the measurements lenders use to assess a borrower's ability to repay in order to qualify for a mortgage. Nearly 77 percent of FHA borrowers with credit scores below 640 purchased discount points, while 65 percent of all FHA borrowers paid discount points.

Discount points were most common among borrowers with cash-out refinances, with 87 percent of those borrowers in September 2023 paying discount points, up from 61 percent in January 2021. Nearly 61 percent of borrowers with home purchase loans and 58 percent of borrowers with non-cash-out refinance loans also paid discount points in September 2023, up from 31 and 36 percent in 2021, respectively. Borrowers with cash-out refinances also paid a greater number of discount points. The median amount of discount points in the 2023 quarterly data was 2.1 points for cash-out refinance loans, 1.1 points for non-cash-out refinances, and 1.0 point for home purchase loans.

HMDA data are the most comprehensive source of publicly available information on the U.S. mortgage market. In addition to submitting annual application-level data, the largest mortgage lenders must submit quarterly HMDA data to their regulators. Aggregate statistics from the

quarterly data are publicly available in the HMDA quarterly graphs.

What You Need to Do:

Informational; please share with interested team members.

FFIEC: 2024 Guide to HMDA Reporting: Getting It Right! (May 15, 2024)

Link

https://www.ffiec.gov/hmda/guide.htm

Text

The Guide is a valuable resource for assisting all institutions in their HMDA reporting. It includes a summary of responsibilities and requirements, directions for assembling the necessary tools, and instructions for reporting HMDA data.

What You Need to Do:

Very important resource; please share with HMDA-responsible team members.

CFPB: Interpretive Rule "Buy Now, Pay Later" (May 22 2024)

Link

https://files.consumerfinance.gov/f/documents/cfpb_bnpl-interpretive-rule_2024-05.pdf

Text

The Consumer Financial Protection Bureau (CFPB) issued this interpretive rule to address the applicability of subpart B of Regulation Z to lenders that issue digital user accounts used to access credit, including to those lenders that market loans as "Buy Now, Pay Later" (BNPL). This interpretive rule describes how these lenders meet the criteria for being "card issuers" for purposes of Regulation Z. Such lenders that extend credit are also "creditors" subject to subpart B of Regulation Z, including those provisions governing periodic statements and billing disputes.

This interpretive rule is applicable as of July 30, 2024. Comments must be received by August 1, 2024.

SUPPLEMENTARY INFORMATION:

Executive Summary

Over the past three years, the CFPB has extensively analyzed lenders marketing their loans as "Buy Now, Pay Later." This includes a major study published in 2022, insights from supervisory examinations, and other market monitoring and investigation. Although market participants' loan offerings vary in this lending sector, the CFPB is publishing this interpretive rule to clarify existing obligations for market participants with specific business practices.

This interpretive rule's legal analysis states that lenders that issue digital user accounts that consumers use from time to time to access credit products to purchase goods and services are "card issuers" under Regulation Z, including when those products are marketed as Buy Now, Pay Later (BNPL). Such lenders are "card issuers" because such digital user accounts are "credit cards" under Regulation Z. Traditional BNPL products are closed-end loans payable in four or fewer installments without a finance charge, used to make purchases on credit. Consequently, BNPL loans are subject to some, but not all, of Regulation Z's credit card regulations.

Digital user accounts that consumers use to access BNPL credit mimic conventional credit cards. They meet the regulatory definition of "credit cards" as defined at 12 CFR 1026.2(a)(15)(i). Lenders that issue such digital user accounts are "card issuers" as defined at 12 CFR 1026.2(a)(7) and "creditors" for purposes of subpart B of Regulation Z, as defined at 12 CFR 1026.2(a)(17)(iii). However, traditional BNPL products do not meet the definition of "open-end credit" as defined at 12 CFR 1026.2(a)(20) or of a "credit card account under an open-end (not home-secured) consumer

credit plan" as defined at 12 CFR 1026.2(a)(15)(ii).

Accordingly, lenders that issue digital user account to access BNPL credit are subject to the regulations appearing in subpart B of Regulation Z, including, most importantly, provisions governing credit card dispute and refund rights. Although subpart B is labeled "Open-End Credit," 12 CFR 1026.2(a)(17)(iii) specifically states that subpart B also applies to credit that is not open end if, as with BNPL, the credit is not subject to a finance charge and is not payable by written agreement in more than four installments. This is the case because Congress expressly instructed the Bureau to apply open-end credit regulations to this form of credit that is not open end. The Truth in Lending Act (TILA) says that "the Bureau shall, by regulation, apply [open-end credit] requirements to [card issuers that extend credit with no finance charge that is payable in four or fewer installments], to the extent appropriate, even though the requirements [of the open-end credit provisions] are by their terms applicable only to creditors offering open-end credit plans."

Lenders that issue digital user accounts to access BNPL credit are generally not subject to the credit card regulations appearing in subpart G of Regulation Z (e.g., penalty fee limits and ability-to-repay requirements).

Background

Since the mid-2010s, a financing method marketed as "Buy Now, Pay Later" (BNPL) has rapidly gained popularity as an alternative to conventional credit cards in the United States and abroad. While variations of the product exist, for this interpretive rule, BNPL refers to a consumer loan for a retail transaction that is repaid in four (or fewer) interest-free installments and does not otherwise impose a finance charge. The loan generally requires an initial down payment of 25 percent, followed by three additional installments due every two weeks.

BNPL lenders currently acquire customers primarily through two channels: the merchant partner acquisition model and the app-driven acquisition model. In the merchant partner acquisition model, BNPL lenders typically establish contracts with online merchants to offer their BNPL product as a payment option on the merchant's website or mobile app checkout page. The BNPL lenders provide merchants with the necessary digital code to integrate or embed access to the BNPL product into the merchant websites or mobile apps. Such digital code or other integrations are referred to in this interpretive rule as "integrations."

In the app-driven acquisition model, which is less common but rapidly expanding, consumers use the BNPL lender's own website or mobile app directly to create a digital user account to access the BNPL product. Once activated by the provider, the consumer can use their digital user account through the BNPL website or mobile app to access credit and make purchases directly with partner merchants. For non-partner merchants, the BNPL lender enables the payment part of the credit process by issuing a single-use virtual card to the consumer, normally through an issuer processor and a bank partner. The consumer then typically has 24 hours to complete their purchase directly with the merchant, using the virtual card.

In addition, BNPL lenders may issue credit through other methods, such as in-store or through browser extensions. These methods generally operate the same as the acquisition methods described above, allowing the consumer to access credit with their BNPL digital user account to make purchases either through the merchant's website or through the issuance of a single-use virtual card.

Regardless of how consumers access BNPL, a BNPL digital user account is activated when a consumer first accesses BNPL credit, similar to how a virtual credit card number for a traditional

credit card account is issued at the same time a consumer opens the credit card account online and makes their first purchase on the card. These digital user accounts are secure, personal profiles that the BNPL provider activates for a consumer, enabling the consumer to access and utilize BNPL credit. Once a digital user account is activated, the consumer can then immediately use their BNPL digital user account on an ongoing basis to access credit to make additional purchases. BNPL providers typically inform consumers of their "amount available to spend," similar to a credit limit for conventional credit cards, and offer a frictionless borrowing process allowing consumers to rapidly access the BNPL credit.

A significant and increasing number of Americans who purchase goods and services on credit do so with BNPL credit instead of conventional credit cards. According to a recent CFPB Making Ends Meet survey, 17 percent of consumers with a credit record made at least one purchase using BNPL between February 2021 and February 2022. And data from five leading BNPL lenders reflect that originations have increased from $2 billion in 2019 to over $24 billion in 2021. BNPL borrowers also increased their repeat usage during this timeframe. The data reveal that the average number of BNPL loans taken out by BNPL consumers from a single lender each quarter rose from 1.9 to 2.8. The percentage of BNPL borrowers with more than five loans per quarter also increased, from 6.3 percent to 15.5 percent.

BNPL is popular among a broad range of consumers, but certain groups have shown a significantly higher likelihood of using BNPL. These groups include Black, Hispanic, and female consumers, as well as consumers with an annual household income between $20,001– $50,000 and consumers under the age of 35. In comparison to non-BNPL borrowers, BNPL borrowers tend to have higher levels of debt, carry balances on their conventional credit cards, have delinquencies on traditional credit products, and make use of higher-cost financial services like payday loans, pawn, and overdraft. BNPL borrowers are also more likely to use other credit products like conventional credit cards, personal loans, and student loans, but have less liquidity and savings compared to non-BNPL borrowers.

Consumers often use BNPL offerings as an alternative to conventional credit cards, and the two share many similarities. Both combine payment processing and credit services. Both charge transaction fees to merchants and are extensively used for retail transactions. And consumers often use these two payment methods in a similar manner. In fact, often when a consumer is making purchases online from a merchant's website, the only options for paying on credit consist of conventional credit cards and BNPL, which are presented next to each other as alternatives.

The CFPB has been closely monitoring the BNPL market by issuing reports based on collected BNPL data and supervising certain BNPL lenders. In December 2021, the CFPB issued mandatory data collection orders to five large BNPL lenders to understand market trends and practices. These responses formed the basis of the September 2022 report "Buy Now Pay Later: Market Trends and Consumer Impacts," which highlighted industry growth, as well as consumer benefits and risks associated with BNPL loans. The report noted, among other findings, a lack of standardized disclosures and challenges in resolving disputes. In March 2023, the CFPB published "Consumer Use of Buy Now, Pay Later," which used data from the annual Making Ends Meet survey and credit bureaus to identify demographic and other characteristics of BNPL borrowers. In March 2024, the CFPB released its "Consumer Response Annual Report" for 2023, which noted issues consumers faced with merchants regarding BNPL, such as non-receipt of items and challenges in canceling loans. Through monitoring consumer complaints, the CFPB has further refined its understanding of the BNPL market. The CFPB continues to observe the industry and monitor new market and product trends.

Recognizing the importance of adequate consumer protections for BNPL loans, the CFPB is issuing this interpretive rule so that BNPL providers understand their obligations. As this interpretive rule explains, lenders that issue BNPL digital user accounts are "card issuers" under Regulation Z because the digital user accounts they issue constitute "credit cards" under Regulation Z. The term "credit card"— which, as defined by TILA and Regulation Z, includes the term "other credit device" or "other single credit device" used for the purpose of obtaining credit—encompasses digital user accounts that consumers can use through websites, mobile apps, browser extensions, or integrations with merchant websites or mobile apps to access BNPL credit for the purchase of goods and services. The CFPB also affirms through this interpretive rule that BNPL lenders that extend credit— even though that credit is not subject to a finance charge and is not payable by written agreement in more than four installments—are creditors subject to subpart B of Regulation Z, including those provisions governing cost of credit disclosures and billing disputes.

Legal Analysis

This interpretive rule discusses the application of subpart B of Regulation Z to lenders that issue digital user accounts that consumers use from time to time to access credit, which includes those lenders that market their loans as "Buy Now, Pay Later." Regulation Z implements the Truth in Lending Act (TILA). The purpose of TILA is to "assure a meaningful disclosure of credit terms so that the consumer will be able to compare more readily the various credit terms available to him and avoid the uninformed use of credit, and to protect the consumer against inaccurate and unfair credit billing and credit card practices." Accordingly, TILA and its implementing regulation generally establish uniform methods for calculating the cost of credit, require meaningful disclosure of those costs to consumers, and provide standardized mechanisms for resolving credit billing disputes.

Although subpart B primarily covers open-end credit, many of its provisions apply more broadly, including to closed-end credit, under certain circumstances. Certain subpart B provisions, such as those governing cardholder liability, apply to any "card issuer," regardless of the type of credit offered. Regulation Z defines "card issuer" as "a person that issues a credit card or that person's agent with respect to the card." Additionally, "card issuers" are considered "creditors" for purposes of subpart B if they also extend "either open-end credit or credit that is not subject to a finance charge and is not payable by written agreement in more than four installments." Such "creditors" are broadly subject to the provisions of subpart B, including those governing disclosures and billing dispute resolution. Thus, BNPL lenders that issue a credit card as defined by Regulation Z are card issuers for purposes of the regulation. And as they also extend credit, even though that credit is not subject to a finance charge and not payable by written agreement in more than four installments, those BNPL lenders are creditors subject to the provisions of subpart B.

The definition of "credit card" in TILA and Regulation Z is not limited to a plastic or metal embossed physical card. While the term certainly includes those, it also includes archaic forms of credit devices like plates and coupon books, and non-physical credit devices like account numbers, including virtual credit cards where the account number itself is the "credit card." In creating these definitions, Congress understood the need for flexibility to cover evolving types of credit devices, reflecting the rapid advancement of credit mechanisms at the time of enactment. TILA defines "credit card" as "any card, plate, coupon book or other credit device existing for the purpose of obtaining money, property, labor, or services on credit." Regulation Z similarly defines "credit card" as "any card, plate, or other single credit device that may be used from time to time to obtain credit."

The CFPB interprets the terms "other credit device" and "other single credit device" found within the TILA and Regulation Z definitions of credit card to include a BNPL digital user account that a consumer can use through websites, mobile apps, browser extensions, or integrations with merchant websites or mobile apps to access BNPL credit, to the extent the user account is used to draw, transfer, or authorize the draw or transfer of credit in the course of authorizing, settling, or otherwise completing transactions to obtain goods or services. The broad catch-all terms "other credit device" and "other single credit device" are not defined by TILA and Regulation Z. However, this interpretation is consistent with the ordinary meaning and historical context of the words.

The CFPB's interpretation flows from the ordinary meaning of the word "device." Merriam-Webster Dictionary contains several definitions for the word "device," including "something devised or contrived: such as . . . [a] plan, procedure, [or] technique . . . [or] a piece of equipment or a mechanism designed to serve a special purpose or perform a special function." Similarly, Oxford English Dictionary defines "device" in part to mean "[t]he result of contriving; something devised or framed by art or inventive power; an invention, contrivance; esp. a mechanical contrivance (usually of a simple character) for some particular purpose." These definitions indicate that the ordinary meaning of "device" is broad and incorporates a wide range of mechanisms, tools, or procedures specifically designed or contrived to achieve a particular purpose.

The CFPB's interpretation is also consistent with use of the word "device" broadly in other contexts. For example, both the CFPB, and the Federal Reserve Board (Board) before it, have interpreted "access device" in Regulation E to include such nonphysical devices as personal identification numbers (PINs), telephone transfer and bill payment codes, and other means that may be used by a consumer to initiate an electronic fund transfer.

The CFPB's interpretation is also consistent with Congress' intent to define the terms "other credit device" and "credit card" broadly. As a preliminary matter, courts have routinely held that, as a remedial statute, TILA should be interpreted expansively in favor of the consumer. More specifically, as courts have recognized, the inclusion of the phrase "other credit device" in the statutory definition of "credit card" indicates that Congress intended the term "credit card" to encompass a wider scope than its customary usage. Congress initially enacted the definitions in 1970 at the height of a rapid evolution of credit devices, which first included now-archaic credit devices such as coins and plates before the use of conventional credit cards became widespread. In this context, Congress appears to have intended a flexible and comprehensive definition of "credit card" that could encompass both the entire range of existing credit devices and also those "other credit devices" that might not yet exist.

Indeed, the Board, which previously had jurisdiction over Regulation Z, adopted a similarly broad interpretation of "other single credit device" in 2010. The Board clarified in Official Staff Interpretations of Regulation Z that nonphysical devices—in that case, account numbers—could be considered "credit cards" under the definition. The Board explained in the rulemaking preamble that while Congress did not generally intend to treat all account numbers as credit cards—for example, where credit is transferred into a consumer's asset account—it would be inconsistent with Congressional intent not to do so when the account number could be used to access credit for the purchase of goods and services. As an example, the Board provided a hypothetical scenario in which an open-end credit account was designed for online purchases, functioning like a conventional credit card account, but only accessible with an account number. In such circumstances, the Board stated, it believed that TILA's credit card protections should apply.

This analysis applies equally in the BNPL context. BNPL is a product primarily designed for the online purchase of goods and services and a digital BNPL user account functions like a conventional credit card. Consumers can use their BNPL digital user accounts through BNPL websites, mobile apps, browser extensions, or integrations with merchant websites or mobile apps to access credit for purchases. Given its similarities to conventional credit cards, a consumer's BNPL digital user account is among the types of "credit devices" that Congress would have had in mind in enacting TILA.

In order for a device to constitute a credit card under Regulation Z, it must be usable from time to time to obtain credit. The commentary to Regulation Z interprets the term "time to time" to "involve[ ] the possibility of repeated use of a single device." The CFPB interprets the phrase "usable from time to time" to cover a consumer's BNPL digital user account that is issued as part of a business model designed for repeat use that can be used through websites, mobile apps, browser extensions, or integrations with merchant websites or mobile apps, to access credit for the purchase of goods and services. Like conventional credit cards, the BNPL business model is designed around the repeat use of a digital user account to make real-time purchases on credit. The CFPB therefore interprets the term "credit cards" to include such digital credit devices for purposes of TILA and Regulation Z.

Of course, not all digital user accounts are credit cards. However, digital user accounts with the purpose of giving consumers access to credit from time to time in the course of completing transactions to purchase goods or services, including those marketed as BNPL, meet the regulatory definition of "credit card." When consumers use them through websites, mobile apps, browser extensions, and integrations, they get credit in the course of completing transactions to pay for a product at check-out or even in physical stores. And these digital user accounts "exist for [that] purpose." They are, effectively, digital replacements for conventional credit cards, and consumers use them in the same way as conventional credit cards. The statutory and regulatory definitions of "credit card" are broad enough to capture new, technologically advanced "devices" designed to mimic the core features of conventional credit cards.

Consequently, BNPL providers issuing the credit cards (and their agents with respect to the credit card) are "card issuers" for purposes of Regulation Z. Additionally, as noted above, a "card issuer" is a "creditor" for purposes of subpart B if it extends credit, even though that credit is not subject to a finance charge and not payable by written agreement in more than four installments. Thus, BNPL lenders that issue credit cards are "creditors" for purposes of subpart B and must comply with its requirements, including the provisions related to disclosures and billing dispute resolution.

What You Need to Do:

Review, and implement, as applicable.

CFPB: Small Business Lending under the Equal Credit Opportunity Act (Regulation B); Extension of Compliance Dates (June 25, 2024)

Link

https://www.govinfo.gov/content/pkg/FR-2024-07-03/pdf/2024-14396.pdf

Text

In light of court orders in ongoing litigation, the Consumer Financial Protection Bureau is amending Regulation B to extend the compliance dates set forth in its 2023 small business lending rule and to make other date-related conforming adjustments.

This interim final rule is effective August 2, 2024.

SUPPLEMENTARY INFORMATION:

Background

In 2010, Congress passed the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act). Section 1071 of that Act amended the Equal Credit Opportunity Act (ECOA) to require that financial institutions collect and report to the CFPB certain data regarding applications for credit for women-owned, minority-owned, and small businesses. Section 1071's statutory purposes are to (1) facilitate enforcement of fair lending laws, and (2) enable communities, governmental entities, and creditors to identify business and community development needs and opportunities of women-owned, minority-owned, and small businesses.

Section 1071 directs the CFPB to prescribe such rules and issue such guidance as may be necessary to carry out, enforce, and compile data pursuant to section 1071. On March 30, 2023, the CFPB issued a final rule to implement section 1071 by adding subpart B to Regulation B (2023 final rule). The 2023 final rule was published in the *Federal Register* on May 31, 2023. Further details about section 1071 and this rulemaking can be found in the preamble to the 2023 final rule.

Subsequently, some lenders filed challenges to the 2023 final rule in the United States District Court for the Southern District of Texas. On July 31, 2023, the court issued an order that preliminarily enjoined the CFPB from implementing and enforcing the 2023 final rule against plaintiffs and their members pending the Supreme Court's reversal of *Community Financial Services Association of America, Ltd. v. CFPB*, 51 F.4th 616 (5th Cir. 2022), cert. granted, 143 S. Ct. 978 (2023) (CFSA), a trial on the merits, or until further court order. The court's order also stayed all deadlines for compliance with the requirements of the 2023 final rule for plaintiffs and their members pending the outcome of the Supreme Court case. The Texas court ordered that, in

the event of a reversal in the Supreme Court case, the CFPB extend plaintiffs' and their members' deadlines for compliance with the 2023 final rule to compensate for the period stayed. Following motions to intervene by a number of other parties, on October 26, 2023, the Texas court extended the terms of its order to all covered financial institutions (i.e., issued a nationwide stay).

On May 16, 2024, the Supreme Court reversed the Fifth Circuit's ruling in CFSA.

Summary of the Interim Final Rule

In this interim final rule, the CFPB is extending the compliance dates set forth in the 2023 final rule and making conforming adjustments. Consistent with existing court orders, the compliance dates are being extended 290 days to compensate for the period the rule was stayed (July 31, 2023 to May 16, 2024). Thus, covered financial institutions must begin collecting data as follows:

TABLE 1 – COMPLIANCE DATES AND FILING DEADLINES

Compliance Tier	Original Compliance Date	New Compliance Date	First Filing Deadline
Highest volume lenders	Oct 1, 2024	July 18, 2025	June 1, 2026
Moderate volume lenders	April 1, 2025	Jan 16, 2026	June 1, 2027
Smallest volume lenders	Jan 1, 2026	Oct 18, 2026	June 1, 2027

Covered financial institutions are permitted to continue using their small business originations from 2022 and 2023 to determine their compliance tier, or they may use their originations from 2023 and 2024. Covered financial institutions are permitted to begin collecting protected demographic data required under the 2023 final rule 12 months before their new compliance date, in order to test their procedures and systems. As illustrated above, the deadline for submitting small business lending data will remain June 1 following the calendar year for which data are collected. Finally, the CFPB is updating its grace period policy statement to reflect the revised compliance dates. The CFPB seeks comment on this interim final rule.

Discussion of the Final Rule

As discussed above, the court in *Texas Bankers Association v. CFPB* directed the CFPB to extend the compliance dates set forth in the 2023 final rule to compensate for the period the rule was stayed pending the Supreme Court's decision in CFSA. To facilitate compliance across all covered financial institutions, the CFPB is using July 31, 2023 as the base date to calculate the length of the compliance date extension for all covered financial institutions, including the initial plaintiffs and their members as well as the intervening parties. The CFPB is extending the 2023 final rule's compliance dates by 290 days (i.e., the number of days that elapsed between the court's July 31, 2023 order and the Supreme Court's decision in CFSA on May 16, 2024).

Changes to Compliance Date Provisions

The 2023 final rule's compliance dates are set forth in § 1002.114(b). That section looks to a financial institution's volume of covered credit transactions for small businesses in each of

calendar years 2022 and 2023 to determine the applicable compliance date. The 2023 final rule provided that covered financial institutions that originated at least 2,500 covered transactions in both years were required to comply with the requirements of the 2023 final rule beginning October 1, 2024 (sometimes referred to as Tier 1 institutions). Covered financial institutions not in Tier 1 that originated at least 500 covered transactions in both years were required to comply beginning April 1, 2025 (Tier 2), and covered financial institutions not in Tier 1 or Tier 2 that originated at least 100 covered transactions in both years were required to comply beginning January 1, 2026 (Tier 3). The 2023 final rule also provided that a financial institution that did not originate at least 100 covered transactions in both 2022 and 2023 but that subsequently originates at least 100 such transactions in two consecutive calendar years must comply with the rule in accordance with § 1002.105(b), but in any case no earlier than January 1, 2026.

In this interim final rule, the CFPB is extending each of the compliance dates set forth in § 1002.114(b) by 290 days. Thus, Tier 1 institutions now have a compliance date of July 18, 2025, Tier 2 institutions now have a compliance date of January 16, 2026, and Tier 3 institutions now have a compliance date of October 18, 2026. Likewise, institutions that did not originate at least 100 covered transactions in 2022 and 2023 but subsequently do in two consecutive calendar years are not required to comply with the rule until October 18, 2026 at the earliest. The CFPB is making corresponding updates throughout the commentary accompanying § 1002.114(b), which provide additional guidance and examples regarding compliance dates. The CFPB is also revising comments 105(b)–2 and –6 and 109(b)–1, which involve examples of data collection occurring in years affected by the extended compliance dates in this interim final rule.

Voluntary Early Collection of Protected Demographic Data

Section 1002.114(c) addresses several transitional issues. Section 1002.114(c)(1) permits financial institutions to collect protected demographic information required under the 2023 final rule from small business applicants beginning 12 months prior to its compliance date. As this provision does not list any compliance dates specifically, no revisions are needed. Thus, a Tier 1 institution is permitted to begin collecting protected demographic information on or after July 18, 2024; a Tier 2 institution may begin on or after January 16, 2025; and a Tier 3 institution may begin on or after October 18, 2025, in order to test their procedures and systems for compiling and maintaining this information in advance of actually being required to collect and subsequently report it to the CFPB.

Alternative Period for Counting Covered Originations To Determine Compliance Tier

The CFPB is adopting new § 1002.114(c)(3), which permits (but does not require) a financial institution to use its originations of covered credit transactions in each of calendar years 2023 and 2024, rather than those in 2022 and 2023, to determine its compliance date. Financial institutions may use whichever set of dates they prefer (i.e., 2022 and 2023, or 2023 and 2024). Existing comment 114(b)–4 provides examples illustrating how a financial institution uses its originations in 2022 and 2023 to determine its compliance tier; new comment 114(b)– 4.viii illustrates using 2023 and 2024 originations to determine compliance tier.

Determining Compliance Dates for Financial Institutions That Do Not Collect Information Sufficient To Determine Small Business Status

Section 1002.114(c)(2) provides that a financial institution that is unable to determine the number of covered credit transactions it originated in 2022 and 2023 for purposes of determining

its compliance tier is permitted to use any reasonable method to estimate its originations to small businesses for either or both of 2022 and 2023. Existing comment 114(c)–5 lists several reasonable methods a financial institution may use to estimate its originations.

Pursuant to new § 1002.114(c)(3), which permits a financial institution to use its originations of covered credit transactions in each of calendar years 2023 and 2024 to determine its compliance date, financial institutions are likewise permitted to use any reasonable method to estimate their originations for either or both of 2023 and 2024. The CFPB is revising comment 114(c)–5 to make this clear and adding new comment 114(c)–6.vii to provide an example.

Deadline for Annual Data Submissions

Section 1002.109(a)(1) provides that covered financial institutions must submit their small business lending application registers to the CFPB on or before June 1 following the calendar year for which the data are compiled and maintained. As this provision does not list any compliance dates specifically, no revisions are needed. Thus, Tier 1 institutions will make their first data submission by June 1, 2026; Tier 2 and Tier 3 by June 1, 2027.

Grace Period Policy Statement

In the 2023 final rule, the CFPB adopted a 12-month grace period during which the CFPB—for covered financial institutions under its supervisory and enforcement jurisdiction—would not intend to assess penalties for errors in data reporting, and would intend to conduct examinations only to diagnose compliance weaknesses, to the extent that these institutions engaged in good faith compliance efforts. The Grace Period Policy Statement set forth in the 2023 final rule explained the CFPB's reasons for adopting such a grace period along with how the CFPB intended to implement such a grace period. The CFPB is updating this policy statement to reflect the new compliance dates set forth in this interim final rule.

The following discussion explains how the CFPB intends to exercise its supervisory and enforcement discretion for the first 12 months of data collected after a covered financial institution's initial compliance date.

With respect to covered financial institutions subject to the CFPB's supervisory or enforcement jurisdiction that make good faith efforts to comply with the 2023 final rule, the CFPB intends to provide a grace period to reflect the new compliance dates as follows:

TABLE 2 – GRACE PERIOD

Financial institutions covered by the grace period	Dates covered by the grace period
Financial institutions with a compliance date specified in § 1002.114(b)(1) (i.e., Tier 1 institutions), as well as any financial institutions that make a voluntary submission for the first time for data collected in 2025	The data collected in 2025 (from July 18, 2025 through December 31, 2025) as well as a portion of data collected in 2026 (from January 1, 2026 through July 17, 2026).
Financial institutions with a compliance date specified in § 1002.114(b)(2) (i.e., Tier 2 institution), as well as any financial institutions that make a voluntary submission for the first time for data collected in 2026.	The data collected in 2026 (from January 16, 2026 through December 31, 2026) as well as a portion of data collected in 2027 (from January 1, 2027 through January 15, 2027).

TABLE 2 – GRACE PERIOD	
Financial institutions covered by the grace period	**Dates covered by the grace period**
Financial institutions with a compliance date specified in § 1002.114(b)(3) (i.e., Tier 3 institution), as well as any financial institutions that make a voluntary submission for the first time for data collected in 2027.	The data collected in 2026 (from October 18, 2026 through December 31, 2026) as well as a portion of data collected in 2027 (from January 1, 2027 through October 17, 2027).

As discussed in the 2023 final rule, the CFPB believes that a 12-month grace period for each compliance tier will give institutions time to diagnose and address unintentional errors without the prospect of penalties for inadvertent compliance issues, and may ultimately assist other covered financial institutions, especially those in later compliance tiers, in identifying best practices. While the CFPB anticipates that financial institutions in each compliance tier are capable of fully preparing to comply with the 2023 final rule by their respective new compliance dates, it views this grace period as enabling deliberate and thoughtful compliance with the rule, while still providing important data regarding small business lending as soon as practical.

During the grace period, if the CFPB identifies errors in a financial institution's initial data submissions, it does not intend to require data resubmission unless data errors are material. Further, the CFPB does not intend to assess penalties with respect to unintentional and good faith errors in the initial data submissions. Any examinations of these initial data submissions will be diagnostic and will help to identify compliance weaknesses. However, errors that are not the result of good faith compliance efforts by financial institutions, especially attempts to discourage applicants from providing data, will remain subject to the CFPB's full supervisory and enforcement authority, including the assessment of penalties.

The CFPB believes that the grace period covering the initial data submissions will provide financial institutions an opportunity to identify any gaps in their implementation of the 2023 final rule and make improvements in their compliance management systems for future data submissions. In addition, a grace period will permit the CFPB to help financial institutions identify errors and, thereby, self-correct to avoid such errors in the future. The CFPB can also use data collected during the grace period to alert financial institutions of common errors and potential best practices in data collection and submissions under this rule.

CFPA Section 1022(b) Analysis

Overview

In developing the interim final rule, the CFPB has considered the potential benefits, costs, and impacts as required by section 1022(b)(2) of the Consumer Financial Protection Act of 2010 (CFPA). Section 1022(b)(2) calls for the CFPB to consider the potential benefits and costs of a regulation to consumers and covered persons, including the potential reduction of consumer access to consumer financial products or services, the impact on depository institutions and credit unions with $10 billion or less in total assets as described in section 1026 of the CFPA, and the impact on consumers in rural areas. In addition, section 1022(b)(2)(B) directs the CFPB to consult with appropriate prudential regulators or other Federal agencies, regarding consistency with the objectives those agencies administer. The CFPB has accordingly consulted with the appropriate prudential regulators and other Federal agencies regarding consistency with any prudential,

market, or systemic objectives administered by these agencies.

In this interim final rule, the CFPB is extending by 290 days the compliance dates set forth in the 2023 small business lending rule and making several conforming adjustments. Thus, covered financial institutions with the highest volume of small business originations (Tier 1) must begin collecting data by July 18, 2025; moderate-volume institutions (Tier 2) by January 16, 2026; and the smallest volume institutions (Tier 3) by October 18, 2026. Covered financial institutions are permitted to continue using their small business originations from 2022 and 2023 to determine their compliance tier, or instead they may use their originations from 2023 and 2024.

The CFPB expects covered institutions to benefit from the extension of the compliance dates, but expects that the impacts of this interim final rule on covered institutions are small relative to the overall impacts of the 2023 final rule it modifies. The CFPB additionally expects this interim final rule to have minimal impacts on small businesses, due to the long-term nature of the benefits of the 2023 final rule and an expectation that the 2023 final rule will have a limited effect on the cost of small business credit.

Data Limitation and Quantification of Benefits, Costs, and Impacts

The discussion below relies on information the CFPB has obtained from industry, other regulatory agencies, and publicly available sources. The CFPB provides estimates, to the extent possible, of the potential benefits, costs, and impacts to consumers and covered persons of this interim final rule given available data.

To estimate the number of depository institutions covered by the interim final rule, the CFPB relies in part on data from publicly available sources, such as the Federal Financial Institutions Examination Council's Reports on Condition of Income (Call Reports), the National Credit Union Administration's Call Reports, and data reported under the Community Reinvestment Act. As described in detail in part IX.E of the 2023 final rule, information on the cost of compliance is derived from the CFPB's previous Home Mortgage Disclosure Act rulemaking activities and a One-time Cost Survey the CFPB administered in 2020 as part of its small business lending rule development process.

There are limitations, such as limited comprehensive data on non-depository institutions potentially subject to the 2023 final rule and thus this interim final rule, and limited data on which to quantify benefits of the interim final rule with precision. The CFPB supplements the data sources described above with general economic principles and the CFPB's expertise in consumer financial markets. The CFPB qualitatively describes potential benefits, costs, and impacts where the ability to provide quantitative estimates are impacted by these limitations.

Baseline for Analysis

In evaluating the potential benefits, costs, and impacts of the interim final rule, the CFPB takes as a baseline Regulation B as amended by the 2023 final rule. Part IV above describes in detail the provisions of the 2023 final rule. The CFPB's analysis of the potential costs, benefits, and impacts of this interim final rule are relative to the original compliance dates and other requirements of the 2023 final rule.

Potential Benefits and Costs to Covered Persons and Small Businesses

1. Potential Benefits and Costs to Covered Persons

Based on the methodology used to determine coverage in the 2023 final rule, the CFPB expects about 100 financial institutions to be required to report in Tier 1, about 450 to be required to report in Tier 2, and about 2,000 to be required to report in Tier 3.

By extending the compliance dates by 290 days for all covered institutions, financial institutions will benefit by the delay in the expected costs of compliance with the 2023 final rule. The benefit from the compliance date extension will differ depending on whether the cost was expected to be "one-time" or "ongoing." Part IX.E of the 2023 final rule described two categories of cost that the CFPB expected covered financial institutions to incur. "One-time" costs refer to expenses that the financial institution will incur initially and only once to implement changes required to comply with the requirements of the rule. "Ongoing" costs are expenses incurred because of the ongoing reporting requirements of the rule, accrued on an annual basis.

The CFPB expects covered institutions to experience an annual ongoing cost of compliance in perpetuity. Therefore, extending the compliance dates by 290 days potentially saves financial institutions up to 290 days in expected annual compliance costs. In the 2023 rule, the CFPB detailed its methodology and estimates of this annual ongoing cost for institutions of different levels of complexity in their processes for collecting, checking, and reporting data on applications for small business credit. These "types" were Type A (least complex), Type B (medium complexity), and Type C (most complex) and were related to small business credit application volume. The 2023 final rule gave estimates of compliance costs for representative institutions of each type as well as the market-level estimate for all complying institutions.

The CFPB estimated that, per application for small business credit, Type A institutions would incur $83 in annual ongoing costs, Type B institutions would incur $100, and Type C institutions would incur $46. Based on the CFPB's estimates of application volumes for all institutions, the expected market level annual ongoing cost was between $310 and $330 million for depository institutions and $62.3 million for non-depository institutions. The CFPB expects covered financial institutions to avoid 290 days of ongoing costs due to the compliance date extension. Institutions will effectively receive this benefit at the time they would have originally been required to start collecting data. Thus, Tier 3 institutions will receive this benefit farther in the future than Tier 2 institutions, who will receive the benefit farther in the future than Tier 1 institutions. In present value terms, Tier 1 institutions will see a proportionally larger benefit compared to baseline, relative to Tier 2 and Tier 3 institutions.

This interim final rule does not change the nominal value of the onetime costs that will be incurred by covered institutions but does potentially delay the realization of those costs up to 290 days into the future for institutions in each compliance tier. Thus, the new one-time costs are the baseline one-time costs discounted by 290 days. The present value of the benefit associated with the interim final rule's impact on one-time costs is the difference between the baseline one-time costs and the new discounted costs.

The CFPB additionally expects that the compliance date extension and the associated flexibility in years of origination data that can be used to determine coverage would confer a benefit to covered institutions with the additional time to prepare for compliance relative to the baseline.

With the extension of the compliance dates by 290 days, this interim final rule delays the realization of these potential benefits to covered financial institutions. As enumerated in the 2023 final rule, benefits include more efficient fair lending review prioritization by regulators and the institutions' own use of small business lending data to better understand small business credit demand and the supply by their competitors.

2. Potential Benefits and Costs to Small Businesses

As with the 2023 final rule, this interim final rule will not directly impact consumers, as that term is defined by the Dodd-Frank Act. Some consumers will be impacted in their separate capacity as sole owners of small businesses covered by the rule. The CFPB has elected to consider the costs to small businesses from this interim final rule as it did in the 2023 final rule.

In part IX.F of the 2023 final rule, the CFPB described how small businesses would benefit from the impact of the rule on the enforcement of fair lending laws and on community development. In an environment with limited data sources on small business credit, the CFPB expects data collected under the rule to enable communities, governmental entities, and creditors to identify business and community development needs and opportunities for women-owned, minority-owned, and small businesses. The CFPB also expects data collected under the 2023 final rule to facilitate fair lending enforcement by Federal, State, and local enforcement agencies. Due to limitations on data and methodology, the CFPB mostly described these benefits qualitatively.

To the extent small businesses benefit in the above ways from the 2023 final rule, the extension of the compliance dates reduces the benefits accruing to small businesses by delaying the realization of these benefits. While compliance dates are extended by 290 days, Tier 1 financial institutions will be required to file data one year later than expected under the 2023 final rule (i.e., by June 1, 2026 rather than June 1, 2025). The CFPB expects that the benefits of the original rule will primarily begin with the publication of the data. Thus, small businesses' and financial institutions' realizations of the benefits arising from the 2023 final rule will likewise be delayed by at least one year, reducing the real net present value of these expected future benefits. The CFPB is unable to readily quantify the costs associated with delaying future benefits because the CFPB does not have the data to quantify all the benefits of the 2023 final rule.

The 2023 final rule also described that the CFPB expects financial institutions to pass on a portion of their annual ongoing costs to small business borrowers in the form of higher rates or fees. While, in general, the CFPB expects the magnitude of any passthrough to be a small portion of the total cost of the average loan to a small business applicant, extended compliance dates could benefit small business borrowers by delaying these increased costs.

3. Distribution of Small Business Impacts

The differences in the impacts of this interim final rule between different types of small businesses is likely to be small with only 290 days added to each of the compliance dates. Most of the distribution of benefits and costs are likely to be derived from whether small businesses are serviced by lenders in different compliance tiers and the difference in present discounted values.

Potential Impacts on Depository Institutions and Credit Unions With $10 Billion or Less in Total Assets, as Described in CFPA Section 1026

Using the methodology described in the 2023 final rule, the CFPB estimates that between 1,700 and 1,900 banks, savings associations, and credit unions with $10 billion or less in total assets will be affected by this interim final rule. The CFPB believes that the impacts of the interim final rule on these small depository institutions will be similar to those impacts on covered financial institutions as a whole, discussed above. These institutions would incur benefits from up to 290 fewer days in annual ongoing costs and the postponement of up to 290 days of one-time costs. They would also potentially benefit from additional time to develop software and other resources used to comply with the 2023 final rule.

Potential Impacts on Small Businesses' Access to Credit and on Small Businesses in Rural Areas

The CFPB does not expect this interim final rule to have a significant impact on small businesses' access to credit. In the 2023 final rule, the CFPB described how the likeliest effect of the rule on access to credit would be a small increase in interest rates or fees. This interim final rule shifts this potential effect by 290 days without any additional provisions that would affect credit access.

In part IX.H of the final rule, the CFPB described how existing data sources limited its ability to precisely estimate the number of financial institutions who serve rural areas who are covered under the 2023 final rule. The CFPB expects that 65 to 70 percent of rural bank and savings associations branches and 14 percent of rural credit union branches would be affected by the interim final rule using this methodology.

Small businesses in rural areas are expected to experience similar costs and benefits of small businesses more broadly. Small businesses in rural areas would experience a reduction in benefits via a postponement of the benefits of the 2023 final rule on fair lending enforcement and community development. These small businesses would also experience a benefit by the postponement of expected small increases in interest rates and fees.

Revised Regulatory Text

PART 1002 - EQUAL CREDIT OPPORTUNITY ACT (REGULATION B)

§ 1002.114 Effective date, compliance date, and special transitional rules.

* * * * *

(c) * * *

(3) **Alternative time period for determining compliance dates.** A financial institution is permitted to use its originations of covered credit transactions in each of calendar years 2023 and 2024 in lieu of calendar years 2022 and 2023 as specified in paragraphs (b) and (c)(2) of this section.

Revised Commentary

Revised Supplement I to Part 1002—Official Interpretations

* * * * *

Section 1002.105—Covered Financial Institutions and Exempt Institutions

* * * * *

105(b) Covered Financial Institution

1. ***Preceding calendar year.*** *The definition of covered financial institution refers to preceding calendar years. For example, in 2029, the two preceding calendar years are 2027 and 2028. Accordingly, in 2029, Financial Institution A does not meet the loan-volume threshold in § 1002.105(b) if did not originate at least 100 covered credit transactions for small businesses both during 2027 and during 2028.*

2. ***Origination threshold.*** *A financial institution qualifies as a covered financial institution based on total covered credit transactions originated for small businesses, rather than covered applications received from small businesses. For example, if in both 2026 and 2027, Financial Institution B received 105 covered applications from small businesses and originated 95 covered credit transactions for small businesses, then for 2028, Financial Institution B is not a covered financial institution.*

3. ***Counting originations when multiple financial institutions are involved in originating a covered credit transaction****. For the purpose of counting originations to determine whether a financial institution is a covered financial institution under § 1002.105(b), in a situation where multiple financial institutions are involved in originating a single covered credit transaction, only the last financial institution with authority to set the material terms of the covered credit transaction is required to count the origination.*

4. ***Counting originations after adjustments to the gross annual revenue threshold due to inflation.*** *Pursuant to § 1002.106(b)(2), every five years, the gross annual revenue threshold used to define a small business in § 1002.106(b)(1) shall be adjusted, if necessary, to account for inflation. The first time such an adjustment could occur is in 2030, with an effective date of January 1, 2031. A financial institution seeking to determine whether it is a covered financial institution applies the gross annual revenue threshold that is in effect for each year it is evaluating. For example, a financial institution seeking to determine whether it is a covered financial institution in 2032 counts its originations of covered credit transactions for small businesses in calendar years 2030 and 2031. The financial institution applies the initial $5 million threshold to evaluate whether its originations were to small businesses in 2030. In this example, if the small business threshold were increased to $5.5 million effective January 1, 2031, the financial institution applies the $5.5 million threshold to count its originations for small businesses in 2031.*

5. ***Reevaluation, extension, or renewal requests, as well as credit line increases and other requests for additional credit amounts.*** *While requests for additional credit amounts on an existing account can constitute a "covered application" pursuant to § 1002.103(b)(1), such requests are not counted as originations for the purpose of determining whether a financial institution is a covered financial institution pursuant to § 1002.105(b). In addition, transactions that extend, renew, or otherwise amend a transaction are not counted as originations. For example, if a financial institution originates 50 term loans and 30 lines of credit for small businesses in each of the preceding two calendar years, along with 25 line*

increases for small businesses in each of those years, the financial institution is not a covered financial institution because it has not originated at least 100 covered credit transactions in each of the two preceding calendar years.

6. ***Annual consideration.*** *Whether a financial institution is a covered financial institution for a particular year depends on its small business lending activity in the preceding two calendar years. Therefore, whether a financial institution is a covered financial institution is an annual consideration for each year that data may be compiled and maintained for purposes of subpart B of this part. A financial institution may be a covered financial institution for a given year of data collection (and the obligations arising from qualifying as a covered financial institution shall continue into subsequent years, pursuant to §§ 1002.110 and 1002.111), but the same financial institution may not be a covered financial institution for the following year of data collection. For example, Financial Institution C originated 105 covered transactions for small businesses in both 2027 and 2028. In 2029, Financial Institution C is a covered financial institution and therefore is obligated to compile and maintain applicable 2029 small business lending data under § 1002.107(a). During 2029, Financial Institution C originates 95 covered transactions for small businesses. In 2030, Financial Institution C is not a covered financial institution with respect to 2030 small business lending data, and is not obligated to compile and maintain 2030 data under § 1002.107(a) (although Financial Institution C may volunteer to collect and maintain 2030 data pursuant to § 1002.5(a)(4)(vii) and as explained in comment 105(b)–10). Pursuant to § 1002.109(a), Financial Institution C shall submit its small business lending application register for 2029 data in the format prescribed by the Bureau by June 1, 2030 because Financial Institution C is a covered financial institution with respect to 2029 data, and the data submission deadline of June 1, 2030 applies to 2029 data.*

7. ***Merger or acquisition - coverage of surviving or newly formed institution.*** *After a merger or acquisition, the surviving or newly formed financial institution is a covered financial institution under § 1002.105(b) if it, considering the combined lending activity of the surviving or newly formed institution and the merged or acquired financial institutions (or acquired branches or locations), satisfies the criteria included in § 1002.105(b). For example, Financial Institutions A and B merge. The surviving or newly formed financial institution meets the threshold in § 1002.105(b) if the combined previous components of the surviving or newly formed financial institution (A plus B) would have originated at least 100 covered credit transactions for small businesses for each of the two preceding calendar years. Similarly, if the combined previous components and the surviving or newly formed financial institution would have reported at least 100 covered transactions for small businesses for the year previous to the merger as well as 100 covered transactions for small businesses for the year of the merger, the threshold described in § 1002.105(b) would be met and the surviving or newly formed financial institution would be a covered institution under § 1002.105(b) for the year following the merger. Comment 105(b)–8 discusses a financial institution's responsibilities with respect to compiling and maintaining (and subsequently reporting) data during the calendar year of a merger.*

8. ***Merger or acquisition - coverage specific to the calendar year of the merger or acquisition.*** *The scenarios described below illustrate a financial institution's responsibilities specifically for data from the calendar year of a merger or acquisition. For purposes of these illustrations, an "institution that is not covered" means either an institution that is not a financial institution, as defined in § 1002.105(a), or a financial institution that is not a covered financial institution, as defined in § 1002.105(b).*

    i. ***Two institutions that are not covered financial institutions merge.*** *The surviving or newly formed institution meets all of the requirements necessary to be a covered financial institution. No data are required to be compiled, maintained, or reported for*

the calendar year of the merger (even though the merger creates an institution that meets all of the requirements necessary to be a covered financial institution).

ii. ***A covered financial institution and an institution that is not covered merge.*** *The covered financial institution is the surviving institution, or a new covered financial institution is formed. For the calendar year of the merger, data are required to be compiled, maintained, and reported for covered applications from the covered financial institution and is optional for covered applications from the financial institution that was previously not covered.*

iii. ***A covered financial institution and an institution that is not covered merge.*** *The institution that is not covered is the surviving institution and remains not covered after the merger, or a new institution that is not covered is formed. For the calendar year of the merger, data are required to be compiled and maintained (and subsequently reported) for covered applications from the previously covered financial institution that took place prior to the merger. After the merger date, compiling, maintaining, and reporting data is optional for applications from the institution that was previously covered for the remainder of the calendar year of the merger.*

iv. ***Two covered financial institutions merge.*** *The surviving or newly formed financial institution is a covered financial institution. Data are required to be compiled and maintained (and subsequently reported) for the entire calendar year of the merger. The surviving or newly formed financial institution files either a consolidated submission or separate submissions for that calendar year.*

9. ***Foreign applicability.*** *As discussed in comment 1(a)–2, Regulation B (including subpart B) generally does not apply to lending activities that occur outside the United States.*

10. ***Voluntary collection and reporting.*** *Section 1002.5(a)(4)(vii) through (x) permits a creditor that is not a covered financial institution under § 1002.105(b) to voluntarily collect and report information regarding covered applications from small businesses in certain circumstances. If a creditor is voluntarily collecting information for covered applications regarding whether the applicant is a minority-owned business, a women-owned business, and/or an LGBTQI+-owned business under § 1002.107(a)(18), and regarding the ethnicity, race, and sex of the applicant's principal owners under § 1002.107(a)(19), it shall do so in compliance with §§ 1002.107, 1002.108, 1002.111, 1002.112 as though it were a covered financial institution. If a creditor is reporting those covered applications from small businesses to the Bureau, it shall do so in compliance with §§ 1002.109 and 1002.110 as though it were a covered financial institution.*

* * * * *

Section 1002.109—Reporting of Data to the Bureau

* * * * *

109(b) Financial Institution Identifying Information

1. ***Changes to financial institution identifying information.*** *If a financial institution's information required pursuant to § 1002.109(b) changes, the financial institution shall provide the new information with the data submission for the collection year of the change. For example, assume two financial institutions that previously reported data under subpart B of this part merge and the surviving institution retained its Legal Entity Identifier but obtained a new TIN*

in February 2028. The surviving institution must report the new TIN with its data submission for its 2028 data (which is due by June 1, 2029) pursuant to § 1002.109(b)(5). Likewise, if that financial institution's Federal prudential regulator changes in February 2028 as a result of the merger, it must identify its new Federal prudential regulator in its annual submission for its 2028 data.

* * * * *

Section 1002.114—Effective Date, Compliance Date, and Special Transition Rules

114(b) Compliance Date

1. ***Application of compliance date.*** *The applicable compliance date in § 1002.114(b) is the date by which the covered financial institution must begin to compile data as specified in § 1002.107, comply with the firewall requirements of § 1002.108, and begin to maintain records as specified in § 1002.111. In addition, the covered financial institution must comply with § 1002.110(c) and (d) no later than June 1 of the year after the applicable compliance date. For instance, if § 1002.114(b)(2) applies to a financial institution, it must comply with §§ 1002.107 and 1002.108, and portions of § 1002.111, beginning January 16, 2026, and it must comply with § 1002.110(c) and (d), and portions of § 1002.111, no later than June 1, 2027.*

2. ***Initial partial year collections pursuant to § 1002.114(b).***

   i. *When the compliance date of July 18, 2025 specified in § 1002.114(b)(1) applies to a covered financial institution, the financial institution is required to collect data for covered applications during the period from July 18, 2025 to December 31, 2025. The financial institution must compile data for this period pursuant to § 1002.107, comply with the firewall requirements of § 1002.108, and maintain records as specified in § 1002.111. In addition, for data collected during this period, the covered financial institution must comply with §§ 1002.109 and 1002.110(c) and (d) by June 1, 2026.*

   ii. *When the compliance date of January 16, 2026 specified in § 1002.114(b)(2) applies to a covered financial institution, the financial institution is required to collect data for covered applications during the period from January 16, 2026 to December 31, 2026. The financial institution must compile data for this period pursuant to § 1002.107, comply with the firewall requirements of § 1002.108, and maintain records as specified in § 1002.111. In addition, for data collected during this period, the covered financial institution must comply with §§ 1002.109 and 1002.110(c) and (d) by June 1, 2027.*

   iii. *When the compliance date of October 18, 2026 specified in § 1002.114(b)(3) or (4) applies to a covered financial institution, the financial institution is required to collect data for covered applications during the period from October 18, 2026 to December 31, 2026. The financial institution must compile data for this period pursuant to § 1002.107, comply with the firewall requirements of § 1002.108, and maintain records as specified in § 1002.111. In addition, for data collected during this period, the covered financial institution must comply with §§ 1002.109 and 1002.110(c) and (d) by June 1, 2027.*

3. ***Informal names for compliance date provisions.*** *To facilitate discussion of the compliance dates specified in § 1002.114(b)(1), (2), and (3), in the official commentary and any other documents referring to these compliance dates, the Bureau adopts the following informal simplified names. Tier 1 refers to the cohort of covered financial institutions that have a compliance date of July 18, 2025 pursuant to § 1002.114(b)(1). Tier 2 refers to the cohort of*

covered financial institutions that have a compliance date of January 16, 2026 pursuant to § 1002.114(b)(2). Tier 3 refers to the cohort of covered financial institutions that have a compliance date of October 18, 2026 pursuant to § 1002.114(b)(3).

4. ***Examples.*** *The following scenarios illustrate how to determine whether a financial institution is a covered financial institution and which compliance date specified in § 1002.114(b) applies. Unless otherwise indicated, in each example the financial institution has chosen to use its originations in 2022 and 2023 (rather than 2023 and 2024 as permitted by § 1002.114(c)(3)) to determine its initial compliance tier.*

   i. Financial Institution A originated 3,000 covered credit transactions for small businesses in calendar year 2022, and 3,000 in calendar year 2023. Financial Institution A is in Tier 1 and has a compliance date of July 18, 2025.

   ii. Financial Institution B originated 2,000 covered credit transactions for small businesses in calendar year 2022, and 3,000 in calendar year 2023. Because Financial Institution B did not originate at least 2,500 covered credit transactions for small businesses in each of 2022 and 2023, it is not in Tier 1. Because Financial Institution B did originate at least 500 covered credit transactions for small businesses in each of 2022 and 2023, it is in Tier 2 and has a compliance date of January 16, 2026.

   iii. Financial Institution C originated 400 covered credit transactions to small businesses in calendar year 2022, and 1,000 in calendar year 2023. Because Financial Institution C did not originate at least 2,500 covered credit transactions for small businesses in each of 2022 and 2023, it is not in Tier 1, and because it did not originate at least 500 covered credit transactions for small businesses in each of 2022 and 2023, it is not in Tier 2. Because Financial Institution C did originate at least 100 covered credit transactions for small businesses in each of 2022 and 2023, it is in Tier 3 and has a compliance date of October 18, 2026.

   iv. Financial Institution D originated 90 covered credit transactions to small businesses in calendar year 2022, 120 in calendar year 2023, and 90 in calendar years 2024, 2025, and 2026. Because Financial Institution D did not originate at least 100 covered credit transactions for small businesses in each of 2022 and 2023, it is not in Tier 1, Tier 2, or Tier 3. Because Financial Institution D did not originate at least 100 covered credit transactions for small businesses in subsequent consecutive calendar years, it is not a covered financial institution under § 1002.105(b) and is not required to comply with the rule in 2025, 2026, or 2027.

   v. Financial Institution E originated 120 covered credit transactions for small businesses in each of calendar years 2022, 2023, and 2024, and 90 in 2025. Because Financial Institution E did not originate at least 2,500 or 500 covered credit transactions for small businesses in each of 2022 and 2023, it is not in Tier 1 or Tier 2. Because Financial Institution E originated at least 100 covered credit transactions for small businesses in each of 2022 and 2023, it is in Tier 3 and has a compliance date of October 18, 2026. However, because Financial Institution E did not originate at least 100 covered credit transactions for small businesses in both 2024 and 2025, it no longer satisfies the definition of a covered financial institution in § 1002.105(b) at the time of the compliance date for Tier 3 institutions and thus is not required to comply with the rule in 2026.

   vi. Financial Institution F originated 90 covered credit transactions for small businesses in calendar year 2022, and 120 in 2023, 2024, and 2025. Because Financial Institution F did not originate at least 100 covered credit transactions for small businesses in each of 2022

and 2023, it is not in Tier 1, Tier 2, or Tier 3. Because Financial Institution F originated at least 100 covered credit transactions for small businesses in subsequent calendar years, § 1002.114(b)(4), which cross-references § 1002.105(b), applies to Financial Institution F. Because Financial Institution F originated at least 100 covered credit transactions for small businesses in each of 2024 and 2025, it is a covered financial institution under § 1002.105(b) and is required to comply with the rule beginning October 18, 2026. Alternatively, if Financial Institution F chooses to use its originations in calendar years 2023 and 2024 to determine its compliance tier pursuant to § 1002.114(c)(3), it would be in Tier 3 and likewise required to comply with the rule beginning October 18, 2026.

vii. Financial Institution G originated 90 covered credit transactions for small businesses in each of calendar years 2022, 2023, 2024, 2025, and 2026, and 120 in each of 2027 and 2028. Because Financial Institution F did not originate at least 100 covered credit transactions for small businesses in each of 2022 and 2023, it is not in Tier 1, Tier 2, or Tier 3. Because Financial Institution G originated at least 100 covered credit transactions for small businesses in subsequent calendar years, § 1002.114(b)(4), which cross-references § 1002.105(b), applies to Financial Institution G. Because Financial Institution G originated at least 100 covered credit transactions for small businesses in each of 2027 and 2028, it is a covered financial institution under § 1002.105(b) and is required to comply with the rule beginning January 1, 2029.

viii. Financial Institution H originated 550 covered credit transactions for small businesses in each of calendar years 2022 and 2023, 450 in 2024, and 550 in 2025. Because Financial Institution H originated at least 500 covered credit transactions for small businesses in each of 2022 and 2023, it would be in Tier 2 and have a compliance date of January 16, 2026. However, § 1002.114(c)(3) permits financial institutions to use their originations in 2023 and 2024, rather than in 2022 and 2023, to determine compliance tier. If Financial Institution H elects to use its originations in 2023 and 2024, it would be in Tier 3 and required to comply with the rule beginning October 18, 2026.

114(c) Special Transition Rules

1. ***Collection of certain information prior to a financial institution's compliance date.*** *Notwithstanding § 1002.5(a)(4)(ix), a financial institution that chooses to collect information on covered applications as permitted by § 1002.114(c)(1) in the 12 months prior to its initial compliance date as specified in § 1002.114(b)(1), (2) or (3) need comply only with the requirements set out in §§ 1002.107(a)(18) and (19), 1002.108, and 1002.111(b) and (c) with respect to the information collected. During this 12-month period, a covered financial institution need not comply with the provisions of § 1002.107 (other than §§ 1002.107(a)(18) and (19)), 1002.109, 1002.110, 1002.111(a), or 1002.114.*

2. ***Transition rule for applications received prior to a compliance date but final action is taken after a compliance date.*** *If a covered financial institution receives a covered application from a small business prior to its initial compliance date specified in § 1002.114(b), but takes final action on or after that date, the financial institution is not required to collect data regarding that application pursuant to § 1002.107 nor to report the application pursuant to § 1002.109. For example, if a financial institution is subject to a compliance date of July 18, 2025, and it receives an application on July 7, 2025 but does not take final action on the application until July 25, 2025, the financial institution is not required to collect data pursuant to § 1002.107 nor to report data to the Bureau pursuant to § 1002.109 regarding that*

application.

3. ***Has readily accessible the information needed to determine small business status.*** *A financial institution has readily accessible the information needed to determine whether its originations of covered credit transactions were for small businesses as defined in § 1002.106 if, for instance, it in the ordinary course of business collects data on the precise gross annual revenue of the businesses for which it originates loans, it obtains information sufficient to determine whether an applicant for business credit had gross annual revenues of $5 million or less, or if it collects and reports similar data to Federal or State government agencies pursuant to other laws or regulations.*

4. ***Does not have readily accessible the information needed to determine small business status.*** *A financial institution does not have readily accessible the information needed to determine whether its originations of covered credit transactions were for small businesses as defined in § 1002.106 if it did not in the ordinary course of business collect either precise or approximate information on whether the businesses to which it originated covered credit transactions had gross annual revenue of $5 million or less. In addition, even if precise or approximate information on gross annual revenue was initially collected, a financial institution does not have readily accessible this information if, to retrieve this information, for example, it must review paper loan files, recall such information from either archived paper records or scanned records in digital archives, or obtain such information from third parties that initially obtained this information but did not transmit such information to the financial institution.*

5. ***Reasonable method to estimate the number of originations.*** *The reasonable methods that financial institutions may use to estimate originations for 2022 and 2023 (or for 2023 and 2024, pursuant to § 1002.114(c)(3)) include, but are not limited to, the following:*

   i. A financial institution may comply with § 1002.114(c)(2) by determining the small business status of covered credit transactions by asking every applicant, prior to the closing of approved transactions, to self-report whether it had gross annual revenue for its preceding fiscal year of $5 million or less, during the period October 1 through December 31, 2023. The financial institution may annualize the number of covered credit transactions it originates to small businesses from October 1 through December 31, 2023 by quadrupling the originations for this period, and apply the annualized number of originations to both calendar years 2022 and 2023. Pursuant to § 1002.114(c)(3), a financial institution is permitted to use its originations in 2023 and 2024, rather than 2022 and 2023, to determine its compliance tier. Thus, a financial institution may ask applicants to self-report revenue information during the period of October 1 through December 31, 2024, and then may annualize the number of covered credit transactions it originated to small businesses during that period and apply the annualized number of originations to both calendar years 2023 and 2024.

   ii. A financial institution may comply with § 1002.114(c)(2) by assuming that every covered credit transaction it originates for business customers in calendar years 2022 and 2023 (or in 2023 and 2024) is to a small business.

   iii. A financial institution may comply with § 1002.114(c)(2) by using another methodology provided that such methodology is reasonable and documented in writing.

6. ***Examples.*** *The following scenarios illustrate the potential application of § 1002.114(c)(2) to a financial institution's compliance date under § 1002.114(b). Unless otherwise indicated, in each example the financial institution has chosen to estimate its originations for 2022 and 2023 (rather than 2023 and 2024 as permitted by § 1002.114(c)(3)) to determine its initial compliance*

tier.

*i. Prior to October 1, 2023, Financial Institution A did not collect gross annual revenue or other information that would allow it to determine the small business status of the businesses for whom it originated covered credit transactions in calendar years 2022 and 2023. Financial Institution A chose to use the methodology set out in comment 114(c)–5.i and as of October 1, 2023 began to collect information on gross annual revenue as defined in § 1002.107(a)(14) for its covered credit transactions originated for businesses. Using this information, Financial Institution A determined that it had originated 750 covered credit transactions for businesses that were small as defined in § 1002.106. On an annualized basis, Financial Institution A originated 3,000 covered credit transactions for small businesses (750 originations * 4 = 3,000 originations per year). Applying this annualized figure of 3,000 originations to both calendar years 2022 and 2023, Financial Institution A is in Tier 1 and has a compliance date of July 18, 2025.*

*ii. Prior to July 1, 2023, Financial Institution B collected gross annual revenue information for some applicants for business credit, but such information was only noted in its paper loan files. Financial Institution B thus does not have reasonable access to information that would allow it to determine the small business status of the businesses for whom it originated covered credit transactions for calendar years 2022 and 2023. Financial Institution B chose to use the methodology set out in comment 114(c)–5.i, and as of October 1, 2023, Financial Institution B began to ask all businesses for whom it was closing covered credit transactions if they had gross annual revenues in the preceding fiscal year of $5 million or less. Using this information, Financial Institution B determined that it had originated 350 covered credit transactions for businesses that were small as defined in § 1002.106. On an annualized basis, Financial Institution B originated 1,400 covered credit transactions for small businesses (350 originations * 4 = 1,400 originations per year). Applying this estimated figure of 1,400 originations to both calendar years 2022 and 2023, Financial Institution B is in Tier 2 and has a compliance date of January 16, 2026.*

*iii. Prior to April 1, 2023, Financial Institution C did not collect gross annual revenue or other information that would allow it to determine the small business status of the businesses for whom it originated covered credit transactions in calendar years 2022 and 2023. Financial Institution C chose its own methodology pursuant to comment 114(c)–5.iii, basing it in part on the methodology specified in comment 114(c)–5.i. Starting on April 1, 2023, Financial Institution C began to ask all business applicants for covered credit transactions if they had gross annual revenue in their preceding fiscal year of $5 million or less. Using this information, Financial Institution C determined that it had originated 100 covered credit transactions for businesses that were small as defined in § 1002.106. On an annualized basis, Financial Institution C originated approximately 133 covered credit transactions for small businesses ((100 originations * 365 days)/275 days = 132.73 originations per year). Applying this estimate of 133 originations to both calendar years 2022 and 2023, Financial Institution C is in Tier 3 and has a compliance date of October 18, 2026.*

iv. Financial Institution D did not collect gross annual revenue or other information that would allow it to determine the small business status of the businesses for whom it originated covered credit transactions in calendar years 2022 and 2023. Financial Institution D determined that it had originated 3,000 total covered credit transactions for businesses in each of 2022 and 2023. Applying the methodology specified in comment 114(c)–5.ii, Financial Institution D assumed that all 3,000 covered credit transactions originated in each of 2022 and 2023 were to small businesses. On that basis, Financial Institution D is in Tier 1 and has a compliance date of July 18, 2025.

v. Financial Institution E did not collect gross annual revenue or other information that would allow it to determine the small business status of the businesses for whom it originated covered credit transactions in calendar years 2022 and 2023. Financial Institution E determined that it had originated 700 total covered credit transactions for businesses in each of 2022 and 2023. Applying the methodology specified in comment 114(c)–5.ii, Financial Institution E assumed that all such transactions in each of 2022 and 2023 were originated for small businesses. On that basis, Financial Institution E is in Tier 2 and has a compliance date of January 16, 2026.

vi. Financial Institution F does not have readily accessible gross annual revenue or other information that would allow it to determine the small business status of the businesses for whom it originated covered credit transactions in calendar years 2022 and 2023. Financial Institution F determined that it had originated 80 total covered credit transactions for businesses in 2022 and 150 total covered credit transactions for businesses in 2023. Applying the methodology set out in comment 114(c)–5.ii, Financial Institution F assumed that all such transactions originated in 2022 and 2023 were originated for small businesses. On that basis, Financial Institution E is not in Tier 1, Tier 2 or Tier 3, and is subject to the compliance date provision specified in § 1002.114(b)(4).

*vii. Financial Institution G does not have readily accessible gross annual revenue or other information that would allow it to determine the small business status of the businesses for whom it originated covered credit transactions in calendar years 2022, 2023, or 2024. Financial Institution G chose to use the methodology set out in comment 114(c)–5.i, and as of October 1, 2024, Financial Institution G began to ask all businesses for whom it was closing covered credit transactions if they had gross annual revenue in the preceding fiscal year of $5 million or less. Using this information, Financial Institution G determined that it had originated 700 covered credit transactions during that period for businesses that were small as defined in § 1002.106. On an annualized basis, Financial Institution G originated 2,800 covered credit transactions for small businesses (700 originations * 4 = 2,800 originations per year). Applying this estimated figure of 2,800 originations to both calendar years 2023 and 2024, Financial Institution G is in Tier 1 and has a compliance date of July 18, 2025.*

* * * * *

What You Need to Do:

Please review and share with affected team members. Implement according to the new compliance dates and filing deadlines.

Depository Issues

Section 1: Regulation CC – Expedited Funds Availability Act

FRB,CFPB: Inflation-Adjusted Dollar Thresholds (Maay 13, 2024)

Link

https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20240513a1.pdf

Text

The Federal Reserve Board and the Consumer Financial Protection Bureau jointly adjusted for inflation dollar amounts relating to the availability of customer funds.

These changes in Regulation CC include the minimum amount of deposited funds that banks must make available for withdrawal by opening of business on the next day for certain check deposits as well as the amount of funds deposited by certain checks in a new account that are subject to next-day availability.

By law, the agencies are required to adjust these dollar thresholds every five years by the annual percentage increase in the Consumer Price Index for Urban Wage Earners and Clerical Workers (CPI-W). The inflation measurement period for this adjustment began in July 2018 and ended in July 2023.

To help ensure that depository institutions have sufficient time to implement the adjustments, the compliance date for the new amounts is July 1, 2025.

SUPPLEMENTARY INFORMATION:

Background

Regulation CC (12 CFR part 229) implements the EFA Act and the Check 21 Act. Subpart B of Regulation CC implements the requirements set forth in the EFA Act regarding the availability schedules within which banks must make funds available for withdrawal, exceptions to those schedules, disclosure of funds availability policies, and payment of interest. The EFA Act and subpart B of Regulation CC contain specified dollar amounts, including:

(1) the minimum amount of deposited funds that banks must make available for withdrawal by opening of business on the next day for certain check deposits ("minimum amount");

(2) the amount a bank must make available when using the EFA Act's permissive adjustment to the funds availability rules for withdrawals by cash or other means ("cash withdrawal amount");

(3) the amount of funds deposited by certain checks in a new account that are subject to next-day availability ("new-account amount");

(4) the threshold for using an exception to the funds availability schedules if the aggregate amount of checks on any one banking day exceeds the threshold amount ("large-deposit threshold");

(5) the threshold for determining whether an account has been repeatedly overdrawn ("repeatedly overdrawn threshold"); and

(6) the civil liability amounts for failing to comply with the EFA Act's requirements.

The Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) made certain amendments to the EFA Act, and these amendments were effective on July 21, 2011. Section 609(a) of the EFA Act, as amended by section 1086(d) of the Dodd-Frank Act, provides that the Board and the Director of the CFPB shall jointly prescribe regulations to carry out the provisions of the EFA Act, to prevent the circumvention or evasion of such provisions, and to facilitate compliance with such provisions.

Additionally, section 1086(f) of the Dodd-Frank Act added section 607(f) of the EFA Act, which provides that the dollar amounts under the EFA Act shall be adjusted every five years after December 31, 2011, by the annual percentage increase in the Consumer Price Index for Urban Wage Earners and Clerical Workers (CPI-W), as published by the Bureau of Labor Statistics, rounded to the nearest multiple of $25. In 2019, the Agencies promulgated a final rule that implemented this section of the EFA Act. The final rule codified a methodology for inflation adjustments and specified that the relevant dollar amounts shall be adjusted effective on July 1, 2020, on July 1, 2025, and on July 1 of every fifth year after 2025. For dollar amount adjustments that are effective on July 1, 2025, the inflation measurement period begins in July 2018 and ends in July 2023.

Adjustment

As a result of the 21.8 percent increase in the CPI-W between July 2018 and July 2023, the following thresholds are effective July 1, 2025:

Section	Threshold
Minimum Amount, 12 CFR 229.10(c)(1)(vii)	$275
Cash Withdrawal Amount, 12 CFR 229.12(d)	$550
New-Account Amount, 12 CFR 229.13(a)(1)(ii)	$6,725
Large-Deposit Threshold, 12 CFR 229.13(b)	$6,725
Repeatedly Overdrawn Threshold, 12 CFR 229.13(d)(2)	$6,725
Civil Liability Minimum and Maximum for Individual Action, 12 CFR 229.21(a)(2)(i)	$125 $1,350
Civil Liability Maximum for Class Action, 12 CFR 229.21(a)(2)(ii)(B)	$672,950

PART 229—AVAILABILITY OF FUNDS AND COLLECTIONS OF CHECKS (REGULATION CC)

§ 229.10 [Amended]

In § 229.10, remove "$225," and add in its place "$275;" in paragraph (c)(1)(vii)(A).

In § 229.11, revise paragraph (c) to read as follows:

§ 229.11 Adjustment of dollar amounts

* * * * *

(c) **Amounts.**

(1) For purposes of § 229.10(c)(1)(vii), the dollar amount in effect during a particular period is the amount stated in this paragraph (c)(1) for that period.

(i) Prior to July 21, 2011, the amount is $100.

(ii) From July 21, 2011, through June 30, 2020, by operation of section 603(a)(2)(D) of the EFA Act (12 U.S.C. 4002(a)(2)(D)) the amount is $200.

(iii) From July 1, 2020, through June 30, 2025, the amount is $225.

(iv) Effective July 1, 2025, the amount is $275.

(2) For purposes of § 229.12(d), the dollar amount in effect during a particular period is the amount stated in this paragraph (c)(2) for that period.

(i) Prior to July 1, 2020, the amount is $400.

(ii) From July 1, 2020, through June 30, 2025, the amount is $450.

(iii) Effective July 1, 2025, the amount is $550.

(3) For purposes of §§ 229.13(a), 229.13(b), and 229.13(d), the dollar amount in effect during a particular period is the amount stated in this paragraph (c)(3) for that period.

(i) Prior to July 1, 2020, the amount is $5,000.

(ii) From July 1, 2020, through June 30, 2025, the amount is $5,525.

(iii) Effective July 1, 2025, the amount is $6,725.

(4) For purposes of § 229.21(a), the dollar amounts in effect during a particular period are the amounts stated in this paragraph (c)(4) for the period.

(i) Prior to July 1, 2020, the amounts are $100, $1,000, and $500,000 respectively.

(ii) From July 1, 2020, through June 30, 2025, the amounts are $100, $1,100, and $552,500 respectively.

(iii) Effective July 1, 2025, the amounts are $125, $1,350, and $672,950 respectively.

§ 229.12 [Amended]

In § 229.12, remove “$450” and “$225” and add in their places “$550” and “$275”, respectively, in paragraph (d).

§ 229.13 [Amended]

In § 229.13, remove “$5,525” and add in its place “$6,725” in paragraphs (a)(1)(ii), (b), and (d)(2).

§ 229.21 [Amended]

In § 229.21:

a. Remove “$100” and “$1,100” add in their places “$125” and “$1,350”, respectively, in paragraph (a)(2)(i).

b. Remove “$552,500” and add in its place “672,950” in paragraph (a)(2)(ii)(B).

Appendix E to Part 229 [Amended]

In appendix E to part 229, remove the dollar amounts in the “Remove” column wherever they appear within the section indicated in the “Section” column, and add in their places the dollar amounts in the “Add” column in the following table:

[Table omitted]

What You Need to Do:
Revise policies, procedures, systems, and train prior to July 1, 2025.

Other Issues

CFPB: Prepared Remarks of Director Rohit Chopra at the Mortgage Bankers Association (May 20, 2024)

Link

https://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-of-cfpb-director-rohit-chopra-at-the-mortgage-bankers-association/

Text

While home prices and interest rates often command headlines, there are many other forces at play that are pushing costs up for both mortgage lenders and for homeowners, which can make it harder for families purchasing a home.

Mortgage lenders in the U.S. increasingly face a lack of competition when it comes to accessing data and reports needed for loan origination. In many cases, a handful of firms have cornered the market, allowing those companies to levy a tax on every mortgage application or transaction in the country. The result is that mortgage lenders can evaluate fewer applicants, and homeowners end up eating higher costs, typically at closing.

Today, I want to talk about credit reports and credit scores. The credit reporting industry is dominated by three players: Equifax, Experian, and TransUnion. The market for credit scores has long been dominated by one company's algorithm: the Fair Isaac Corporation, which sells the FICO score. Mortgage lenders have shared that costs for credit reports and scores have increased, sometimes by 400% since 2022.

I want to explain a bit more about the mechanics of how credit reports and scores are pulled, as well as how these costs are passed on to both homebuyers and lenders. Finally, I want to talk about how the CFPB is thinking about ways to lower these costs.

Increased Credit Reporting Costs Being Put on Mortgage Lenders

As all of you here know, mortgage origination is heavily influenced by capital markets. Investors in the secondary market rely on credit scores as a key way to analyze pools of mortgages and mortgage-backed securities. Lenders are required to certify that all the loans in a particular pool have been extended to borrowers who meet a certain credit score threshold. Origination guidelines from Fannie Mae and Freddie Mac help to institutionalize this reliance.

Most mortgage lenders purchase a credit report from resellers, who submit requests to Equifax, Experian, and TransUnion to obtain information about a borrower. Mortgage companies generally order a single credit report to initially determine if a borrower qualifies for a loan program. If the borrower's score is over a certain threshold, the report can be automatically or manually converted to a report that includes all three reports, sometimes referred to as a tri-merge.

Amidst higher interest rates and a corresponding drop in home loan originations, mortgage lenders have recently raised concerns about the increasing costs of obtaining credit scores from FICO. Lenders have no choice but to pay for these increased fees. Lenders, who would otherwise rely on other data for underwriting, can only avoid the FICO fees if they also skip the secondary market and hold the loans in portfolio, which is infeasible for many lenders, especially small ones.

With a captive customer base, vendors have implemented annual price increases that significantly outpace inflation. And in order to get the credit score and credit reports, mortgage lenders generally must pay twice; once to confirm eligibility and once just before the loan closes. If there are multiple applicants for the mortgage, such as two spouses, lenders will end up paying the credit report fee four or more times.

And because many investors still require reports from Equifax, Experian, and TransUnion, lenders often end up paying for essentially the same information six or twelve times. In addition, lenders often must pay fees to have the reports transmitted in the correct machine-readable format to the initial purchaser of the loan, as a precursor to the loan's securitization. There are also usually additional fees for things like employment verification.

Lenders generally have to eat the costs of the initial applicant screening for applicants who don't qualify or decide not to pursue a loan. As a result, lenders often pack the cost of screening applicants into their origination fees or interest rates, rather than charging borrowers upfront for the cost of credit reporting. In some sense, borrowers that close aren't just paying for the credit reports and scores for themselves, they're also paying for inflated fees on the applicants who don't close.

Price Hikes for FICO Scores and Credit Reports

FICO scores have long been required by all the major secondary market participants, including Fannie Mae and Freddie Mac. FICO itself claims that its FICO scores are used by 90% of top lenders and in 90% of U.S. lending decisions.

FICO develops its models using de-identified credit reporting data from Equifax, Experian, and TransUnion. FICO's models generate scores that rank and order consumers according to the model's prediction of the probability a consumer will meet their credit obligations over a 24-month horizon.

Equifax, Experian, and TransUnion distribute the individual consumer scores to end users, such as lenders, for use in a variety of consumer credit decisions, including mortgage underwriting. The users typically pay the credit reporting conglomerates for each individual score, and the companies in turn pay a licensing fee to FICO.

Single credit reports now typically cost between $18 to $30 for an individual report, $24 to $40 for a joint report, and $40 to $60 for a tri-merge report provided by resellers. When mortgage credit reports and scores are requested for a mortgage underwriting decision, Equifax, Experian, and TransUnion typically set the wholesale price that resellers pay, which is then passed on to users. This is often implemented through an additional fee as compensation for their services in the underwriting process.

In November 2023, FICO announced that it would no longer use a pricing structure based on volume, and instead it began charging one flat price to all lenders. This resulted in sharp cost increases of over 400% for most mortgage lenders positioned in FICO's "third tier".

For 2024, FICO now charges consumer reporting companies a licensing fee of $3.50 per FICO score used, or approximately $10 for all three scores if a lender obtains a tri-merge report and score bundle. That fee doubles if two borrowers apply together. The companies and their resellers also raised the price for "soft pulls" to match that of "hard pulls" despite the significant difference between the two data reports.

Making matters worse, credit reports are often rife with inaccuracies discovered by borrowers and lenders. Credit reporting conglomerates are required to have procedures in place to assure maximum possible accuracy, but the CFPB is inundated with consumer complaints regarding these problems.

The credit reporting industry has actually devised a way to profit from those problems – it's called the "rapid rescore." It's a pay-to-play service where mortgage loan officers can, for an extra fee, get consumer credit files reviewed and updated quickly.

When there is a dispute about the information contained in a credit report, rapid rescores help resolve the dispute quickly – but for a price. Fees can run anywhere from $25-$40 per credit file, per credit reporting company. A report full of junk data is another opportunity for these companies to leverage their position as indispensable market actors, and extract yet more money from consumers who have no other options.

It isn't just reports and scores. We've also observed significant price increases from income verification services. Our market monitoring suggests that prices for the Equifax's "Work Number" product, used by mortgage lenders across the country, rose from under $20 per pull in 2016 to up to $90 per pull in 2023, according to some pricing reports. For background screening, users have reported that the current retail price is about $115 per pull. Users tell us that Equifax's market dominance has given it pricing power that it has exercised over the past several years.

Increasing Closing Costs

While these fees may be small relative to the size of mortgages, they add up. As closing costs rise, and downpayments shrink, borrowers may end up paying for mortgage insurance in order to qualify for a loan or risk being shut out completely. Some borrowers end up covering increased loan costs with increased loan amounts. Other homebuyers use seller credits to pay for the closing costs, which can mean a higher sales price. Others use lender credits, which often means a higher rate.

All of these options usually mean both increased mortgage payments going forward and reduced cash reserves for emergencies. It also means the less you put down translates into either higher mortgage payments or being shut out of homeownership altogether.

Lenders who attempt to pass on to borrowers the cost of screening applicants risk violating legal limitations on charging borrowers legitimate fees. This means that as the costs of screening applicants rise, and in particular, the costs increase for the initial screening credit reports, some mortgage lenders will choose to evaluate fewer borrowers overall. This, too, can shut people out of the market.

Stopping Price Gouging in the Future

These steep price increases raise big questions. Why are lenders and borrowers being charged repeatedly for their information? The FHFA has undertaken significant work on credit reporting issues. The CFPB is also analyzing the rise in mortgage closing costs, including credit reporting costs. We are eager to hear from lenders and will look at possible rulemaking and guidance to

improve competition, choice, and affordability.

To lower costs for credit reports in mortgage lending, limiting chokepoints from specific data monopolists is critical.

The CFPB administers rules regarding the Fair Credit Reporting Act. Under provisions of this law, consumers are entitled to one free credit report per year from Equifax, Experian, and TransUnion. Other credit reports, as well as additional reports from these three conglomerates, are subject to price regulation, given that the structure of this market is like a utility.

In some circumstances, the Fair Credit Reporting Act capped certain fees for credit files at $8, adjusted for inflation, which now totals $15.50. The law also requires that fees for credit scores are "fair and reasonable," as determined by the CFPB. This provision was originally administered by the Federal Trade Commission, which never offered a clear threshold.

While these fee caps apply in specific circumstances described in the Fair Credit Reporting, it is clear that the mortgage industry needs to do more to share input on what, if anything, the CFPB should do to address price gouging in this market.

More broadly, the CFPB is looking at ways to accelerate the shift to "open banking" in the U.S. By giving loan applicants the ability to permission transaction and other financial data to potential lenders, underwriters can more easily assess a borrower's ability to repay a loan.

Over the long term, looking directly at applicant-shared information offers lenders a meaningful alternative to check the power of fee harvesters. The CFPB has proposed the Personal Financial Data Rights rule, which activates a long dormant authority enacted by Congress more than a decade ago. This will be an important step towards helping consumers share their information more readily.

When consumers have a greater ability to share their information with new lenders, consumers can access credit at more competitive rates. We are already seeing this happen in mortgage lending. The FHFA is facilitating the use of new approaches to credit scoring, which will help with this.

Capital markets professionals will also need to continue working on ways for investors to assess mortgage pools without solely relying on credit scores. Over the long term, making it easier to access transaction data would also help bring an end to the current overreliance on opaque three-digit credit scores derived from credit reports that are too often rife with inaccuracies.

To conclude, we have a lot to do to think about how we'll use data in ways that broadly benefit the market, rather than just give a handful of firms the ability to extract junk fees and push up costs for everyone.

What You Need to Do:

Informational; please share with applicable team members.

CFPB: Inquiry into Junk Fees in Mortgage Closing Costs (May 30, 2024)

Link

https://www.consumerfinance.gov/rules-policy/notice-opportunities-comment/open-notices/request-for-information-regarding-mortgage-closing-costs/

Text

The Consumer Financial Protection Bureau (CFPB) launched a public inquiry into junk fees that are increasing mortgage closing costs. The CFPB wants to understand why closing costs are increasing, who is benefiting, and how costs for borrowers and lenders could be lowered. According to a CFPB analysis, the closing costs borrowers pay in connection with a mortgage have risen steeply in recent years. From 2021 to 2023, median total loan costs for home mortgages increased by over 36%. The unavoidable fees borrowers must pay at closing can strain household budgets and families' ability to afford a down payment. The fees may also limit the ability of lenders to offer competitive mortgages because they have to absorb the higher costs or pass them on to borrowers.

People rely on mortgage loans to buy their homes and to access home equity. When people purchase a home with a mortgage, they pay a number of fees, such as charges for credit reporting and title insurance. Even if disclosed, borrowers are compelled to pay the fees and may have no control over cost. In 2022, median closing costs were $6,000, and these fees can quickly erode home equity and undercut homeownership.

Mortgage lenders also pay a price when it comes to junk fees and excessive closing costs. For example, in recent years the cost of a credit report has risen substantially. Rising costs can prevent lenders from competing for every potential mortgage because these fees drive up the cost of considering an applicant.

Title insurance is another major fee paid at closing. Most commonly, lender's title insurance is paid by the borrower to protect the lender against problems with the property. Consumers typically have limited options to shop around for title insurance.

The CFPB's request for information seeks input from the public, including borrowers and lenders, about how mortgage closing costs may be inflated and constraining the mortgage lending market. Specifically, the CFPB asks for information about:

- **Which fees are subject to competition:** The CFPB is interested in the extent to which consumers or lenders currently apply competitive pressure on third-party closing costs. The CFPB also wants to learn about market barriers that limit competition.
- **How fees are set and who profits from them**: The CFPB wants to learn about who benefits from required services and whether lenders have oversight or leverage over third-party costs that are passed onto consumers.
- **How fees are changing and how they affect consumers:** The CFPB wants information about which costs have increased most in recent years and the reasons for such increases, including the rise in cost for credit reports and credit scores. The CFPB is also interested in data on the impact of closing costs on housing affordability, access to

homeownership, or home equity.

The CFPB encourages comments and data from the public and all interested stakeholders. Comments must be received on or before August 2, 2024.

What You Need to Do:
Informational; please share with applicable team members.

CFPB: Deception in Contract Fine Print (June4, 2024)

Link

https://www.consumerfinance.gov/compliance/circulars/consumer-financial-protection-circular-2024-03/

Text

The Consumer Financial Protection Bureau (CFPB) issued a circular warning against the use of unlawful or unenforceable terms and conditions in contracts for consumer financial products or services. Companies use this fine print tactic to try to trick consumers into believing they have given up certain legal rights or protections. When financial institutions take these types of actions, they risk violating the Consumer Financial Protection Act. This warning is part of the CFPB's broader efforts to ensure freedom and fairness in people's interactions with financial institutions.

Many consumer contracts include terms and conditions that claim to limit consumer rights and protections. This fine print may just be an attempt to confuse people about their rights. A common example is the general liability waiver, which purports to fully insulate companies from suits even though most states have laws that create hosts of exemptions to these waivers.

Similarly, several federal consumer financial protection laws offer protections that cannot be taken away from people, no matter what a contract says. For example, the Military Lending Act generally prohibits terms in certain consumer credit contracts that require servicemembers and their dependents to waive their right to legal recourse. Another example is mortgage rules, implementing the Truth in Lending Act, which prohibit fine print that forces homeowners into arbitration or other nonjudicial procedures to resolve problems with a mortgage transaction.

This circular explains how and when fine print tricks and intimidation in contracts for consumer financial products and services may violate the Consumer Financial Protection Act's prohibition on deceptive acts and practices. Companies may be liable even if the unenforceable terms are borrowed from form templates or widely available contracts.

The CFPB has taken action with respect to this unlawful conduct on many occasions over the past several years, including on deceptive behavior toward:

- **Mortgage borrowers:** CFPB examiners have repeatedly found examples of deceptive contract terms purporting to waive mortgage borrowers' rights that cannot be waived.

- **Bank accountholders:** The CFPB found that a bank deceived consumers through contract terms that it claimed waived consumers' right to hold the bank liable for improperly responding to garnishment orders when, in fact, this right could not be waived. The bank inserted these terms into deposit agreements with broad fine print language.
- **Remittance transfer consumers:** The CFPB found that a remittance transfer provider violated the Consumer Financial Protection Act's deception prohibition when it included misleading statements in disclosures purporting to limit consumers' error resolution rights, which would be unenforceable under the Electronic Fund Transfer Act and the Remittance Rule.
- **Auto loan borrowers**: The CFPB found an auto loan servicer deceptively included language in contracts that indicated that consumers could not exercise bankruptcy rights, when in fact, waivers of bankruptcy rights generally are void as a matter of public policy.

This circular builds on previous initiatives and guidance provided by the CFPB that are intended to ensure freedom and fairness in people's interactions with financial institutions. Last year, the CFPB proposed a rule to require certain supervised nonbank companies to register with the CFPB information about their use of contractual terms that claim to waive or limit consumer rights. The CFPB also has explained that banks and financial companies attempting to silence consumers from posting honest online reviews through contract terms undermine fair competition and may be breaking the law. The CFPB additionally has highlighted that certain tuition payment plans include terms and conditions that are likely unenforceable. And the CFPB recently filed an amicus brief with the Justice Department to help ensure that servicemembers can file lawsuits to enforce the Servicemembers Civil Relief Act notwithstanding unenforceable fine print in contracts.

Consumer Financial Protection Circular 2024-03

Unlawful and Unenforceable Contract Terms and Conditions

Question presented

Can persons that include unlawful or unenforceable terms and conditions in contracts for consumer financial products and services violate the prohibition on deceptive acts or practices in the Consumer Financial Protection Act (CFPA)?

Response

Yes. "Covered persons" and "service providers" must comply with the prohibition on deceptive acts or practices in the CFPA. The inclusion of certain terms in contracts for consumer financial products or services may violate the prohibition when applicable federal or state law renders such contractual terms, including those that purport to waive consumer rights, unlawful or unenforceable.

Background on Unlawful and Unenforceable Contract Terms

Many federal laws—including statutes enforced by the CFPB—render unlawful or unenforceable various contract terms in certain contexts. For example, as highlighted in a recent CFPB compliance bulletin, the Consumer Review Fairness Act of 2016 generally prohibits the use

of form contracts that limit how consumers communicate their reviews, assessments, or similar analysis of the sale of goods or services, and invalidates these types of contract terms and conditions. As another example, Regulation Z, which implements the Truth-in-Lending Act (TILA), prohibits the inclusion in a residential mortgage loan or open-ended consumer credit plan secured by the principal dwelling of terms requiring arbitration or any other nonjudicial procedure as the method for resolving any controversy or settling claims arising out of the transaction. The Electronic Fund Transfer Act (EFTA) prohibits contract terms that contain a "waiver of any right conferred" by EFTA and prohibits waivers of any "cause of action" under EFTA. And the Military Lending Act and its implementing regulations generally prohibit terms in certain consumer credit contracts that require servicemembers and their dependents to "waive the covered borrower's right to legal recourse under any otherwise applicable provision of State or Federal law . . . ."

In addition to express prohibitions like these, a recent federal district court decision held that the Servicemembers Civil Relief Act (SCRA) renders unenforceable provisions in contracts with servicemembers that purport to waive their right to participate in class actions to enforce the SCRA. The Federal Trade Commission also administers laws that forbid certain contractual waivers. And certain state laws similarly prohibit or restrict the use of waivers in consumer contracts.

Analysis

The CFPB is issuing this Circular to emphasize that covered persons who include unlawful or unenforceable terms in their consumer contracts may violate the CFPA's prohibition on deceptive acts or practices.

Covered persons may violate the CFPA's prohibition on deceptive acts or practices if they include terms, including waiver provisions, in their consumer contracts that are rendered unlawful or unenforceable by federal or state law. Under the CFPA, a representation or omission is deceptive if it is likely to mislead a reasonable consumer and is material. A representation is "material" if it "involves information that is important to consumers and, hence, likely to affect their choice of, or *conduct regarding*, a product." A contractual provision stating that a consumer agrees not to exercise a legal right is likely to affect a consumer's willingness to attempt to exercise that right in the event of a dispute. Moreover, certain categories of information, including express representations, are presumptively material.

In the recent compliance bulletin noted above, the CFPB reminded covered persons that they could be liable under the CFPA if they deceive consumers using form contract restrictions on consumer reviews that are unenforceable. The CFPB explained that "including an unenforceable material term in a consumer contract is deceptive, because it misleads consumers into believing the contract term is enforceable," and that "disclaimers in a contract such as 'subject to applicable law' do not cure the misrepresentation caused by the inclusion of an unenforceable contract term." Similarly, qualifying a provision that purports to waive a consumer right with "except where unenforceable" is unlikely to cure the provision's misleading or material nature. Neither do disclaimers that are issued after the fact.

CFPB supervisory examiners have identified several violations of the CFPA's prohibition on deception stemming from covered persons' use of unlawful or unenforceable contract terms and conditions. In addition, in several prior enforcement matters, the CFPB has found covered persons to have violated the CFPA by including in contracts for consumer financial products or services terms that are unlawful or unenforceable under federal or state law, such as waivers that are prohibited by federal or state law. For example, the CFPB found that a respondent bank engaged in a deceptive practice under the CFPA when it represented to consumers that because they signed

a deposit agreement including broad language directing the bank not to contest legal process, consumers had waived their right to hold the bank liable for improperly responding to garnishment notices; in fact, regardless of the language in the account agreement, consumers had the right to challenge the garnishments. In another matter, the CFPB found that a respondent auto loan servicer violated the CFPA's deception prohibition when it used loan extension agreements or written confirmations that included language that created the net misimpression that consumers could not exercise bankruptcy protection rights, which was false. In fact, an agreement to waive an individual's right to file for bankruptcy is void as against public policy, rendering terms that purport to waive such right generally unenforceable. The CFPB found in a different matter that a respondent non-bank remittance transfer provider engaged in a deceptive act or practice in violation of the CFPA when it made misleading statements in disclosures purporting to limit consumers' error resolution rights, in violation of EFTA and the Remittance Rule. And, in a recent report, the CFPB highlighted that certain student tuition payment plan agreements and financial responsibility agreements "include terms and conditions that purport to waive consumers' legal protections, limit how consumers enforce their rights, or misrepresent the rights or protections available to consumers under existing law." Some of these terms and conditions, such as purported waivers of the right to retain counsel and the right to seek discharge in bankruptcy proceedings, are likely unenforceable and thus similarly raise deception risk.

As these examples demonstrate, the inclusion of unlawful or unenforceable terms and conditions in consumer contracts is likely to mislead a reasonable consumer into believing that the terms are lawful and/or enforceable, when in fact they are not. Further, the representations made by the presence of such terms are often material, presumptively so when they are made expressly. In particular, consumers are unlikely to be aware of the existence of laws that render the terms or conditions at issue unlawful or unenforceable, so in the event of a dispute, they are likely to conclude they lawfully agreed to waive their legal rights or protections after reviewing the contract on their own or when covered persons point out the existence of these contractual terms and conditions. Deceptive acts and practices such as these pose risk to consumers, whose rights are undermined as a result, and distort markets to the disadvantage of covered persons who abide by the law by including only lawful terms and conditions in their consumer contracts.

Thus, the inclusion of unlawful or unenforceable terms in consumer contracts, including unlawful or unenforceable waiver provisions, may violate the CFPA's prohibition on deceptive acts or practices.

What You Need to Do:

Informational; please share with applicable team members.

CFPB: Comment to Illinois Joint Committee on Administrative Rules on the State's Proposed Community Reinvestment Act Rules (April 9, 2024)

Link

https://www.consumerfinance.gov/about-us/newsroom/cfpb-comment-to-illinois-joint-committee-on-administrative-rules-on-the-states-proposed-community-reinvestment-act-rules/

Text

On behalf of the Consumer Financial Protection Bureau (CFPB), I am pleased to submit this comment regarding the Illinois Department of Financial and Professional Regulation's (IDFPR's) proposed rules for the state's Community Reinvestment Act (CRA).

By way of background, I serve as the CFPB's Deputy Director. I also serve as the CFPB's representative on the Appraisal Subcommittee of the Federal Financial Institutions Examination Council. Since April 1, 2022, I have served as Chair of the Appraisal Subcommittee, which has recently held the fourth in a series of hearings on appraisal bias.

The CFPB's work intersects with topics related to state Community Reinvestment Acts in a number of ways. The CFPB has conducted extensive analysis and research on access to credit across a range of products, including mortgage lending, small business lending, and others. One recent analysis of note is the CFPB's report on state CRA laws, which highlighted the importance of these laws to ensure that financial institutions' lending, services, and investment activities meet the credit needs of their communities. The report also identified how an institution's compliance with federal consumer financial protection laws are incorporated into state CRA evaluations. Additionally, the CFPB has regulatory authority with respect to the nation's mortgage lenders and supervisory and enforcement authority over many such lenders, both depository and non-depository, for compliance with applicable consumer protection laws.

The CFPB has authority to interpret and issue rules under the Equal Credit Opportunity Act (ECOA) and to enforce the statute's requirements. And the CFPB has a statutory objective to ensure federal consumer financial laws are enforced consistently. As such, the CFPB's views concerning the applicable legal standards for discrimination under ECOA may be of assistance to the Joint Committee on Administrative Rules.

In particular, the CFPB submits this comment in support of the proposed appraisal-related changes to 38 IAC 345.280(c)(1)(A) (Bank Community Reinvestment), 38 IAC 185.280(c)(1)(A) (Credit Union Community Reinvestment), and 38 IAC 1055.240(c)(1) (Mortgage Community Reinvestment Act). These provisions state that a lender "relying on or giving force or effect to discriminatory appraisals to deny loan applications where the covered financial institution knew or should have known of the discrimination" is an example of a violation of ECOA. As explained

below, these provisions accurately describe ECOA.

The CFPB, in conjunction with the U.S. Department of Justice, has stated that "[a] lender violates both the [Fair Housing Act (FHA)] and ECOA if it relies on an appraisal that it knows or should know to be discriminatory," and "even beyond the appraisal context, an entity violates the FHA and ECOA if it enables, gives force to, or participates in a course of conduct that it knows or should know to be discriminatory." Hence, to the degree that discrimination is a relevant factor for determining a financial institution lender's rating under a state CRA or other law, it is appropriate to consider whether there is evidence of the lender's reliance on an appraisal that it knows or should know to be discriminatory, and, beyond the appraisal context, whether a lender enables, gives force to, or participates in a course of conduct that it knows or should know to be discriminatory.

The CFPB also has authority over the Truth in Lending Act's (TILA) Appraisal Independence Rule and has pointed out that it does not conflict with a lender's obligations to comply with civil rights laws, including ECOA. Specifically, CFPB has noted that TILA permits a creditor to "ask[] an appraiser to . . . [c]onsider additional, appropriate property information, including the consideration of additional comparable properties to make or support an appraisal[,]" or "[c]orrect errors in the appraisal report." A [creditor/lender] may also "[o]btain[] multiple valuations for the consumer's principal dwelling to select the most reliable valuation," and, more generally, take "action permitted or required by applicable Federal or state statute, regulation, or agency guidance," such as not relying on an appraisal that is inaccurate or violates the law.

Owning a home is one of the most effective ways to build intergenerational wealth. Obtaining an accurate estimate of home value is a critical step in mortgage origination and refinancing. A biased home appraisal is not only inaccurate but can worsen racial inequities and distort the housing market.

States play a critical role in the oversight of appraisals, promoting reinvestment by financial institutions, and they have the unique ability to tailor reinvestment obligations to the needs of their states. By adopting the proposed provisions discussed herein, the state of Illinois would be acting in accordance with existing legal standards for discrimination and utilizing its available tools to ensure a fair marketplace.

The CFPB welcomes the opportunity to submit this comment and to work together in the future.

What You Need to Do:

FOR ILLINOIS BANKS ONLY

FFIEC: Updated 2024 Median Family Income Report (June 25, 2024)

Link

https://www.ffiec.gov/Medianincome.htm

Text

The FFIEC released an updated 2024 FFIEC Median Family Income Report. The report now includes the FFIEC Estimated Median Family Income, which incorporates the boundary changes from OMB Bulletin 23-01. The FFIEC Median Family Income (MFI) Report shows the estimate MFI that corresponds to the year when loan application data are collected.

For 2012 and forward, the MFI data are calculated by the FFIEC. For years 1998 through 2011, the MFI data were calculated by HUD.

What You Need to Do:

Informational; please share with applicable team members.

Section 3: Personal Financial Data Rights Rule

CFPB: Qualifications to Become a "Recognized Industry Standard Setting Body (June 5, 2024)

Link

https://files.consumerfinance.gov/f/documents/cfpb_personal-financial-data-rights_final-rule_2024-06.pdf

Text

The Consumer Financial Protection Bureau (CFPB) finalized a rule outlining the qualifications to become a recognized industry standard setting body, which can issue standards that companies can use to help them comply with the CFPB's upcoming Personal Financial Data Rights Rule. This rule identifies the attributes that standard setting bodies must demonstrate in order to be recognized by the CFPB. The rule also includes a step-by-step guide for how standard setters can apply for recognition and how the CFPB will evaluate applications.

The CFPB is working to accelerate the shift to open banking in the United States. In 2010, Congress passed into law new personal financial data rights for consumers. Guaranteeing a consumer's right to their data will open up more opportunities for smaller financial institutions and startups offering products and services. However, these new rights have not taken full effect, because the CFPB never issued a rule. In October 2023, the CFPB proposed a rule to implement these rights and will finalize it in the coming months.

As part of the upcoming Personal Financial Data Rights rule, the CFPB expects to allow companies to use technical standards developed by standard-setting organizations recognized by the CFPB. Today's rule kicks off the process for standard-setting organizations to seek formal recognition.

The new rule identifies the attributes that standard setters must demonstrate in order to be recognized by the CFPB. Consensus standards issued by recognized standard setters can help put the Personal Financial Data Rights rule into action and accelerate the financial system's movement towards truly open banking.

To be recognized by the CFPB, the standard setters must apply to the CFPB and display the following attributes:

- **Openness**: The CFPB will not recognize any standard-setting organization that is rigged in favor of any set of industry players. The process must be open to all interested parties, including public interest groups, app developers, and a broad range of financial firms with a stake in open banking.
- **Transparency**: Procedures must be transparent to participants and publicly available.

- **Balanced decision-making**: The decision-making power to set standards must be balanced across all interested parties, including consumer and other public interest groups. There must also be meaningful representation for large and small commercial entities. No single special interest can dominate the decision-making process.
- **Consensus**: Standards development must proceed by consensus, though not necessarily unanimity. Comments and objections must be considered using fair and impartial processes.
- **Due process and appeals**: The standard-setting body must use documented and publicly available policies and procedures, provide adequate notice of meetings, sufficient time to review drafts and prepare views and objections, access to views and objections of other participants, and a fair and impartial process for resolving conflicting views. An appeals process is also available for the impartial handling of procedural appeals.

This rule also includes a mechanism for the CFPB to revoke the recognition of standard setters and a maximum recognition duration of five years, after which recognized standard setters will have to apply for re-recognition. These protections will ensure recognized standard setters' ongoing adherence to the attributes codified by the CFPB today. The rule also contains a step-by-step guide to help interested standard setters apply for recognition. The guide describes five steps in the application and recognition process, and the CFPB invites interested standard setters to begin engaging with us when they are ready to demonstrate their adherence to the attributes the CFPB codified today.

This final rule is effective July 11, 2024.

SUPPLEMENTARY INFORMATION:

Summary

The CFPB is finalizing certain provisions of its Required Rulemaking on Personal Financial Data Rights (Personal Financial Data Rights rule), which, among other proposed provisions in the rule, sought to promote fair, open, and inclusive industry standard-setting. The CFPB proposed that standards adopted by CFPB-recognized standard setters might be used to facilitate implementation of a final Personal Financial Data Rights rule. Today's rule revises and finalizes part of proposed § 1033.131 (definitions) and all of proposed § 1033.141 (attributes a standard-setting body must demonstrate in order to be recognized by the CFPB). Included with this rule is a step-by-step guide for how standard setters apply for recognition and how the CFPB will evaluate applications.

Background

Introduction

Consumer electronic access to personal financial data, including and especially open banking, holds the potential to intensify consumer-friendly competition and innovation. Fair, open, and inclusive industry standard-setting play a critical role in ensuring the open banking system reaches its full potential to benefit consumers and competition. By including section 1033 in the Consumer Financial Protection Act of 2010 (CFPA), Congress explicitly recognized the importance of personal financial data rights, and section 1033(d) recognizes the importance of standardized

formats, especially with regard to data formats. In 2023, the CFPB issued a proposed rule to begin implementing section 1033, with the goal of accelerating the shift to a more open and decentralized system of consumer data access.

The proposed rule reflected the CFPB's preliminary determination that conformance with industry standards would constitute certain evidence of compliance with various substantive provisions of the proposed rule (or, in the case of data formats, would be sufficient for a data provider to be deemed compliant), provided that such standards were issued by a body recognized by the CFPB as possessing certain attributes. The proposed rule set forth the CFPB's view that industry standard setters that operate in a fair, open, and inclusive manner have a critical role to play in ensuring a safe, secure, reliable, and competitive data access framework. In the proposed rule, the CFPB noted that Federal regulations with very granular technical requirements could rapidly become obsolete, while industry-led standard-setting would be better able to keep pace with changes in the market and technology, as long as that standard-setting was fair, open, and inclusive.

U.S. government agencies have been historically involved in the development and use of standards to meet agency missions and priorities. Office of Management and Budget (OMB) Circular A-119 reflects the U.S. government's commitment to a U.S. industry-led, voluntary consensus standards system. Broad use of such standards enhances the safety and security of products, reduces consumer costs, and expands consumers' options in the marketplace. Additionally, voluntary consensus standards ensure that no faction of industry can use its market power to impose its preferences on the entire market. Further, the use of consensus standards significantly reduces costs to agencies that would otherwise be incurred if agencies had to develop and maintain agency-unique standards.

Summary of the Rulemaking Process

Outreach and Engagement

The CFPB published its proposed rule on October 31, 2023. The public comment period on the proposed rule closed on December 29, 2023, and the CFPB received comments from individuals and entities representing various diverse interests. In addition, the CFPB also considered comments received after the comment period closed via ex parte submissions and meetings. Materials on the record, including all ex parte submissions and summaries of ex parte meetings, are available on the public docket for this rulemaking.

This final rule discusses those substantive comments relevant to the attributes of standard-setting bodies or the process by which the CFPB will recognize standard-setting bodies. For the most part, commenters that addressed the issues discussed in this final rule and in the appended application procedures supported the CFPB's plan to recognize standard setters that are fair, open, and inclusive, and generally agreed with the attributes the CFPB proposed to use to determine whether a standard-setting body was fair, open, and inclusive. Some commenters requested that the CFPB alter, clarify, or remove specific provisions of the proposed attributes, or made suggestions for how the CFPB should make its determination as to whether to recognize a given standard-setting body. Other commenters argued that the CFPB does not have legal authority to recognize standard-setting bodies, or critiqued how the proposed rule described a potential recognition process. The CFPB has considered these comments in adopting this final rule. The CFPB will discuss and address all other substantive comments when it finalizes the remainder of the Personal Financial Data Rights rule, including the many comments received concerning the role that adherence to a consensus standard should or should not play in evaluating compliance with the particular underlying provisions of the final rule. Comments

focused on the application procedures described in the appendix are discussed in section IV.C.

Prior to issuing this final rule, in accordance with CFPA sections 1033(e) and 1022(b)(2)(B), the CFPB consulted on several occasions with staff from the prudential regulators and the Federal Trade Commission to discuss various aspects of the proposed rule, including criteria for and processes with respect to standard-setting bodies.

Legal Authority

The CFPB is issuing this final rule pursuant to its authority under the CFPA. As set forth in section 1021 of the CFPA, Congress established the CFPB to ensure that "all consumers have access to markets for consumer financial products and services and that markets for consumer financial products and services are fair, transparent, and competitive." Congress also authorized the CFPB to exercise its authorities under Federal consumer financial law, including the CFPA, to ensure that, with respect to consumer financial products and services, consumers have "timely and understandable information to make responsible decisions about financial transactions," "consumers are protected from unfair, deceptive, or abusive acts and practices and from discrimination," that "markets for consumer financial products and services operate transparently and efficiently to facilitate access and innovation," and that "Federal consumer financial law is enforced consistently without regard to the status of a person as a depository institution in order to promote fair competition."

CFPA section 1033

CFPA section 1033(a) and (b) provide that, subject to rules prescribed by the CFPB, a covered person shall make available to a consumer, upon request, information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained from such covered person, subject to certain exceptions. The information must be made available in an electronic form usable by consumers. In addition, CFPA section 1033(d) provides that the CFPB, by rule, shall prescribe standards applicable to covered persons to promote the development and use of standardized formats for information, including through the use of machine-readable files, to be made available to consumers under this section. Recognition of standard-setting bodies that are fair, open, and inclusive can facilitate implementation of these authorities. Further, CFPA section 1033(e) requires that the CFPB consult with the prudential regulators and the FTC to ensure, to the extent appropriate, that certain objectives are met.

CFPA section 1022(b)

CFPA section 1022(b)(1) authorizes the CFPB to, among other things, prescribe rules and issue orders "as may be necessary or appropriate to enable the CFPB to administer and carry out the purposes and objectives of the Federal consumer financial laws, and to prevent evasions thereof." The CFPA is a Federal consumer financial law. This rule carries out the purposes and objectives of the CFPA and prevents evasions thereof, by requiring standard-setting bodies to apply through the CFPB for recognition to adopt consensus standards.

Discussion of the Final Rule

Overview

This final rule identifies the attributes that a standard-setting body must demonstrate in order to be recognized by the CFPB. It also includes procedures for standard setters to apply for recognition by the CFPB. The following addresses comments on the proposed rule relevant to each topic. B. Consensus standards and recognized standard setters Definitions for Recognized Standard Setter and Consensus Standard The CFPB proposed in § 1033.131 to define a "qualified industry standard" as a standard issued by a standard-setting body that is fair, open, and inclusive in accordance with proposed § 1033.141(a).The CFPB proposed in § 1033.141 that a standard-setting body is fair, open and inclusive when it satisfies seven requisite attributes: openness, balance, due process, appeals, consensus, transparency, and that the standard-setting body have been recognized by the CFPB as an issuer of qualified industry standards within the last three years.

Some commenters asked the CFPB to clarify when a standard issued by a recognized standard-setting body becomes a consensus standard, and, conversely, when a consensus standard ceases to have consensus status. A trade group commenter suggested that the CFPB remove the language in proposed § 1033.141(a)(7) that a standard-setting body must have been recognized by the CFPB within the last three years, suggesting that this recognition period would make it difficult for industry to use such standards or, appropriate, switch away from them. One commenter expressed concern that the loss of a standard's status as a consensus standard could cause market uncertainty, because the covered financial institutions would need to identify a different recognized standard setter and possibly have to modify its practices to conform with the consensus standards of that recognized standard setter.

After considering these comments, the CFPB is making several changes to §§ 1033.131 and 1033.141 relating to both standard setters and the standards they issue. First, this final rule replaces the term "qualified industry standard" with "consensus standard," and adds a definition of "recognized standard setter," a term not defined in the proposed rule. These editorial changes are intended to better organize the structure of these key terms, enhance readability of the final rule, and adopt terminology that more clearly describes the defined terms.

The definition of "consensus standard" in final § 1033.131 provides additional specificity regarding when a given standard is a consensus standard. Final § 1033.131 provides that to be a "consensus standard" the standard must be one that is adopted by a recognized standard setter, and that continues to be maintained by that recognized standard setter. Regarding the commenters' concern about market uncertainty, the CFPB expects revocation of recognition for a standard setter to be a rare occurrence, and in that event the CFPB would issue guidance to help manage a transition.

The CFPB has determined that it is appropriate to require a recognized standard setter to seek renewal of its recognition on a periodic basis. However, in § 1033.141(a), this final rule extends the maximum duration of the CFPB's recognition of a standard-setting body from the proposed duration of three years to five years. Periodic review and re-recognition mitigate the risk of outdated standards, which the CFPB's approach to industry standards was intended in part to avoid. Additionally, periodic review by the CFPB will ensure standard setters carefully mind their governance and procedures and keep them in conformance with the attributes. However, extending the maximum recognition period to five years in this final rule is warranted, for two main reasons. First, a five-year recognition period will mean that, should one or more standard-setting body receive early recognition from the CFPB, such recognition—and by extension their

standards' status as consensus standards—would last further into the period during which industry is initially coming into compliance with the forthcoming Personal Financial Data Rights rule, providing additional certainty to smaller data providers covered by the rule. Additionally, the CFPB expects that reducing the frequency of periodic review and re-recognition by the CFPB will encourage standard-setting bodies to obtain recognition because their standards will retain consensus status for a longer period without the burden of seeking re-recognition.

The CFPB's authority to recognize standard-setting bodies

Several industry commenters disputed the Bureau's legal authority to recognize standard-setting bodies that would then issue consensus standards for purposes of facilitating implementation of a final Personal Financial Data Rights rule. In response, the CFPB notes that, as discussed above in this final rule, establishing a framework for standard setting is authorized by CFPA section 1033(a) and (d) and the CFPB's authority to issue rules under CFPA section 1022(b)(1). The CFPB expects that individual recognition decisions will be authorized by this final rule, by the CFPB's authority to issue orders under CFPA section 1022(b)(1), and additionally by the CFPB's authority to issue declaratory orders to "to terminate a controversy or remove uncertainty" under section 554(e) of the Administrative Procedure Act.

Attributes of standard-setting bodies

Openness

The CFPB proposed to include "openness" as a necessary attribute for CFPB recognition, and that a standard-setting body's openness would be evaluated by reviewing whether the standard-setting body's sources, procedures, and processes are open to all interested parties, and whether those interested parties can meaningfully participate in standards development on a nondiscriminatory basis.

A few commenters addressed the proposed openness attribute. Consumer advocate commenters supported the explicit inclusion of consumer groups as an interested party for an open standard-setting body. A small number of commenters recommended alterations to the attribute. One industry trade group called for the CFPB to clarify that only the members of the standard-setting body would need to meaningfully participate in the standards development. Additionally, some third-party industry commenters asked the CFPB to clarify that a standard-setting body that is "open" for purposes of the attribute includes all types of financial institutions, including financial technology companies. In support of this consideration, one commenter highlighted what it described as the undue influence of banks in another country's standard-setting body due to the other country's exclusion of financial technology voices in the standard-setting body.

This final rule adopts § 1033.141(a)(1) mostly as proposed, with some additional clarifying text. In response to commenter concern that certain financial technology sectors might be excluded if not explicitly mentioned, the CFPB has added explicit reference to "data recipients" as an interested party in this final rule. The inclusion of data recipients also helps ensure that data providers and recipients are not forever compelled to rely on intermediaries with commercial interests that may not consistently align with the advancement of open banking standards. This final rule does not adopt commenters' request to limit "openness" to only members of the standard-setting body. As stated in this final rule, the sources of the standard-setting body must be available to all interested parties. This language reiterates that the CFPB expects an "open" standard-setting body to utilize open-source materials that interested parties can reference. Such open-

source materials would not truly be open unless they were made available outside the standard-setting body's membership.

Balance

The CFPB proposed to include "balance" as a necessary attribute for CFPB recognition. The CFPB proposed that a standard-setting body's balance would be evaluated by the CFPB reviewing whether the standard-setting body's decision-making power is balanced across all interested parties at all levels of the standard-setting body. Further, the proposed attribute clarifies that balance could be impacted by entities playing multiple roles, such as data provider and third party. Additionally, the CFPB proposed that it could consider the ownership of an entity when reviewing a standard setter's balance. Finally, the CFPB proposed that balance would include meaningful representation of small and large commercial entities.

A number of commenters addressed this attribute. One consumer advocate commenter expressed their support for the proposed rule's inclusion of consumer advocates as interested parties in an open standard-setting body. Another consumer advocate commenter noted that some current standards bodies do not provide the same voting rights across categories of membership. A few commenters asked for clarification as to what the CFPB will consider "meaningful representation," noting the importance of including small entity voices in the decision-making processes. Additionally, one consumer advocate commenter and one industry commenter recommended that a final rule extend balanced representation considerations to any committee or sub-committee involved in the standard setters decision-making processes.

After considering these comments, the CFPB is finalizing the requirement in § 1033.141(a)(2) largely as proposed, with some modifications. To address commenters' concerns about representation at the committee and sub-committee level, the CFPB has revised this final rule to state that balanced representation must be reflected at all levels of the standard-setting body. The additional "reflected" language provides a standard-setting body with some flexibility to arrange adequate committee and sub-committee representation, while also mitigating the possibility that a particular committee or sub-committee's representation become so unbalanced that it hinders the overall decision-making of the standard-setting body. This final rule does not further define "meaningful representation" because after consideration the CFPB concludes that the additional language reading "[n]o single interest or set of interests dominates decision-making" sufficiently describes the scope of meaningful representation. Finally, to address concerns about weighting of voting rights, this final rule clarifies that if a participant plays multiple roles, the weight of that participant's role will be factored into the balance consideration. As such, if a participant has a vote as a data provider but their primary business is as a third party, this could suggest that the standard-setting body is not balanced. Similarly, the CFPB can look at the ownership of a participant to determine to what degree the role and form of that entity's participation in the standard-setting body furthers or hinders the body's balance.

Due Process and Appeals

The CFPB proposed to include "due process" and "appeals" as necessary attributes for CFPB recognition. The proposed due process attribute would consider whether a standard-setting body uses documented and publicly available policies and procedures and provides a fair and impartial process for resolving conflicting views. The proposed appeals attribute would consider whether the standard-setting body provides an appeals process for the impartial handling of appeals.

A small number of commenters addressed these attributes. A few industry trade groups recommended that a final due process attribute should protect the anonymity of participant

dialogue to encourage open dialogue among the members of the standard-setting body. One consumer advocate commenter recommended that a final appeals attribute focus on the process of creating standards, rather than on the standards themselves.

The CFPB is finalizing the proposed due process and appeals attributes with minimal change and a non-substantive structural modification. The structural modification is to combine the appeals and due process attributes into one attribute (now at § 1033.141(a)(3)), because both address similar issues of procedural fairness. Additionally, the CFPB is finalizing a modification to the appeals attribute that clarifies that the appeals process is available for the impartial handling of procedural appeals. The CFPB is finalizing the remainder of the attribute as proposed. Specifically, this final rule does not add requested language about anonymity within the standard-setting body. While anonymity may in some circumstances help create open dialogue, the CFPB is not including in this final rule the explicit availability of participant viewpoint anonymity because such protection is already provided by this final rule. Standard-setting bodies are not precluded from making viewpoints anonymous, so long as such anonymity policies do not have the potential to undermine a final openness, transparency, or due process attribute.

Consensus

The CFPB proposed to include "consensus" as a necessary attribute for CFPB recognition. Specifically, the proposed attribute looks at whether the standards development processes would proceed by consensus, defined as general agreement but not unanimity.

The CFPB received little commenter input concerning the consensus attribute. One third-party trade group recommended that a final rule consider consensus to be when there is consensus within a particular sector. The commenter suggested that if all third parties or all data providers oppose a standard, then that standard should not be adopted. Additionally, one data provider commenter recommended that a final rule consider that the majority of the standards proposed in the Personal Financial Data Rights rulemaking are obligations on data providers, and, as such, consensus should require data providers to be in agreement with a particular decision-making process of the standard-setting body.

The CFPB is finalizing the attribute largely as proposed, and adding language stating that consensus does not necessarily require unanimity. This modification is to clarify that general agreement can include unanimous decisions by the members of the standard-setting body. This final rule does not include language stating that a single class of standard-setting group members (like data providers or third parties) could have unilateral power in a standard-setting body. While consensus is important, privileging one group of members would inappropriately give that group unwarranted influence. The provision is also renumbered to § 1033.141(a)(4) to reflect organizational changes.

Transparency

The CFPB proposed to include "transparency" as an attribute for CFPB recognition consideration. Specifically, the proposed attribute would look at whether the procedures or processes for participating in standards development and for developing standards are transparent to participants and publicly available.

Several industry trade groups recommended that a final transparency attribute protect the anonymity of participant dialogue to encourage open dialogue among the participants in the setting of consensus standards. As stated above in the discussion of the proposed due process provision, standard-setting bodies are not precluded from making viewpoints anonymous, so long

as such anonymity policies do not have the potential to undermine a final openness, transparency, or due process attribute. Accordingly, for the reasons discussed in the proposal, the CFPB is finalizing the transparency attribute as proposed. The provision is also renumbered to § 1033.141(a)(5) to reflect organizational changes.

Additional attributes

In response to the CFPB's request for comment on whether it should include additional attributes when evaluating a standard setter for recognition, at least one commenter suggested that a final rule should adjust the attribute list to account for the relevance of standards that a standard-setting body adopts.

This final rule does not include an additional "relevance" attribute. However, demonstrating the attributes in this final rule is the minimum requirement for recognition; accordingly, the CFPB may consider other information when reviewing an application for recognition, including whether the standard-setting body will adopt and maintain standards relevant to open banking.

Procedures for CFPB recognition of standard-setting bodies

High-level comment summary

A number of commenters on the proposed rule encouraged the CFPB to establish a process for recognizing standard setters as soon as possible. Their comments generally focused on seeking clarity and transparency from the CFPB about this process. Some industry commenters requested that the CFPB publish its recognition procedures for comment.

In response to comments that the CFPB quickly establish a process for recognizing standard-setting bodies, the CFPB is publishing the procedures included at appendix A. These constitute a rule of agency organization, procedure, or practice, and thus do not require notice and comment under the Administrative Procedure Act. As published, these procedures take account of comments received on the proposed rule regarding procedures for recognizing standard-setting bodies. The CFPB may publish amendments to the procedures from time-to-time as it develops experience with this recognition process and receives stakeholder feedback on them.

Discussion of procedures for recognition

The CFPB is providing a plain language guide for how standard setters should apply for recognition, how the CFPB evaluates applications, and what standard setters can expect once recognized. When submitting a request for recognition, the applicant should provide information sufficient to enable a determination by the CFPB of whether the applicant satisfies the requirements for recognition articulated in § 1033.141(a)(1) through (5). Other information provided, such as a description of how the applicant's current and/or anticipated standards relate to open banking, will help the CFPB understand the relevance of the standard setter to open banking.

The procedures also allow for a pre-filing meeting with the CFPB prior to submission of an application, so that the Bureau can provide information about the application process and assist organizations with submitting a complete application. During its review and discussions with the applicant, the CFPB may request additional information from the applicant necessary for the submission to be complete. Once it receives a complete application, the CFPB may publish the application, so as to enable stakeholders who believe the application is deficient to bring the

CFPB's attention to any evidence that might substantiate such claims of deficiency. In this event, the CFPB expects to ask the applicant to provide written responses to any such claims, which the CFPB can then consider as part of its review and assessment of the application. This procedure addresses comments requesting greater public participation in the recognition process.

The CFPB will consider the complete application, including any adverse evidence provided to the CFPB, to evaluate whether the applicant satisfies the recognition requirements articulated in § 1033.141(a)(1) through (5). The CFPB will also evaluate whether the information provided in the application is accurate and complete, including regarding the applicant's policies and actual practices.

As part of its evaluation of an application, the CFPB will consider how granting a recognition request might support its own role in open banking pursuant to its CFPA section 1033 authority. However, the CFPB is not adopting the recommendation of one trade association commenter that a standard-setting body should not be eligible for CFPB recognition unless it had already promulgated standards central to the safe and efficient operation of open banking. Rather, the CFPB is retaining the flexibility suggested by other commenters that will enable the CFPB to recognize an organization at earlier stages of standards development in a given area. The CFPB emphasizes, however, that a recognition request from an entity that has not adopted, and does not intend to adopt, standards relevant to the CFPB's statutorily-authorized objectives for open banking is unlikely to be prioritized and may not be approved.

In acting on an application, in addition to either recognizing or not recognizing an applicant, the CFPB may provide contingent recognition to an applicant that has presented a satisfactory written plan specifying how and when it will address contingencies that the CFPB has identified. Once the applicant presents sufficient evidence that it has addressed such contingencies, the CFPB may recognize the applicant. The CFPB expects to use contingent recognition, which is not formal recognition under § 12 CFR 1033.131, when it determines that an applicant is close to realizing, but has not yet realized, recognition requirements. The availability of contingent recognition responds to a trade association comment on the proposed rule that advocated for a phased approach to recognition, during which the CFPB would—before granting full recognition—offer feedback on steps to full recognition and support standard setters with garnering necessary stakeholder participation for recognition.

Consistent with trade association comments requesting that the CFPB publish a list of standard setters it recognizes, the CFPB will publicly disclose on its website each recognition and contingent recognition, along with the applicable terms and conditions of each. Some terms and conditions may be tailored to the circumstances of the applicant. For example, if the CFPB grants recognition based on the intention of a standard setter to develop and publish a consensus standard on a given subject matter, the CFPB may condition recognition on good faith efforts to develop a consensus standard in the given area.

Some commenters requested that the CFPB publish denials and include in its procedures a process to appeal such denials. The CFPB will publish denials as required by law, but applicants may also withdraw a pending application at any time for any reason. The CFPB is not providing a specialized appeals process. Consistent with the suggestion of one industry trade association, the CFPB may permit consultation with agency officials to help remedy issues after a submitted application is denied—although the agency intends pre-decisional consultation to minimize recourse to this option.

Next, the procedures describe the interaction between the CFPB and a standard setter once it is recognized. As noted above, each recognized standard setter must agree to a set of applicable terms and conditions. The procedures highlight terms and conditions related to CFPB observation

or participation in standard-setting activities, notification requirements on the part of the standard setter, and monitoring of the standard setter by the CFPB. They also explain how a standard setter may request re-recognition.

In view of a trade association comment noting the need for market participants to have adequate time to transition from a consensus standard if the associated standard setter's recognition expires, the procedures state that recognized standard setters intending to apply for re-recognition should do so at least 180 days before their recognition expires. The CFPB may temporarily extend a recognition while a re-recognition application is pending. Both provisions related to re-recognition are intended to reduce the likelihood that a consensus standard loses its status due to a recognition expiring before re-recognition is granted.

Finally, the procedures describe the circumstances under which the CFPB may modify or revoke recognition. One advocacy organization indicated that the CFPB should revoke recognition when requirements of recognition are no longer met. Other industry commenters stated that the CFPB should clarify the circumstances under which recognition may be revoked, and also allow for the standard setter to cure deficiencies.

The CFPB expects to base a modification or revocation decision, which it would publish on its website, on whether the standard-setting body has failed to comply with applicable terms and conditions, otherwise no longer meets the required attributes, or otherwise no longer warrants recognition. The CFPB also expects to inform the standard setter of reasons for modification or revocation, and to provide the standard setter with an opportunity to address concerns.

Regulatory Text

PART 1033—PERSONAL FINANCIAL DATA RIGHTS

SUBPART A—GENERAL

Sec.

1033.101 Authority, purpose, and organization.

1033.111 [Reserved].

1033.121 [Reserved].

1033.131 Definitions.

1033.141 Standard-setting bodies.

SUBPART B—[RESERVED]

SUBPART C—[RESERVED]

SUBPART D—[RESERVED]

APPENDIX A— HOW TO APPLY FOR RECOGNITION AS A STANDARD SETTER

SUBPART A—GENERAL

§ 1033.101 Authority, purpose, and organization.

(a) **Authority.** The regulation in this part is issued by the Consumer Financial Protection Bureau (CFPB) pursuant to the Consumer Financial Protection Act of 2010 (CFPA), Pub. L. 111-203, tit. X, 124 Stat. 1955.

(b) **Purpose.** This part implements the provisions of section 1033 of the CFPA, in part, by utilizing industry standards developed by standard-setting bodies recognized by the CFPB.

(c) ***Organization.*** This part is organized as follows:

(1) Subpart A establishes the authority, purpose, organization, and definitions applicable to this part, and is reserved for other purposes.

(2) Subpart B is reserved.

(3) Subpart C is reserved.

(4) Subpart D is reserved.

(5) Appendix A provides instructions for how a standard-setting body would apply for CFPB recognition.

§ 1033.111 [Reserved].

§ 1033.121 [Reserved].

§ 1033.131 Definitions.

For purposes of this part, the following definitions apply:

Consensus standard means a standard that is adopted by a recognized standard setter and that continues to be maintained by that recognized standard setter.

Recognized standard setter means a standard-setting body that has been recognized by the CFPB under § 1033.141.

§ 1033.141 Standard-setting bodies.

(a) ***Recognition of a standard-setting body.*** A standard-setting body may request CFPB recognition. Recognition will last up to five years, absent revocation. The CFPB will not recognize a standard-setting body unless it demonstrates that it satisfies the following attributes:

(1) **Openness:** The sources, procedures, and processes used are open to all interested parties, including: consumer and other public interest groups with expertise in consumer protection, financial services, community development, fair lending, and civil rights; authorized third parties; data providers; data recipients; data aggregators and other providers of services to authorized third parties; and relevant trade associations. Parties can meaningfully participate in standards development on a non-discriminatory basis.

(2) **Balance:** The decision-making power is balanced across all interested parties, including consumer and other public interest groups, and is reflected at all levels of the standard-setting body. There is meaningful representation for large and small commercial entities within these categories. No single interest or set of interests dominates decision-making. Achieving balance requires recognition that, even when a participant may play multiple roles, such as data provider and authorized third party, the weight of that participant's

commercial concerns may align primarily with one set of interests. The ownership of participants is considered in achieving balance.

(3) **Due process and appeals:** The standard-setting body uses documented and publicly available policies and procedures, and it provides adequate notice of meetings and standards development, sufficient time to review drafts and prepare views and objections, access to views and objections of other participants, and a fair and impartial process for resolving conflicting views. An appeals process is available for the impartial handling of procedural appeals.

(4) **Consensus:** Standards development proceeds by consensus, which is defined as general agreement, though not necessarily unanimity. During the development of consensus, comments and objections are considered using fair, impartial, open, and transparent processes.

(5) **Transparency:** Procedures or processes for participating in standards development and for developing standards are transparent to participants and publicly available.

SUBPART B—[RESERVED]

SUBPART C—[RESERVED]

SUBPART D—[RESERVED]

APPENDIX A TO PART 1033—PERSONAL FINANCIAL DATA RIGHTS RULE: HOW TO APPLY FOR RECOGNITION AS A STANDARD SETTER

If you want the CFPB to designate your organization as a recognized standard setter, you should follow the steps described below.

We may amend this process from time to time.

STEP ONE: REQUESTING RECOGNITION

Submit a written request for recognition.

This should include key contact information, evidence of your organization's policies and practices, and an explanation of how your organization satisfies each of the requirements in the Personal Financial Data Rights rule to be a recognized standard setter. Your request should also describe how current and/or anticipated standards issued by your organization relate to open banking.

In advance of filing your request, you can seek a pre-filing meeting with us. We can walk you through the application process and help you make a complete submission.

Send formal submissions, as well as requests for pre-filing meetings, to: openbankingstandards@cfpb.gov.

STEP TWO: ADDITIONAL INFORMATION AND PUBLIC COMMENT

After reviewing your submission, we may request additional information to ensure that your application is complete.

We may publish your application.

We may also seek public input on your application and invite your responses to any information we receive on that basis.

STEP THREE: OUR REVIEW

When reviewing your application, we consider whether your policies and practices meet all the requirements for recognition. We also evaluate whether your application is accurate and complete.

We prioritize and review applications based on the extent to which recognizing your organization helps us to implement open banking.

STEP FOUR: APPLICATION DECISION

CFPB recognition will be publicly disclosed on our website, along with the applicable terms and conditions of such recognition, such as its duration.

If the CFPB declines to recognize your organization, we will notify you.

You may withdraw your application at any time or for any reason.

If we determine that your organization is close to meeting, but does not yet meet, the requirements for CFPB recognition, we may ask you to provide a written plan specifying how and when you will take the steps required for full recognition. If that plan is satisfactory, we may state on our website that your organization has received contingent recognition. Once you provide us with evidence that you have successfully executed on that plan (or otherwise addressed the relevant contingences), the CFPB may extend full recognition.

STEP FIVE: RECOGNITION

There are several points to keep in mind about recognition.

As a recognized standard setter, you agree that the CFPB may monitor your organization and that you will provide information that we request.

You must also provide us, within 10 days, written explanation of any material change to information that was submitted with your application or during recognition, as well as any reason your organization may no longer meet underlying requirements for recognition.

In addition, you must meet any other specified terms and conditions of your recognition, which may include our reserving the right to observe or participate in standard setting.

If your recognition is set to expire, you can apply for re-recognition by re-starting at Step One at least 180 days before expiration. We may temporarily extend your recognition while we consider your request for re-recognition.

We may modify or revoke your recognition. The CFPB expects to notify you of the reasons it intends to revoke or modify recognition, and to provide your organization with an opportunity to address the CFPB's concerns.

What You Need to Do:

Review and share with affected team members; implement if applicable.

Section 4: Retail Nondeposit Investment Products

OCC: Handbook (June 11, 2024)

Link

https://occ.gov/publications-and-resources/publications/comptrollers-handbook/files/retail-nondeposit-invest-products/pub-ch-retail-nondeposit.pdf

Text

The Office of the Comptroller of the Currency (OCC) issued version 2.0 of the "Retail Nondeposit Investment Products" booklet of the *Comptroller's Handbook*. This booklet discusses risks and risk management practices associated with the recommendation or sale of nondeposit investment products to retail customers. This booklet also provides examiners with a framework for evaluating a bank's retail nondeposit investment product program.

The revised booklet replaces version 1.0 of the booklet with the same title issued January 2015. Also rescinded is OCC Bulletin 2015-2, "Retail Nondeposit Investment Products: Revised Comptroller's Handbook Booklet and Rescissions."

The revised booklet

- incorporates significant regulatory changes adopted in the U.S. Securities and Exchange Commission's Regulation Best Interest that may relate to banks' securities activities.
- reflects OCC and interagency issuances that have been published or rescinded since January 2015.
- provides further clarity regarding sound risk management practices and guidance to examiners.
- includes other minor updates for general clarity.

What You Need to Do:

Informational for OCC-supervised institutions.

Bank Secrecy Act

FRB: Resources to Combat Increased Check Fraud (April 4, 2024)

Link

https://www.consumercomplianceoutlook.org/2024/first-issue/compliance-spotlight/

Text

The Federal Reserve System (Federal Reserve) recognizes that check fraud is a top concern of bankers. In 2023, the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) noted that financial institutions reported 680,000 suspicious activity reports for possible check fraud in 2022, a significant increase from 2021. While the Federal Reserve actively monitors trends in check fraud, it generally does not intervene in fraud disputes between banks, including banks over which it may not be the primary federal banking regulator. The Federal Reserve is sharing these resources and sound practices to help financial institutions respond to check fraud.

- **The Federal Reserve**
  - ***Consumer Compliance Outlook* (*CCO*).** In 2018, *CCO* published an article titled "Responding to Counterfeit Instrument Scams." This article identifies common schemes involving counterfeit instruments and sound practices to mitigate risk.
  - ***Contact Us* link.** Financial institutions can communicate their concerns about check fraud and other issues to the Federal Reserve at this link. If a bank chooses to report a fraud incident, the notice should provide full details in the comment section at the bottom, without including any personally identifiable information. Board staff will review the information received, which may include sharing it within the Federal Reserve System and with other banking supervisory agencies.
- **FinCEN.** On February 27, 2023, FinCEN issued an alert about the surge in check fraud. This alert provides red flag indicators to assist financial institutions in meeting their Bank Secrecy Act obligation to identify and report suspicious activity. It emphasizes that information sharing among financial institutions is critical to identifying, reporting, and preventing mail-theft related check fraud. The alert strongly encourages financial institutions to share information under the safe harbor authorized by Section 314(b) of the USA PATRIOT Act; refer to FinCEN's Section 314(b) page for additional information.
- **U.S. Postal Inspection Service (USPIS).** The USPIS has published Tips & Prevention on scams in general, an information page on check fraud, and a brochure financial institutions can send to their customers, titled "Don't Be a Victim of a Check Scam." It also provides forms to report fraud.
- **The American Bankers Association (ABA).** The ABA's Check Fraud Claim Directory provides a searchable database of contact information for banks needing to file a check

warranty breach claim with another financial institution. To access the directory, a bank must participate by providing its fraud contacts but does not need to be an ABA member.

- **Check Service Providers.** Check service providers may offer products and services designed to mitigate check fraud, such as duplicate detect and positive pay products that can help spot duplicate check presentment or accelerated presentment options that may help institutions detect problems earlier in the check collection process. Institutions can contact their provider about whether these sorts of potential features are offered.

What You Need to Do:

Informational; please share with affected team members.

CCO occasionally issues individual Compliance Spotlights or Compliance Alerts to our electronic subscribers to share timely regulatory information. To receive Alerts and Spotlights electronically, go to the *CCO* home page and select the email notification link to subscribe.

FinCEN: Notice on the Use of Counterfeit U.S. Passport Cards to Perpetrate Identity Theft and Fraud Schemes at Financial Institutions (April 15, 2024)

Link

https://www.fincen.gov/sites/default/files/shared/FinCEN_Notice_Counterfeit_US_Passport_FINAL508.pdf

Text

The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN), in close coordination with the U.S. Department of State's Diplomatic Security Service (DSS), is issuing this Notice to financial institutions urging them to be vigilant in identifying and reporting suspicious activity related to the use of counterfeit U.S. passport cards for identity theft and fraud schemes (hereinafter, "U.S. passport card fraud"). Since 2018, DSS has identified a concerning increase in the use of counterfeit U.S. passport cards by individuals and fraud rings to gain access to victim accounts at financial institutions nationwide. This fraud occurs in person at financial institutions and involves an individual impersonating a victim by using a counterfeit U.S. passport card that contains the victim's actual information. DSS assesses that from 2018 to 2023, these schemes have resulted in $10 million in actual losses and $8 million in additional attempted losses, with over 4,000 victims in the United States. However, DSS and other law enforcement agencies assess that losses associated with U.S. passport card fraud and associated identity theft are likely significantly greater and seek increased reporting by financial institutions to identify additional illicit activity.

FinCEN is issuing this Notice to ensure that financial institutions identify and report suspicious activity potentially related to U.S. passport card fraud. This Notice: (i) provides an overview of several typologies related to U.S. passport card fraud; (ii) highlights select technical, behavioral, and financial red flags to assist financial institutions in identifying and reporting suspicious activity; and (iii) reminds financial institutions of their reporting requirements under the Bank Secrecy Act (BSA).

Fraud, including identity theft and impersonation schemes, is the largest source of illicit proceeds in the United States and represents one of the most significant money laundering threats to the United States as highlighted by the Department of the Treasury in its latest National Money Laundering Risk Assessment. Combating fraud is one of FinCEN's Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) National Priorities.

The information contained in this Notice is derived from open-source reporting and information provided by DSS and other law enforcement partners.

Emerging Risks and Typologies of Identity Theft and Fraud Schemes Involving Counterfeit U.S. Passport Cards

Counterfeiting of U.S. Passport Cards

According to DSS and other law enforcement agencies, individuals and fraud rings are falsely making, selling, and using counterfeit U.S. passport cards to impersonate and defraud persons holding accounts at financial institutions. Illicit actors are counterfeiting U.S. passport cards because U.S. passport cards are a less familiar form of U.S. government-issued identification, thereby potentially decreasing the likelihood of detection by financial institutions. U.S. Passport cards are also significantly cheaper to counterfeit compared to U.S. passport books.

U.S. Passport Card

The U.S. passport card is a REAL ID compliant identity and travel document issued by the U.S. Department of State for use by U.S. citizens. It can be used for purposes of identity, proof of U.S. citizenship, domestic air travel, and land and sea border crossings into the United States from Canada, Mexico, the Caribbean, and Bermuda. The U.S. Department of State began issuing the passport card in July 2008 as an alternative travel document to the U.S. passport book. The passport card provides a less expensive, smaller, and convenient alternative to the U.S. passport book for those who travel frequently to these destinations by land or by sea.

Illicit actors acquire a potential victim's personal identifiable information (PII) from either the U.S. Mail or the Darknet. Using the stolen PII, the illicit actors create—or order and purchase from other fraud rings—a counterfeit U.S. passport card that includes a passport photo of themselves or of a "money mule" they have recruited to participate in the scheme, but which reflects the PII of the victim.

Identity Theft and Fraud Typologies Using Counterfeit U.S. Passport Cards

After creating a fraudulent U.S. passport card, the illicit actor or the money mule will use the fraudulent identification to impersonate the victim at a branch of the victim's known financial institution. The illicit actors may avoid branches of the financial institution the victim frequents to evade detection by employees who may be familiar with, or recognize, the victim. If the illicit

actor's identity is called into question by financial institution staff and they are asked to present a second form of identification, they may present a counterfeit credit card bearing the name of the victim they are impersonating as proof of identity.

U.S. Passport Card Fraud

It is a federal crime to make, forge, counterfeit, mutilate, or alter any passport card with the intent to use it. It is also a federal crime to willfully and knowingly use, or attempt to use, or furnish to another for use any such false, forged, counterfeited, mutilated, or altered passport card.

However, these credit cards are also usually fraudulent and not tied to any account or third-party vendor. DSS has indicated that it is a common tactic for illicit actors to work in pairs and that money mules may be directed by phone from a vehicle outside of the financial institution or located somewhere off premises. In the event an imposter cannot answer specific questions regarding their victim's identity, they may be fed information from their co-conspirator or handlers through an earpiece or other inconspicuous device.

Upon successfully bypassing account access security protocols at the branch location, DSS has observed that illicit actors may attempt the following transactions:

1. The illicit actor will seek to gain information about a victim's account, by, for example, asking questions regarding the account balance and withdrawal limits. Once such information is obtained, the illicit actor will quickly withdraw large amounts of cash below the Currency Transaction Reporting (CTR) threshold, purchase cashier's checks or money orders, or initiate wires. To evade the CTR threshold, the illicit actor may visit other bank branch locations and repeat the process, using the same victim's information.
2. The illicit actor cashes stolen or forged checks to obtain funds from a victim's account.
3. The illicit actor establishes a new joint account, using the victim's account information, with a second illicit actor as a joint owner. After the joint account is established in person, the illicit actor will then transfer funds out of the victim's existing account into the newly established joint account. The funds in the joint account are then wired to other accounts wholly controlled by illicit actors.

In each of these cases, the objective is to expeditiously remove all remaining funds from a victim's account. Once successful, the illicit actor may quickly move on to their next victim with a new counterfeit U.S. passport card and repeat the fraud scheme.

Case Study

Fraudster Sentenced to 13+ Years in $1.9 Million Scheme

Nohmaan Malik, 30, pleaded guilty in November 2022 to conspiracy to commit bank fraud, passport fraud, and aggravated identity theft. Malik, the mastermind behind the $1.9 million bank fraud, was sentenced to more than 13 years in federal prison. The Court ordered restitution in the amount of $1.9 million, the amount of loss the victims suffered. According to plea papers, Mr. Malik admitted he and coconspirators defrauded Chase Bank customers. They selected customers with sizeable balances at Chase and created counterfeit passport cards using the customers' names and identifying information but with conspirators' photographs. Using those counterfeit passport cards, conspirators imitating the bank customers opened fraudulent joint bank accounts with other conspirators acting as money mules. The impersonator or the money mule then transferred money from the customers' actual account to the joint bank account, and then transferred the money from the joint account into a third bank account controlled solely by the conspirators.

Red Flag Indicators of Identity Theft and Fraud Involving Counterfeit U.S. Passport Cards

FinCEN, in consultation with DSS, has identified the following red flag indicators to help detect, prevent, and report potential suspicious activity related to the use of counterfeit passport cards in identity theft and fraud schemes. Because no single red flag is determinative of illicit or other suspicious activity, financial institutions should consider the surrounding facts and circumstances, such as a 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 transaction or attempted transaction is indicative of identity theft and fraud involving the use of counterfeit U.S. passport cards or is otherwise suspicious.

Technical Red Flags

1. The photo on the presented U.S passport card has a white, blurry border; a dark gray square surrounding the photo; or is in color. Legitimate U.S. passport cards are laser engraved, which produces a clear and crisp grayscale portrait image.
2. The photo of the account holder on file does not match the individual present who is pictured in the counterfeit U.S. passport card.
3. The card bearer's date of birth and other areas of text are flat and do not feel raised when touched. Legitimate U.S. passport cards have tactile text on certain areas of the card and should feel textured.
4. The holographic U.S. Department of State seal is missing or has been substituted with a seal from an unrelated agency.
5. The smaller portrait is blurry and does not contain micro-printed text with information specific to the bearer of the card, or the portraits are of different people. On legitimate U.S. passport cards, the secondary photo is a complex image that contains personalized details that are microprinted to create the image.
6. The signature of a customer presenting a U.S. passport card for identification does not match the customer's signature card on file.

Behavioral Red Flags

7. A customer presenting a U.S. passport card as identification may not know or be able to reference personal identifiers, including date of birth or social security number.
8. If a customer presenting a U.S. passport card as identification does know or is able to reference personal identifiers, including date of birth or social security number, they nevertheless lack basic account knowledge and are excessively interested in specific details about their account balances and withdrawal limits.
9. A customer appears to be following directions by phone from a third-party.
10. A customer presents a U.S. passport card for identification and opens a new joint account with a third-party with whom the customer has no prior relationship.
11. A customer conducts transactions characteristic of U.S. passport card fraud at branch locations outside of their geographical footprint.

Financial Red Flags

12. A customer presents a U.S. passport card as a form of identification and subsequently withdraws cash, purchases a cashier's check, purchases money orders, or initiates wire transfers for a large amount for no business or apparent lawful purpose.
13. A customer presents a U.S. passport card as a form of identification and attempts to negotiate an uncharacteristic, sudden, or abnormally large volume of checks made payable to cash.
14. A customer presents a U.S. passport card as a form of identification, asks for daily withdrawal and transfer limits, and subsequently withdraws cash, initiates a wire transfer, or purchases a cashier's check made payable to a third party.
15. A customer presents a U.S. passport card before transferring funds out of an existing account to a recently established joint account, and the funds are then rapidly withdrawn or wired from the joint account to a separate, unrelated account.
16. A customer makes withdrawals from an account at multiple branch locations for no business or apparent lawful purpose using a U.S. passport card as identification.
17. A customer engages in behavior that suggests efforts to evade the CTR filing requirements (e.g., the customer alters or cancels a transaction when informed of the CTR filing requirement, or engages in structuring by conducting multiple cash withdrawals below $10,000 during one business day).

Appendix: Security Features of Legitimate U.S. Passport Cards

CHECK VISUALLY

1. A complex holographic security feature overlaps the lower right of the card bearer's portrait. Tilt the hologram to see animation. Be suspicious if the hologram artwork is poor or the colors don't change
2. The back of the card contains a patch of color shifting ink. When tilted, it changes from gold to green. Be suspicious if the quality of the artwork is poor or the ink does not change color when tilted.

CHECK VISUALLY AND BY TOUCHSS

3. Textured, clear artwork of the Great Seal of the United States intersects the upper left of the card bearer's portrait. Be suspicious if the artwork is missing, blurry, or does not have a texture.
4. The card bearer's date of birth, and some other areas of the text, is deep black and has a distinct texture. Be suspicious if the date of birth print does not feel rough when touched.

CHECK WITH MAGNIFICATION OR ULTRAVIOLET LIGHT

5. The large portrait on the left is grayscale and contains fine lines that can be inspected with a magnifier. Be suspicious if the portrait is in color, is of poor quality, or obscures the red and blue art behind it.
6. When checked with a magnifier, the small portrait contains tiny text with information specific to the owner of the card. Be suspicious if the text is blurry or the two portraits are of different people.
7. The colorful background artwork contains tiny text in several different locations. When checked with a magnifier, be suspicious if this microprinting is unreadable or if the background art is blurry.
8. Passport cards contain invisible printing that can only be inspected with ultraviolet (UV) light. Be suspicious if the UV art is missing, shows different graphics, or is discontinuous over the portrait.

Reporting U.S. Passport Card Fraud to DSS

In addition to filing a SAR, financial institutions are encouraged to refer their customers who may be victims of U.S. passport card fraud to DSS. Victims and financial institutions can report U.S. passport card fraud by contacting their nearest DSS field office or sending an email to DSS at DS_DO_USPCFraud@state.gov.

Reminder of Relevant BSA Obligations and Tools for U.S. Financial Institutions

Suspicious Activity Reporting

A financial institution is required to file a SAR if it knows, suspects, or has reason to suspect a transaction conducted or attempted by, at, or through the financial institution involves funds derived from illegal activity; is intended or conducted to disguise funds derived from illegal activity; is designed to evade regulations promulgated under the BSA; lacks a business or apparent lawful purpose; or involves the use of the financial institution to facilitate criminal activity. All statutorily defined financial institutions may voluntarily report suspicious transactions under the existing suspicious activity reporting safe harbor.

When a financial institution files a SAR, it is required to maintain a copy of the SAR and the original or business record equivalent of any supporting documentation for a period of five years from the date of filing the SAR. Financial institutions must provide any requested SAR and all documentation supporting the filing of a SAR upon request by FinCEN or an appropriate law enforcement or supervisory agency. When requested to provide supporting documentation, financial institutions should take special care to verify that a requestor of information is, in fact, a representative of FinCEN or an appropriate law enforcement or supervisory agency. A financial

institution should incorporate procedures for such verification into its BSA compliance or AML program. These procedures may include, for example, independent employment verification with the requestor's field office or face-to-face review of the requestor's credentials.

SAR Filing Instructions

SARs, and compliance with other BSA requirements, are crucial to identifying and stopping U.S. passport card identity theft and fraud schemes. FinCEN requests that financial institutions indicate a connection between the suspicious activity being reported and the activities highlighted in this notice by including the key term "**FIN-2024-NTC1**"in SAR field 2 (Filing Institution Note to FinCEN), as well as in the narrative. Financial institutions may highlight additional advisory or notice keywords in the narrative, if applicable.

Financial institutions should select SAR Field 34(z) (FRAUD-Other) as the associated suspicious activity type and include the term "**Passport Card**" in the text box. Financial institutions also should select all other relevant suspicious activity fields, such as those in SAR Fields 36 (Money Laundering) and 38 (Other Suspicious Activities), if applicable.

Financial institutions should include all available information relating to the account and locations involved in the reported activity, identifying information related to other entities and persons involved in the depositing or cashing of suspicious checks and the status of their accounts with the institution. Financial institutions also should provide all available information regarding other domestic and foreign financial institutions involved in the activity; where appropriate, financial institutions should consider filing a SAR jointly on shared suspicious activity.

Other Relevant BSA Reporting Requirements

Financial institutions and other entities or persons also may have other relevant BSA reporting requirements to provide information in connection with the subject of this notice. These include obligations related to the Currency Transaction Report (CTR), Report of Cash Payments Over $10,000 Received in a Trade or Business (Form 8300), Report of Foreign Bank and Financial Accounts (FBAR), Report of International Transportation of Currency or Monetary Instruments (CMIR), Registration of Money Services Business (RMSB), and Designation of Exempt Person (DOEP). These standard reporting requirements may not have an obvious connection to illicit finance, but may ultimately prove highly useful to law enforcement.

Form 8300 Filing Instructions

When filing a Form 8300 involving a suspicious transaction relevant to this Notice, FinCEN requests that the filer select ***Box 1b*** ("suspicious transaction") and include the key term "**FIN-2024-NTC1**" in the "**Comments**" section of the report.

Information Sharing

Information sharing among financial institutions is critical to identifying, reporting, and preventing identity theft and fraud schemes involving counterfeit U.S. passport cards or other illicit financial activity. Financial institutions and associations of financial institutions sharing information under the safe harbor authorized by section 314(b) of the USA PATRIOT Act are reminded that they may share information with one another regarding individuals, entities, organizations, and countries suspected of possible terrorist financing or money laundering.

FinCEN strongly encourages such voluntary information sharing. FinCEN encourages U.S. financial institutions to use, and potentially expand, their existing processes to collect and share information with foreign financial institutions in furtherance of investigations that involve cross-border activity.

For Further Information

FinCEN's website at https://www.fincen.gov/ contains information on how to register for FinCEN Updates. Questions or comments regarding the contents of this Notice should be addressed to the FinCEN Regulatory Support Section at frc@fincen.gov.

What You Need to Do:

Please share with BSA Officer and other affected team members.

FinCEN: Real Estate Geographic Targeting Orders (April 17, 2024)

Link

https://www.fincen.gov/sites/default/files/shared/RRE-GTOs-Phase-18-Order.pdf

Text

The Financial Crimes Enforcement Network (FinCEN) announced the renewal of its Geographic Targeting Orders (GTOs) that require U.S. title insurance companies to identify the natural persons behind shell companies used in non-financed purchases of residential real estate.

The terms of the GTOs are effective beginning April 19, 2024, and ending on October 15, 2024. The GTOs continue to provide valuable data on the purchase of residential real estate by persons possibly involved in various illicit enterprises. Renewing the GTOs will further assist in tracking illicit funds and other criminal or illicit activity, as well as continuing to inform FinCEN's regulatory efforts in this sector. FinCEN renewed the GTOs that **cover *certain counties and major U.S. metropolitan areas in California, Colorado, Connecticut, Florida, Hawaii, Illinois, Maryland, Massachusetts, Nevada, New York, Texas, Washington, Virgina, and the District of Columbia.***

The purchase amount threshold remains $300,000 for each covered metropolitan area, with the exception of the City and County of Baltimore, where the purchase threshold is $50,000.

FinCEN appreciates the continued assistance and cooperation of title insurance companies and the American Land Title Association in protecting real estate markets from abuse by illicit actors.

In February 2024, FinCEN issued a notice of proposed rulemaking for an anti-money laundering regulation in the residential real estate sector. The comment period for the proposed rule closed on April 16, 2024 and FinCEN is renewing the GTOs while it reviews and considers

all of the comments submitted.

Any questions about the Orders should be directed to FinCEN's Regulatory Support Section at FRC@FinCEN.gov.

What You Need to Do:

Informational; please share with interested team members.

FinCEN: Analysis on Elder Financial Exploitation (April 18, 2024)

Link

https://www.fincen.gov/sites/default/files/shared/FTA_Elder_Financial_Exploitation_508Final.pdf

Text

The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) issued a Financial Trend Analysis focusing on patterns and trends identified in Bank Secrecy Act (BSA) data linked to Elder Financial Exploitation (EFE), or the illegal or improper use of an older adult's funds, property, or assets. FinCEN examined BSA reports filed between June 15, 2022 and June 15, 2023 that either used the key term referenced in FinCEN's or checked "Elder Financial Exploitation" as a suspicious activity type. This amounted to 155,415 filings over this period indicating roughly $27 billion in EFE-related suspicious activity.

Financial institutions began filing BSA reports featuring the advisory's key term on the same day that FinCEN published its 2022 advisory. FinCEN has continued to receive EFE BSA reports, averaging 15,993 per month between June 15, 2023 and January 15, 2024. Banks have submitted the vast majority of EFE-related BSA filings.

EFE typically consists of two subcategories: elder scams and elder theft. Elder scams, identified in approximately 80% of the EFE BSA reports that FinCEN analyzed, involve the transfer of money to a stranger or imposter for a promised benefit that the older adult does not receive. In elder theft, identified in approximately 20% of the reports, an otherwise trusted person steals an older adult's assets, funds, or income. Among other conclusions, FinCEN's analysis revealed that most elder scam-related BSA filings referenced "account takeover" by a perpetrator unknown to the victim; that adult children were the most frequent elder theft-related perpetrators; and that illicit actors mostly relied on unsophisticated means to steal funds that minimize direct contact with financial institution employees.

EFE-related losses affect personal savings, checking accounts, retirement savings, and investments, and can severely impact victims' well-being and financial security as they age. In addition to filing a Suspicious Activity Report, FinCEN recommends that financial institutions refer customers who may be victims of EFE to the Department of Justice's National Elder Fraud Hotline at 833-FRAUD-11 or 833-372-8311 for assistance with reporting suspected fraud to the

appropriate government agencies. Additionally, FinCEN recommends EFE victims file incident reports to the FBI's Internet Crime Complaint Center (IC3) and the Federal Trade Commission. For educational resources on EFE and scams targeting older adults, please see the Consumer Financial Protection Bureau's Office for Older Americans and the Department of Justice's resources provided as part of World Elder Abuse Awareness Day, which is June 15.

What You Need to Do:

Informational; please share with BSA Officer and other affected team members.

FinCEN: Reminder to Remain Vigilant to Environmental Crimes (April 22, 2024)

Link

https://www.fincen.gov/news/news-releases/fincen-reminds-financial-institutions-remain-vigilant-environmental-crimes

Text

As the nation reflects on the many ways to protect our environment this Earth Day, the Financial Crimes Enforcement Network (FinCEN) reminds financial institutions to remain vigilant in identifying and reporting suspicious activity related to environmental crimes. Environmental crimes frequently involve transnational criminal activity related to several of FinCEN's Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) National Priorities, including corruption, fraud, human trafficking, and drug trafficking.

FinCEN has previously published resources to help stakeholders identify and combat environmental crimes and associated illicit financial activity. FinCEN's December 2021 Financial Threat Analysis contains information on wildlife trafficking threat patterns and trend information identified in Bank Secrecy Act (BSA) data. FinCEN's Notice FIN-2021-NTC4 provides financial institutions with specific Suspicious Activity Report (SAR) filing instructions and highlights illicit financial activity related to several types of environmental crimes such as wildlife trafficking and illegal logging, fishing, or mining. SAR filings, along with effective implementation of BSA compliance requirements, are crucial to identifying and stopping environmental crimes and related money laundering.

FinCEN Resources on Environmental Crimes

- Financial Threat Analysis: Illicit Finance Threat Involving Wildlife Trafficking and Related Trends in Bank Secrecy Act Data (December 2021)
- FIN-2021-NTC4: FinCEN Calls Attention to Environmental Crimes and Related Financial Activity (November 2021)

What You Need to Do:

Informational; please share with BSA Officer and other affected team members.

FinCEN: Advisory on Iran-Backed Terrorist Organizations (May 8, 2024)

Link

https://www.fincen.gov/sites/default/files/advisory/2024-05-07/FinCEN-Advisory-Iran-Backed-TF-508C.pdf

Text

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to assist financial institutions in detecting potentially illicit transactions related to Islamic Republic of Iran (Iran)-backed terrorist organizations amid intensified terrorist activity in the Middle East. Recent events have underscored Iran's involvement in and financing of terrorist activity in the region. Iran seeks, among other goals, to project power by exporting terrorism throughout the Middle East and beyond through the financing of a range of regional armed groups, some of which are U.S.-designated Foreign Terrorist Organizations (FTOs) or Specially Designated Global Terrorist organizations (SDGTs). These terrorist organizations include Lebanese Hizballah (Hizballah), Hamas, the Palestinian Islamic Jihad (PIJ), the Houthis (Ansarallah), and several Iran-aligned militia groups in Iraq and Syria. As demonstrated by the October 7, 2023, Hamas attack on Israel and recent Houthi attacks in the Red Sea, these organizations are capable of perpetrating horrific violence, causing destruction, and disrupting critical supply chains. The U.S. Department of the Treasury (Treasury) has been systematically working to dismantle these organizations by disrupting their illicit finance networks and eliminating their sources of revenue.

This advisory highlights the means by which terrorist organizations receive support from Iran and describes several typologies these terrorist organizations use to illicitly access or circumvent the international financial system to raise, move, and spend funds. It also provides red flags that may assist financial institutions in identifying related suspicious activity and is consistent with FinCEN's National Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Priorities, which include terrorist financing.

The information contained in this advisory is derived from FinCEN's analysis of Bank Secrecy Act (BSA) data, open-source reporting, and information provided by law enforcement partners.

How Iran Raises and Moves Funds in Support of Terrorism

Iran supports its numerous terrorist partners and proxies through the Islamic Revolutionary Guard Corps (IRGC), a parallel organization to Iran's regular armed forces. In particular, the IRGC division known as the IRGC-Qods Force (IRGC-QF) is responsible for conducting covert lethal activities outside of Iran, such as supporting terrorism globally and serving as a conduit for funds, training, and weapons to Iran-aligned partners and proxies.

Iran's Sources of Foreign Revenue

Iran uses the revenue from the sale of commodities, particularly oil, to countries such as the People's Republic of China (PRC) to fund its terrorist proxies. Following the reimposition of U.S. sanctions against Iran's petroleum sector in 2018, Iran's ability to finance itself through sales of crude oil and petroleum products—its most important economic sector—was severely diminished. In response, Iran established large-scale global oil smuggling and money laundering networks to enable access to foreign currency and the international financial system through the illicit sale of crude oil and petroleum products in global markets.

In 2021, the National Iranian Oil Company sold approximately $40 billion worth of products, and its crude oil and condensate exports reached an average of more than 600,000 barrels per day, with nearly all of it sent to the PRC and Syria. Iran's exports to the PRC have increased over time, reaching approximately 1.3 million barrels per day in 2023. Some of these oil proceeds finance the activities of the IRGC-QF and other terrorist groups. To restrict these sources of revenue, Treasury has designated numerous Iranian- and third-country operatives, front companies, and ships involved in Iran's oil smuggling networks.

Proceeds from Iran's sale of weapons and unmanned aerial vehicles (UAVs), including to buyers in Russia, also benefit the Iranian military, including the IRGC-QF. In response, Treasury has also designated companies that enable Iran's UAV production.

Case Study

In February 2024, the U.S. Department of Justice (DOJ) indicted seven defendants, including a senior IRGC-QF official and officers of a Turkish energy group, on terrorism, sanctions evasion, fraud, and money laundering charges in connection with their illicit billion-dollar network that enabled Iran to sell its oil products to government-affiliated buyers in the PRC, Russia, and Syria and to gain access to foreign currency. The United States seized $108 million that China Oil & Petroleum Limited, a Hong Kong-based IRGC front company, attempted to launder through correspondent transaction accounts at U.S. financial institutions in furtherance of the scheme to fund the IRGC-QF's malign activities through the illicit sale of Iranian oil. In furtherance of this scheme, the defendants charged in the U.S. District Court for the Southern District of New York used a myriad of deceptive techniques including: (1) the use of front companies and intermediaries in countries outside of Iran to disguise the IRGC's role in the oil transactions and the Iranian source of the oil; (2) the use of falsified documentation to misrepresent the source of the oil and deceive unwitting companies and banks to provide services in furtherance of the scheme; and (3) the use of ship-to-ship transfers and the manipulation of location and shipping data for vessels to obscure the loading and unloading of Iranian oil cargoes and therefore avoid identifying vessels used to facilitate oil smuggling.

Likewise, defendants charged in a related U.S. District Court for the District of Columbia indictment allegedly negotiated the sale of and sold illicit Iranian oil to buyers in the PRC. They allegedly obtained the oil from Iran using surreptitious means, and the scheme relied on the use of the U.S. financial system. According to the indictment, the defendants created fraudulent documents to mask the oil's Iranian origin, used electronic communications to arrange for Chinese buyers, used shell corporations to launder the proceeds through the U.S. financial system, provided false information to the U.S. companies about the source of funds generated by the transactions, and used U.S. companies as a "trust" to hold the profits for the IRGC.

Moving the Money

Iranian government agencies, such as the Central Bank of Iran (CBI) and the IRGC-QF, as well as state-sponsored organizations such as Hizballah, play a key role in channeling funds to terrorist proxies using overseas front companies and financial institutions. Financial institutions located outside Iran can—wittingly or unwittingly—become intermediaries for the IRGC-QF's illicit transactions. IRGC-QF officials have been known to collect funds in various currencies from CBI-held accounts at financial institutions in neighboring countries and transfer those funds back to Iran or to terrorist organizations. According to BSA analysis, third-country front companies—often incorporated as "trading companies" or "general trading companies"—and exchange houses act as a global "shadow banking" network that processes illicit commercial transactions and channels money to terrorist organizations on Iran's behalf. Exchange houses and front companies rely on banks with correspondent accounts with U.S. financial institutions, especially to process dollar-denominated transactions. In such cases, Iranian banking customers may omit or falsify identifying details connecting themselves or the transfers to Iran or attempt to pass the transactions off as remittances.

In addition, Iran uses cultural and religious foundations as front organizations for funneling money to terrorist organizations under the guise of cultural or religious support. In 2020, Treasury sanctioned the Reconstruction Organization for the Holy Shrines in Iraq (ROHSI). Ostensibly a religious institution devoted to restoring and preserving Shiite shrines in Iraq, ROHSI is in reality an IRGC-QF front organization that channels funds to terrorist organizations.

Typologies Associated with Iran-Backed Terrorist Organizations

In addition to receiving support from Iran, terrorist organizations and Iran-aligned militia groups in Iraq and Syria employ a range of other mechanisms to raise revenue, including sham or fraudulent charities, engaging in illicit trade activities like arms and drug trafficking, taxing and extorting local populations, and crowdfunding.

Hamas

Hamas is a Sunni terrorist organization based predominantly in the Gaza Strip whose goal is the destruction of Israel and its replacement with an Islamic Palestinian state. Hamas has exercised de facto control over Gaza since 2007, which enabled the group to derive revenue from taxes and fees it imposed on the local population. Until October 2023, Hamas levied taxes on commodities, imports, and businesses operating in Gaza, and charged fees for licenses, birth certificates, customs duties, and vehicles. This source of revenue has effectively disappeared since the October 7, 2023, attacks on Israel and ongoing armed conflict in Gaza, leaving Hamas largely dependent on support from Iran, crowdfunding contributions, and whatever revenue the group can generate from its investment portfolio.

Hamas and its armed element, the Al-Qassam Brigades, have received support from Iran since the 1990s through networks of corporations, banks, and individuals located in multiple countries, including the People's Democratic Republic of Algeria (Algeria), the Republic of Lebanon (Lebanon), the Kingdom of Saudi Arabia (Saudi Arabia), the Republic of Sudan (Sudan), the Republic of Türkiye (Türkiye), and the United Arab Emirates (UAE), that help transfer money directly to Hamas. Iran has provided as much as $100 million per year to Hamas since 2018. To disrupt these sources of support, Treasury has sanctioned numerous financial intermediaries between Iran and Hamas, including money transfer companies, financiers and financial

facilitators who manage Hamas's assets and facilitate money transfers for the organization, and political liaisons to the Government of Iran.

Hamas also has a history of using "sham" charities: usually foreign non-profit organizations (NPOs) that claim to provide humanitarian assistance but instead primarily or exclusively funnel money to terrorist organizations, exploiting the trust and credibility associated with charitable giving. In addition, Hamas and other terrorist groups have exploited crowdfunding and social media platforms to raise funds under the guise of humanitarian or charitable causes worldwide. According to analysis of BSA data, these donations are often placed in bank accounts in third countries, including Lebanon, the State of Qatar (Qatar), and Türkiye, which are then accessed by individuals operating in the Gaza Strip.

Additionally, Hamas has used convertible virtual currency (CVC) for fundraising, leveraging money exchangers that have incorporated CVC into their operations to facilitate cross-border transfers, probably seeking to benefit from the perceived anonymity afforded by certain CVC transactions and the lax regulatory oversight of virtual asset service providers (VASPs) in some high-risk jurisdictions. Hamas has sought CVC contributions in donation drives since at least 2019, and has historically leveraged VASPs in an attempt to safeguard the anonymity of their donors. There is evidence, however, that Hamas has reacted to law enforcement action targeting its use of CVC. For instance, in April 2023, the al-Qassam Brigades announced that they would no longer accept Bitcoin donations, warning that donors could be targeted.

Houthis

The Houthis, or Ansarallah, are an Iran-backed Zaidi Islamist movement that arose in Northern Yemen in 2004. In 2014, the Houthis launched a military campaign to overthrow the internationally recognized Yemeni government, initiating a bloody civil war. Today, the Houthis control a large portion of northern Yemen, including the former capital, Sana'a.

Following the Hamas attacks on Israel on October 7, 2023, the Houthis began attacking commercial and naval vessels transiting the Red Sea and Gulf of Aden. Since October 17, 2023, the Houthis have carried out more than 50 attacks on commercial vessels, forcing companies to divert their shipments to the much costlier route around Africa's Cape of Good Hope. In response, the U.S. Department of State redesignated the Houthis as a Specially Designated Global Terrorist (SDGT), effective February 16, 2024. The United States has also responded by launching Operation Prosperity Guardian, a naval coalition of more than 20 countries to protect commercial vessels; by leading a coalition that has conducted a series of strikes against Houthi targets in Yemen; and by imposing sanctions against the exchange houses and smuggling network through which Iran funds the Houthis.

Much of the Houthis' funding is raised and transferred by means of an elaborate smuggling network connected to Iran-based IRGC-QF-backed Houthi financial facilitator Said Al-Jamal. The network generates tens of millions of dollars in revenue annually through the sale of Iranian commodities like petroleum to customers in Asia, the Middle East, and Africa. Those funds are then funneled to the Houthis in Yemen through a complex network of exchanges and intermediaries spread across multiple countries. Al-Jamal also maintains connections to Hizballah and has worked with the group to send millions of dollars to benefit the Houthis. The Houthis also raise funds by collecting customs revenue from the Hudaydah and Salif ports in Yemen, appropriating public funds using fraudulent contracts, and unlawfully appropriating assets belonging to political opponents or those who have fled the country.

Hizballah

Formed in the wake of Israel's invasion of Lebanon in 1982, Hizballah is a strategic partner through which Iran projects power throughout the Middle East. While primarily based in Lebanon, Hizballah's activities extend to Syria, Iraq, and Yemen. Iran has provided hundreds of millions of dollars in support to Hizballah and has trained thousands of its fighters at camps in Iran. Hizballah in turn has trained and equipped other Iran-aligned militias in the region and acts as a conduit for funds from Iran's IRGC-QF to other Iran-aligned groups.

Estimates indicate that Iran has historically provided Hizballah with approximately $700 million of Hizballah's estimated $1 billion annual budget. While Iran has supported Hizballah and others through a vast network of front companies, banks, and individuals, Hizballah also finances itself through a broad range of illicit activities, including oil smuggling, money laundering, drug trafficking, counterfeiting, and illegal weapons procurement. These activities are global in scale, encompassing the western hemisphere, Europe, Africa, and the Middle East, and often have a nexus to transnational organized criminal groups, drug trafficking organizations, and professional money laundering organizations.

Hizballah also utilizes networks of front companies and legitimate businesses, as well as cryptocurrencies, to raise, launder, and transfer funds. Hizballah financiers make use of free trade zones and countries with weak regulatory frameworks to establish import-export companies that facilitate trade-based money laundering schemes. These companies are often held in the name of a relative of the financier, for example a spouse. Hizballah operatives have been known to operate in the Tri-border area of Argentina, Brazil, and Paraguay, and in free trade zones in Chile and Panama, with members and supporters identified in Colombia and Peru as well. Hizballah's illicit activities also extend to Africa. In 2019, Treasury designated Nazem Said Ahmad, who had used his Africa-based diamond business to launder money on behalf of Hizballah, along with Saleh Assi, who used his Congo-based businesses to launder and raise funds for Hizballah.

Palestinian Islamic Jihad

PIJ is a Sunni Islamist terrorist organization operating in Gaza and the West Bank. It is the second-largest armed group in Gaza and receives support from Iran, Syria, and Hizballah. PIJ and Hamas share many similarities: both are violent offshoots of the Muslim Brotherhood; both seek to create an Islamic Palestinian state through the destruction of Israel; and both receive significant funding and support from Iran. Like Hamas and Hizballah, PIJ's operatives have been trained by Iran to use Iranian-made missiles for long-range rocket attacks against Israeli cities and to carry out suicide bombings.

PIJ relies on many of the same funding channels as Hamas. It receives much of its support from the IRGC and IRGC-QF, which distribute those funds through PIJ intermediaries or through Islamic National Bank of Gaza, which was designated by Treasury in 2010 for being controlled by Hamas. Also like Hamas, PIJ makes use of sham charities to move and launder funds. In 2023, Treasury sanctioned the Al-Ansar Charity Foundation and the Muhjat al-Quds Foundation, through which Iran provided financial support to PIJ fighters and their families.

Iran-aligned Militia Groups in Iraq and Syria

Some of the most prominent Iran-aligned militia groups in Iraq are Kata'ib Hizballah (KH), Kata'ib Sayyid al Shuhada (KSS), Asa'ib Ahl al-Haq (AAH), and Harakat al-Nujaba (HaN). These groups have received support, training, weapons, and intelligence from the IRGC-QF and

Hizballah. These groups have also abused the Iraqi financial system to generate revenue and launder money, including through the use of front companies, fraudulent documentation, identity theft, currency arbitrage, and counterfeit currency. Although some members of Iran-aligned militia groups operate within Iraq's official Popular Mobilization Forces (PMF), these groups frequently operate outside government control and conduct destabilizing attacks in Iraq and neighboring Syria as well as attacks against coalition forces seeking to defeat the Islamic State of Iraq and Syria (ISIS).

Red Flag Indicators Related to the Fundraising and Money Laundering Activities of Iran-Backed Terrorist Organizations

FinCEN has identified the red flags listed below to assist financial institutions in detecting, preventing, and reporting suspicious activity connected to the financing of Iran-backed terrorist organizations. These red flags are in addition to the red flags identified in FinCEN's 2018 Iran advisory and 2023 Hamas alert, all of which remain relevant. As no single red flag is determinative of illicit or suspicious activity, financial institutions should consider the surrounding facts and circumstances, such as a 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 indicative of terrorist finance or is otherwise suspicious.

1. A customer or a customer's counterparty conducts transactions with Office of Foreign Assets Control (OFAC)-designated entities and individuals, or transactions that contain a nexus to identifiers listed for OFAC-designated entities and individuals, to include email addresses, physical addresses, phone numbers, passport numbers, or CVC addresses.
2. Information included in a transaction between customers or in a note accompanying a peer-to-peer transfer include key terms known to be associated with terrorism or terrorist organizations.
3. A customer conducts transactions with a money services business (MSB) or other financial institution, including a VASP, that operates in jurisdictions known for, or at high risk for, terrorist activity and is reasonably believed to have lax customer identification and verification processes, opaque ownership, or otherwise fails to comply with AML/CFT best practices.
4. A customer conducts transactions that originate with, are directed to, or otherwise involve entities that are front companies, general "trading companies" with unclear business purposes, or other companies whose beneficial ownership information indicates that they may have a nexus with Iran or other Iran-supported terrorist groups. Indicators of possible front companies include opaque ownership structures, individuals and/or entities with obscure names that direct the company, or business addresses that are residential or co-located with other companies.
5. A customer that is or purports to be a charitable organization or NPO solicits donations but does not appear to provide any charitable services or openly supports terrorist activity or operations. In some cases, these organizations may post on social media platforms or encrypted messaging apps to solicit donations, including in CVC.
6. A customer receives numerous small CVC payments from many wallets, then transfers the funds to another wallet, particularly if the customer logs in using an Internet Protocol (IP) based in a jurisdiction known for, or at high risk for, terrorist activity. In such cases, financial institutions may also be able to provide associated technical details

such as IP addresses with time stamps and device identifiers that can provide helpful information to authorities.

7. A customer makes money transfers to a jurisdiction known for, or at high risk for, terrorist activity that are inconsistent with their stated occupation or business purpose with vague stated purposes such as "travel expenses," "charity," "aid," or "gifts.
8. A customer account receives large payouts from social media fundraisers or crowdfunding platforms and is then accessed from an IP address in a jurisdiction known for, or at high risk for, terrorist activity, particularly if the social media accounts that contribute to the fundraisers contain content supportive of terrorist campaigns.
9. A customer company is incorporated in the United States or a third-country jurisdiction, but its activities occur solely in jurisdictions known for, or at high risk for, terrorist activity and show no relationship to the company's stated business purpose.

Reminder of Relevant BSA Obligations and Tools for U.S. Financial Institutions

Suspicious Activity Reporting

A financial institution is required to file a suspicious activity report (SAR) if it knows, suspects, or has reason to suspect a transaction conducted or attempted by, at, or through the financial institution involves funds derived from illegal activity; is intended or conducted to disguise funds derived from illegal activity; is designed to evade regulations promulgated under the BSA; lacks a business or apparent lawful purpose; or involves the use of the financial institution to facilitate criminal activity. All statutorily defined financial institutions may voluntarily report suspicious transactions under the existing suspicious activity reporting safe harbor.

Financial institutions are required to file complete and accurate reports that incorporate all relevant information available. In situations involving violations requiring immediate attention, such as ongoing money laundering schemes, financial institution must also immediately notify, by telephone, an appropriate law enforcement authority and its regulator, in addition to filing a timely SAR. Valuable cyber indicators for terrorist finance-related law enforcement investigations can include relevant email addresses, IP addresses with their respective timestamps, login information with location and timestamps, virtual currency addresses, mobile device information (such as device International Mobile Equipment Identity (IMEI) numbers), and descriptions and timing of suspicious electronic communications.

When a financial institution files a SAR, it is required to maintain a copy of the SAR and the original or business record equivalent of any supporting documentation for a period of five years from the date of filing the SAR. Financial institutions must provide any requested documentation supporting the filing of a SAR upon request by FinCEN or an appropriate law enforcement or supervisory agency. When requested to provide supporting documentation, financial institutions should take special care to verify that a requestor of information is, in fact, a representative of FinCEN or an appropriate law enforcement or supervisory agency. A financial institution should incorporate procedures for such verification into its BSA compliance or AML program. These procedures may include, for example, independent employment verification with the requestor's field office or face-to-face review of the requestor's credentials.

SAR Filing Instructions

FinCEN requests that financial institutions indicate any connection between the suspicious activity being reported and the activities highlighted in this advisory by including the key term

"**IRANTF2024-A001**" in SAR field 2 ("Filing Institution Note to FinCEN"), as well as in the narrative. Financial institutions should select SAR Field 33(a) (Terrorist Financing-Known or suspected terrorist/terrorist organization) as the associated suspicious activity type. Financial institutions may highlight additional advisory or alert keywords in the narrative, if applicable.

Financial institutions should include all available information relating to the account(s) and location(s) 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. Financial institutions also should provide all available information regarding other domestic and foreign financial institutions involved in the activity; where appropriate, financial institutions should consider filing a SAR jointly on shared suspicious activity.

Financial institutions wanting to expedite their report of suspicious transactions that may relate to the activity noted in this alert should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day).

Other Relevant BSA Reporting Requirements

Financial institutions and other entities or persons also may have other relevant BSA reporting obligations to provide information in connection with the subject of this advisory. These include obligations related to the CTR, Report of Cash Payments Over $10,000 Received in a Trade or Business (Form 8300), Report of Foreign Bank and Financial Accounts (FBAR), Report of International Transportation of Currency or Monetary Instruments (CMIR), Registration of Money Services Business (RMSB), and Designation of Exempt Person (DOEP). These standard reporting requirements may not have an obvious connection to illicit finance, but may ultimately prove highly useful to law enforcement.

Form 8300 Filing Instructions

When filing a Form 8300 involving a suspicious transaction relevant to this advisory, FinCEN requests that the filer select ***Box 1b*** ("suspicious transaction") and include the key term "**IRANTF-2024-A001**"in the "**Comments**" section of the report.

Due Diligence

Banks, brokers or dealers in securities, mutual funds, and futures commission merchants and introducing brokers in commodities (FCM/IBs) are required to have appropriate risk-based procedures for conducting ongoing customer due diligence that include, but are not limited to: (i) understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and (ii) conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information. Covered financial institutions are required to identify and verify the identity of beneficial owners of legal entity customers, subject to certain exclusions and exemptions. Among other things, this facilitates the identification of legal entities that may be owned or controlled by foreign politically exposed persons (PEPs).

Senior foreign political figures and due diligence obligations for private banking accounts

In addition to these due diligence obligations, under section 312 of the USA PATRIOT Act (31 U.S.C. § 5318(i)) and its implementing regulations, covered financial institutions must implement due diligence programs for private banking accounts held for non-U.S. persons that are designed to detect and report any known or suspected money laundering or suspicious activity conducted through or involving such accounts. Covered financial institutions must establish risk-based controls and procedures for ascertaining the identities of nominal and beneficial owners of such accounts and ascertaining whether any of these owners are senior foreign political figures, and for conducting enhanced scrutiny on accounts held by senior foreign political figures that is reasonably designed to detect and report transactions that may involve the proceeds of foreign corruption.

AML/CFT program and correspondent account due diligence requirements

Financial institutions are reminded of AML/CFT program requirements, and covered financial institutions are reminded of correspondent account due diligence requirements under Section 312 of the USA PATRIOT Act (31 U.S.C. § 5318(i)) and implementing regulations. As described in FinCEN Interpretive Release 2004-1, the AML/CFT program of an MSB must include risk-based policies, procedures, and controls designed to identify and minimize risks associated with foreign agents and counterparties.

Information Sharing

Information sharing among financial institutions is critical to identifying, reporting, and preventing terrorist financing. Financial institutions and associations of financial institutions sharing information under the safe harbor authorized by section 314(b) of the USA PATRIOT Act are reminded that they may share information with one another regarding individuals, entities, organizations, and countries suspected of possible terrorist financing or money laundering. In accordance with the requirements of section 314(b) and its implementing regulations, FinCEN strongly encourages such voluntary information sharing as it relates to money laundering or possible terrorist financing in connection with Foreign Terrorist Organizations (FTOs) and Specially Designated Global Terrorists (SDGTs).

For Further Information

Additional questions or comments regarding the contents of this advisory should be addressed to the FinCEN Regulatory Support Section at frc@fincen.gov.

What You Need to Do:

Informational; please share with BSA Officer and other affected team members.

FinCEN: Remain Vigilant to Elder Financial Exploitation (June 14, 2024)

Link

https://www.fincen.gov/news/news-releases/fincen-reminds-financial-institutions-remain-vigilant-elder-financial

Text

As the nation recognizes World Elder Abuse Awareness Day, the Financial Crimes Enforcement Network (FinCEN) reminds financial institutions to remain vigilant in identifying and reporting suspicious activity related to elder financial exploitation (EFE). EFE-related losses affect personal savings, checking accounts, retirement savings, and investments, and can severely impact victims' well-being and financial security as they age. FinCEN has previously published resources to help stakeholders combat EFE.

Earlier this year, FinCEN issued an analysis focusing on patterns and trends identified in Bank Secrecy Act (BSA) data linked to EFE, which indicated roughly $27 billion in EFE-related suspicious activity. FinCEN examined BSA reports filed by financial institutions between June 15, 2022 and June 15, 2023 where filers either used the key term referenced in FinCEN's June 2022 EFE Advisory or checked "Elder Financial Exploitation" as a suspicious activity type. This amounted to 155,415 filings from financial institutions.

In addition to filing a Suspicious Activity Report, FinCEN recommends that financial institutions refer customers who may be victims of EFE to the Department of Justice's National Elder Fraud Hotline at 833-FRAUD-11 or 833-372-8311 for assistance with reporting suspected fraud to the appropriate government agencies. EFE victims can file incident reports to the Federal Bureau of Investigation's Internet Crime Complaint Center (IC3) and the Federal Trade Commission. For educational resources on EFE and scams targeting older adults, please see the websites of the Consumer Financial Protection Bureau's Office for Older Americans and the Department of Justice.

FinCEN Resources on Elder Financial Exploitation

- Financial Trend Analysis on Elder Financial Exploitation: Threat Pattern & Trend Information, June 2022 to June 2023 (April 2024)
- FinCEN Advisory on Elder Financial Exploitation [FIN-2022-A002] (June 2022)

What You Need to Do:

Informational; please share with BSA Officer and other affected team members.

FinCEN: Supplemental Advisory on the Illicit Procurement of Fentanyl Precursor Chemicals and Manufacturing Equipment (June 20, 2024)

Link

https://www.fincen.gov/sites/default/files/advisory/2024-06-20/FinCEN-Supplemental-Advisory-on-Fentanyl-508C.pdf

Text

Secretary of the Treasury Janet L. Yellen announced today that the Financial Crimes Enforcement Network (FinCEN) has issued an advisory to alert U.S. financial institutions to new trends in the illicit fentanyl supply chain and urge vigilance in identifying and reporting suspicious activity associated with Mexico-based transnational criminal organizations and their illicit procurement of fentanyl precursor chemicals and manufacturing equipment from People's Republic of China-based suppliers. The supplemental advisory builds off FinCEN's 2019 advisory with new typologies and red flags to identify and report suspicious transactions, and fulfills the requirement in Section 3202 of the recently enacted FEND Off Fentanyl Act. Financial institutions with questions about the content of today's supplemental advisory should contact the FinCEN Regulatory Support Section at frc@fincen.gov.

Introduction

Amidst a nationwide opioid epidemic, FinCEN urges vigilance in identifying potential suspicious activity related to the procurement of precursor chemicals, pill presses, die molds, and other manufacturing equipment used for the synthesis of illicit fentanyl and other synthetic opioids.

The opioid crisis continues to pose a significant threat to U.S. national security, economic prosperity, and communities, as illicit fentanyl and other synthetic opioids inflict an unprecedented epidemic of addiction and death across the nation. According to provisional data from the U.S. Centers for Disease Control and Prevention (CDC), over 107,000 Americans died from drug overdoses in the 12-month period ending in December 2023, with over 74,000 of those deaths involving synthetic opioids, principally illicitly manufactured fentanyl. Many of these overdose deaths are the result of fentanyl poisonings, where the victims were unaware that other illicit drugs or counterfeit prescription medications they used contained lethal doses of fentanyl. The social and economic costs from these deaths are sobering, far-reaching, and unprecedented, as American communities lose generations of parents, children, friends, and other loved ones to these deadly drugs.

As part of a larger U.S. government effort to call attention to and combat this unprecedented epidemic, the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) is issuing this supplemental advisory to U.S. financial institutions to highlight new trends in the illicit fentanyl supply chain since the publication of FinCEN's 2019 Advisory on Illicit Financial Schemes and Methods Related to the Trafficking of Fentanyl and Other Synthetic Opioids (hereafter "2019 Fentanyl Advisory"), and to urge vigilance in identifying and reporting related suspicious activity. While the 2019 Fentanyl Advisory and the typologies and red flags

therein remain valid, this supplemental advisory highlights how Mexico-based transnational criminal organizations (TCOs) purchase fentanyl precursor chemicals, pill presses, die molds, and other manufacturing equipment (hereafter "fentanyl precursor chemicals and manufacturing equipment") primarily originating from companies located in the People's Republic of China (PRC) to synthesize illicit fentanyl and other synthetic opioids in Mexico before the substances enter the illicit drug market in the United States.

In alignment with the Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) National Priorities, issued June 30, 2021, the 2024 National Money Laundering Risk Assessment, and in support of the Administration's whole-of-government approach to tackling global illicit drug trafficking, FinCEN is issuing this supplemental advisory, which includes typologies and red flags associated with the purchase of fentanyl precursor chemicals and manufacturing equipment, to assist U.S. financial institutions in identifying and reporting suspicious activity. This supplemental advisory also reminds U.S. financial institutions of their regulatory requirements under the Bank Secrecy Act (BSA) and its implementing regulations. U.S. financial institutions' BSA reporting to FinCEN allows law enforcement to follow the money behind the illicit fentanyl supply chain, identify and prosecute the illicit actors that profit off this unprecedented epidemic, and ultimately aid in the effort to save American lives.

The information contained in this supplemental advisory is derived from FinCEN's analysis of data collected from BSA-related reporting, open-source reporting, and information provided by law enforcement partners.

Recent Developments in the U.S. Opioid Crisis

Shift in the Illicit Fentanyl Supply Chain

U.S. law enforcement has observed a significant shift in the illicit fentanyl supply chain in recent years. Previously, complicit chemical and pharmaceutical companies based in the PRC (hereafter "PRC-based suppliers") directly shipped illicit fentanyl and other synthetic opioids to U.S.-based individuals for personal consumption or domestic distribution, or to TCOs and smaller criminal networks in Mexico to be trafficked into the United States across the U.S. southwest border. After the PRC government scheduled all fentanyl-related substances as a class in May 2019, the direct purchase and shipment of illicit fentanyl and other synthetic opioids from PRC-based suppliers declined substantially. Since 2019, Mexico-based TCOs, such as the Sinaloa Cartel and the Jalisco New Generation Cartel (CJNG), have become the predominant traffickers of illicit fentanyl and other synthetic opioids into the United States. The TCOs purchase fentanyl precursor chemicals and manufacturing equipment primarily from PRC-based suppliers to synthesize illicit fentanyl and other synthetic opioids in clandestine labs in Mexico.

Illicit fentanyl precursor chemicals and manufacturing equipment may be shipped directly from the PRC to Mexico, or be routed to Mexico through third-party jurisdictions, including the United States. After the TCOs use the precursor chemicals and manufacturing equipment to synthesize illicit fentanyl and other synthetic opioids in Mexico, the illicit drugs are typically smuggled across the U.S. southwest border as a powder, as an adulterant in other drugs, or pressed or encapsulated into counterfeit medication. Mexico-based TCOs and smaller criminal organizations then traffic the illicit fentanyl and other synthetic opioids to American consumers via person-to-person drug sales, through the mail from e-commerce marketplaces and Darknet vendors, and in-person deliveries arranged on social media platforms.

Traffickers have flooded American communities with these illicit drugs, and in 2023 alone, the U.S. Drug Enforcement Administration (DEA) seized over 80 million counterfeit prescription pills

laced with fentanyl and 12,000 pounds of fentanyl powder, equating to more than 381 million lethal doses of fentanyl. Also in 2023, U.S. Customs and Border Protection (CBP) seized almost 550,000 pounds of illicit drugs, primarily at the U.S. southwest border, which included nearly 27,000 pounds of fentanyl.

U.S. Government Response

In response to this unprecedented epidemic, in 2021, President Biden declared a national emergency, deeming international drug trafficking, including the trafficking of fentanyl and other synthetic opioids, to be an unusual and extraordinary threat to U.S. national security, foreign policy, and the economy. As part of this declaration, President Biden issued Executive Order (E.O.) 14059, "Imposing Sanctions on Foreign Persons Involved in the Global Illicit Drug Trade," to modernize and expand sanctions authorities to target drug trafficking organizations, their enablers, and financial facilitators perpetrating this epidemic, and E.O. 14060, "Establishing the U.S. Council on Transnational Organized Crime," to coordinate government-wide efforts to combat TCOs.

Through E.O. 14059, Treasury's Office of Foreign Assets Control (OFAC) has sanctioned over 290 foreign nationals and entities involved in the illicit fentanyl supply chain, including: PRC-based suppliers of fentanyl precursor chemicals and manufacturing equipment; chemical brokers based in the PRC, Mexico, and other jurisdictions; Mexico-based manufacturers, smugglers, and traffickers of illicit fentanyl and other synthetic opioids; and money launderers that obfuscate the illicit proceeds sustaining the supply chain. President Biden reaffirmed his commitment to beating the opioid epidemic by making it a key priority in his Unity Agenda for the Nation, which calls for bipartisan action to stop fentanyl from flowing into our communities, to bring to justice those who put it there, and to deliver life-saving medication and care across America.

In addition to designating illicit actors involved in drug trafficking, Treasury has also led international engagements with critical stakeholders to disrupt the financing behind the illicit fentanyl supply chain, including with Mexico and Canada through the North American Drug Dialogue, and with the PRC, as part of the U.S.-PRC Counternarcotics Working Group that was the product of the November 2023 Woodside Summit between President Biden and President Xi, and the U.S.-PRC Financial Working Group. During Secretary Yellen's trip to the PRC in April 2024, the Secretary announced the Joint Treasury-People's Bank of China Cooperation and Exchange on Anti-Money Laundering to enable the PRC and United States to share best practices and information to clamp down on loopholes in our respective financial systems. Treasury has also expanded its public-private partnerships through FinCEN Exchange with U.S. financial institutions and law enforcement, including Internal Revenue Service – Criminal Investigation as part of Treasury's Counter-Fentanyl Strike Force, and through U.S.-Mexico Illicit Finance Roundtables with Mexican regulators, law enforcement, and financial institutions. These public-private partnerships promote effective suspicious activity reporting and information sharing on the synthesis and trafficking of illicit fentanyl and other synthetic opioids, as well as associated money laundering.

U.S.-PRC Counternarcotics Working Group

On November 15, 2023, President Biden and President Xi Jinping of the PRC announced the resumption of bilateral counternarcotics cooperation with a focus on reducing the flow of precursor chemicals fueling illicit fentanyl and synthetic drug trafficking. As part of this resumption of cooperation, the PRC issued a law enforcement notice to its domestic industry advising on the enforcement of laws and regulations related to trade in precursor chemicals and pill press equipment, took regulatory and law enforcement action against dozens of PRC-based synthetic drug and chemical precursor suppliers, and resumed the submission of chemical incidents to the International Narcotics Control Board's global information sharing database. The United States and the PRC also established the U.S.-PRC Counternarcotics Working Group on January 30, 2024, to coordinate on law enforcement actions; address the misuse of precursor chemicals, pill presses, and related equipment to manufacture illicit drugs; target the illicit financing of TCO networks; engage in multilateral fora; and share information to build a common understanding of the dynamic illicit threat posed by synthetic drugs. This work is ongoing.

Current Typologies Associated with the Procurement of Fentanyl Precursor Chemicals and Manufacturing Equipment

According to U.S. law enforcement, Mexico-based TCOs can purchase fentanyl precursor chemicals and manufacturing equipment either directly from PRC-based suppliers or through chemical brokers. Many of these PRC-based suppliers were previously involved in the manufacturing and distribution of fentanyl prior to the PRC placing controls on all fentanyl-related substances in May 2019. Similarly, chemical brokers often serve as middlemen for the illicit procurement of fentanyl precursor chemicals and manufacturing equipment and may represent multiple PRC-based suppliers and Mexico-based TCOs. These chemical brokers can be based in Mexico, the PRC, or other jurisdictions, and leverage their connections in mainland PRC and Mexico to connect the PRC-based suppliers and Mexico-based TCOs.

Through these connections, chemical brokers can sell and purchase fentanyl precursor chemicals and manufacturing equipment on behalf of their clients and ultimately obfuscate the illicit diversion from mainland PRC to Mexico.

Based on recent U.S. Department of Justice (DOJ) indictments and OFAC designations, PRC-based suppliers and chemical brokers may also explicitly advertise in English the sale of fentanyl precursor chemicals and manufacturing equipment on chemical and pharmaceutical company websites, e-commerce marketplaces, social media platforms, and the Darknet. Precursor chemicals are often marketed in advertisements through their associated Chemical Abstracts Service (CAS) number for ease of reference to potential illicit buyers. Advertisements may prominently feature shipping services that would be uncharacteristic of a legitimate supplier, such as explicitly offering to provide "exit and entry customs clearance," which is a euphemism for disguising and mislabeling the shipments to avoid scrutiny by law enforcement and customs officials.

These advertisements may direct Mexico-based TCOs and other illicit buyers to contact a sales representative of the supplier or their chemical broker by email, telephone, text message, or encrypted messaging applications to negotiate the sale. Payments for fentanyl precursor chemicals and manufacturing equipment may be conducted in single or multiple transactions from Mexico and the United States and may be structured through multiple senders and beneficiaries to evade BSA reporting and recordkeeping requirements. Although these payments often involve low-dollar amounts, they can result in significant amounts of potential drug trafficking proceeds

once the Mexico-based TCOs use the precursor chemicals and manufacturing equipment to synthesize and sell illicit fentanyl and other synthetic opioids. FinCEN has identified the use of shell and front companies; money transfers through banks, money services businesses (MSBs), and online payment processors; and payments in virtual currency as financial typologies associated with Mexico-based TCOs and their illicit procurement of fentanyl precursor chemicals and manufacturing equipment. These typologies and red flags in the subsequent section should not be considered an exhaustive list, and U.S. financial institutions should be vigilant of any suspicious activity indicating illicit procurement of fentanyl precursor chemicals and manufacturing equipment from any jurisdiction.

Use of Shell and Front Companies

Shell and front companies serve a critical role in enabling the supply chain and procurement of fentanyl precursor chemicals and manufacturing equipment by Mexico-based TCOs. These shell and front companies, which are used to create opaque layers of corporate ownership and obfuscate the source of activity, may appear to be legitimate Chinese exporters or Mexican importers in the chemical manufacturing and pharmaceutical industries. In some instances, these shell and front companies may also appear to be associated with entirely unrelated business sectors such as textiles, food, or the electronics industry. PRC-based suppliers generally sell fentanyl precursor chemicals and manufacturing equipment to shell and front companies under their control to create the façade of a legitimate transaction and to obfuscate the source of the illicit diversion. The shell and front companies ultimately sell the fentanyl precursor chemicals and manufacturing equipment to Mexico-based TCOs, often utilizing chemical brokers that control other shell and front companies to further obfuscate the supply chain.

Money Transfers Through Banks, MSBs, and Online Payment Processors

Money transfers through banks, MSBs, and online payment processors are a common financial typology associated with TCOs' procurement of fentanyl precursor chemicals and manufacturing equipment. These transactions may be sent from Mexico or the United States to mainland PRC (including via Hong Kong and other jurisdictions) to individuals and shell and front companies associated with either a PRC-based supplier or a chemical broker. While some money transfers are sent from TCOs in Mexico to PRC-based suppliers without crossing the U.S. financial system, many of these foreign transactions are cleared in U.S. dollars through U.S. correspondent banks, Mexico- and PRC-based agents of U.S. MSBs, and U.S. online payment processors.

Virtual Currency

Mexico-based TCOs are increasingly purchasing fentanyl precursor chemicals and manufacturing equipment from PRC-based suppliers in virtual currency, including bitcoin, ether, monero, and tether, among others. Virtual currency payments are often sent to persons affiliated with PRC-based suppliers or secondary money transmitters with hosted wallets at virtual asset service providers.

Preparing for Market Adaptation

Mexico-based TCOs and PRC-based suppliers have demonstrated an ability to adapt rapidly to changes in the regulatory or law enforcement environment in the United States, Mexico, and the PRC. In response to increased coordination and cooperation between the United States and the PRC, Mexico-based TCOs and suppliers of fentanyl precursor chemicals and manufacturing

equipment in the PRC and potentially in other jurisdictions may seek to leverage global networks to evade new restrictions and obscure transactions. This activity could lead to unanticipated shifts in the supply chain for illicit synthetic drugs. FinCEN therefore urges continued vigilance in monitoring for potentially suspicious activity related to the procurement of precursor chemicals, pill presses, die molds, and other manufacturing equipment used for the synthesis of illicit fentanyl and other synthetic opioids.

Red Flag Indicators Related to the Procurement of Fentanyl Precursor Chemicals and Manufacturing Equipment

FinCEN has identified red flags to help financial institutions detect, prevent, and report suspicious activity connected to the procurement of precursor chemicals and manufacturing equipment for the synthesis of illicit fentanyl and other synthetic opioids. These red flags are in addition to the red flags in FinCEN's 2019 Fentanyl Advisory, all of which remain relevant. As no single red flag is determinative of illicit or suspicious activity, financial institutions should consider the surrounding facts and circumstances, such as a 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 illicit procurement of fentanyl precursor chemicals and manufacturing equipment or is otherwise suspicious.

Customer and Counterparty Profile Red Flags

1. A customer or counterparty has previous drug-related convictions or open-source reporting indicates connections to clandestine lab operations.
2. A customer or counterparty is a chemical or pharmaceutical company in the PRC, Hong Kong, or another jurisdiction with a residential address or a business address shared with other similar businesses or that has no physical presence or shows other indicators of possible illicit shell company activity.
3. A counterparty, with no supposed affiliation with the PRC, uses a PRC-based phone number or Internet Protocol (IP) address that is affiliated with the website of a Chinese chemical or pharmaceutical company.
4. A customer or counterparty is a vendor on an e-commerce or Darknet marketplace that advertises the sale of precursor chemicals (using chemical names, abbreviations, or CAS numbers in the advertisement) and manufacturing equipment used for the synthesis of illicit fentanyl and other synthetic opioids.
5. A customer is a Mexican company that, according to open-source and commercially available reporting, is importing shipments of fentanyl precursor chemicals and manufacturing equipment without appropriate importing licenses and registrations in Mexico.
6. A customer is a Mexican company with little or no online presence and is involved in the import of the same precursor chemicals and manufacturing equipment used in the synthesis of fentanyl.
7. Multiple, seemingly unrelated Mexican importing companies share phone numbers, email addresses, or physical addresses and transact with the same PRC-based chemical manufacturing and pharmaceutical companies.

8. A customer is a Mexican importing company that predominantly transacts only with chemical or pharmaceutical companies in the PRC or Hong Kong for no apparent legitimate reason as compared to similar importers that transact with foreign chemical manufacturing and pharmaceutical suppliers in multiple jurisdictions.

Transactional Red Flags

9. A customer sends low-dollar or virtual currency payments for no apparent legitimate purpose to beneficiaries involved in the chemical manufacturing and pharmaceutical industries in the PRC, Hong Kong, or another jurisdiction.
10. Multiple customers send funds for no apparent legitimate purpose to the same beneficiary involved in the chemical manufacturing and pharmaceutical industries in the PRC, Hong Kong, or another jurisdiction (i.e., many-to-one).
11. A Mexico-based entity from an unrelated industry transacts with a PRC-based chemical or pharmaceutical company. Alternatively, a PRC-based entity from an unrelated industry transacts with a Mexico-based chemical or pharmaceutical company.
12. A customer engages in behavior that suggests efforts to evade the Currency Transaction Report (CTR) filing requirement (e.g., the customer alters or cancels a transaction when advised a CTR would be filed or engages in structuring with multiple cash transactions for under $10,000), as well as avoiding recordkeeping requirements.
13. A customer sends virtual currency payments to an address that is linked through blockchain analytics to beneficiaries associated with the PRC-based chemical manufacturing and pharmaceutical industries or to individuals or entities listed in DOJ indictments and OFAC designations.
14. A customer is a Mexican company that does not appear to be involved in the chemical manufacturing and pharmaceutical industries despite transactional activity indicating the procurement of fentanyl precursor chemicals and associated manufacturing equipment.

Reminder of Relevant BSA Obligations and Tools for U.S. Financial Institutions

Suspicious Activity Reporting

A financial institution is required to file a Suspicious Activity Report (SAR) if it knows, suspects, or has reason to suspect a transaction conducted or attempted by, at, or through the financial institution involves funds derived from illegal activity; is intended or conducted to disguise funds derived from illegal activity; is designed to evade regulations promulgated under the BSA; lacks a business or apparent lawful purpose; or involves the use of the financial institution to facilitate criminal activity. All statutorily defined financial institutions may voluntarily report suspicious transactions under the existing suspicious activity reporting safe harbor.

Financial institutions are required to file complete and accurate reports that incorporate all relevant information available, including cyber-related information. When filing a SAR regarding suspicious transactions that involve cyber events, financial institutions should provide all pertinent available information on the event and associated with the suspicious activity, including cyber-related information and technical indicators, in the SAR form and narrative. When filing is

not required, institutions may file a SAR voluntarily to aid law enforcement in protecting the financial sector. Valuable cyber indicators for fentanyl-related law enforcement investigations can include relevant email addresses, IP addresses with their respective timestamps, login information with location and timestamps, virtual currency addresses, mobile device information (such as device International Mobile Equipment Identity (IMEI) numbers), and descriptions and timing of suspicious electronic communications.

When a financial institution files a SAR, it is required to maintain a copy of the SAR and the original or business record equivalent of any supporting documentation for a period of five years from the date of filing the SAR. Financial institutions must provide any requested documentation supporting the filing of a SAR upon request by FinCEN or an appropriate law enforcement or supervisory agency. When requested to provide supporting documentation, financial institutions should take special care to verify that a requestor of information is, in fact, a representative of FinCEN or an appropriate law enforcement or supervisory agency.

A financial institution should incorporate procedures for such verification into its BSA compliance or AML program. These procedures may include, for example, independent employment verification with the requestor's field office or face-to-face review of the requestor's credentials.

SAR Filing Instructions

FinCEN requests that financial institutions indicate any connection between the suspicious activity being reported and the activities highlighted in this advisory by including the key term **"FENTANYL FIN-2024-A002"** in SAR field 2 ("Filing Institution Note to FinCEN"), as well as in the narrative. Financial institutions may highlight additional advisory or alert keywords in the narrative, if applicable.

Financial institutions should include all available information relating to the account(s) and location(s) 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. Financial institutions also should provide all available information regarding other domestic and foreign financial institutions involved in the activity; where appropriate, financial institutions should consider filing a SAR jointly on shared suspicious activity.

Information Sharing

Information sharing among financial institutions is critical to identifying, reporting, and preventing the illicit procurement of fentanyl precursor chemicals and manufacturing equipment or other illicit financial activity. U.S. financial institutions and associations of U.S. financial institutions sharing information under the safe harbor authorized by section 314(b) of the USA PATRIOT Act are reminded that they may share information with each other regarding individuals, entities, organizations, and countries for purposes of identifying, and, where appropriate, reporting activities that may involve possible terrorist activity or money laundering. FinCEN strongly encourages such voluntary information sharing as it relates to money laundering or possible terrorist financing in connection with drug trafficking, including the trafficking of fentanyl and other synthetic opioids, and international drug trafficking.

Given the transnational nature of illicit activity related to the illicit procurement of fentanyl precursor chemicals and manufacturing equipment, FinCEN encourages U.S. financial

institutions to continue to use, and potentially expand, their existing processes to collect and share information with foreign financial institutions in furtherance of investigations that involve cross-border activity.

Other Relevant BSA Reporting Requirements

Financial institutions and other entities or persons also may have other relevant BSA reporting obligations to provide information in connection with the subject of this advisory. These include obligations related to the CTR, Report of Cash Payments Over $10,000 Received in a Trade or Business (Form 8300), Report of Foreign Bank and Financial Accounts (FBAR), Report of International Transportation of Currency or Monetary Instruments (CMIR), Registration of Money Services Business (RMSB), and Designation of Exempt Person (DOEP). These standard reporting requirements may not have an obvious connection to illicit finance, but may ultimately prove highly useful to law enforcement.

Form 8300 Filing Instructions

When filing a Form 8300 involving a suspicious transaction relevant to this advisory, FinCEN requests that the filer select ***Box 1b*** ("suspicious transaction") and include the key term **"FENTANYL FIN-2024-A002"** in the **"Comments"** section of the report.

Due Diligence

Banks, brokers or dealers in securities, mutual funds, and futures commission merchants and introducing brokers in commodities (FCM/IBs) are required to have appropriate risk-based procedures for conducting ongoing customer due diligence that include, but are not limited to: (i) understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and (ii) conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information. Covered financial institutions are required to identify and verify the identity of beneficial owners of legal entity customers, subject to certain exclusions and exemptions. Among other things, this facilitates the identification of legal entities that may be owned or controlled by foreign politically exposed persons (PEPs).

Senior foreign political figures and due diligence obligations for private banking accounts

In addition to these due diligence obligations, under section 312 of the USA PATRIOT Act (31 U.S.C. § 5318(i)) and its implementing regulations, covered financial institutions must implement due diligence programs for private banking accounts held for non-U.S. persons that are designed to detect and report any known or suspected money laundering or suspicious activity conducted through or involving such accounts. Covered financial institutions must establish risk-based controls and procedures for ascertaining the identities of nominal and beneficial owners of such accounts and ascertaining whether any of these owners are senior foreign political figures, and for conducting enhanced scrutiny on accounts held by senior foreign political figures that is reasonably designed to detect and report transactions that may involve the proceeds of foreign corruption.

AML/CFT program and correspondent account due diligence requirements

Financial institutions are reminded of AML/CFT program requirements, and covered financial institutions are reminded of correspondent account due diligence requirements under Section 312 of the USA PATRIOT Act (31 U.S.C. § 5318(i)) and implementing regulations. As described in FinCEN Interpretive Release 2004-1, the AML/CFT program of an MSB must include risk-based policies, procedures, and controls designed to identify and minimize risks associated with foreign agents and counterparties.

For Further Information

Additional questions or comments regarding the contents of this advisory should be addressed to the FinCEN Regulatory Support Section at frc@fincen.gov.

What You Need to Do:

Informational; please share with BSA Officer and other affected team members.

FinCEN: Financial Measure Against Iraq-based Al-Huda Bank to Combat Terrorist Financing (June 26, 2024)

Link

https://www.federalregister.gov/documents/2024/07/03/2024-14415/imposition-of-special-measure-regarding-al-huda-bank-as-a-financial-institution-of-primary-money

Text

The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) issued a final rule under section 311 of the USA PATRIOT Act (section 311) that severs Al-Huda Bank from the United States financial system by prohibiting domestic financial institutions and agencies from opening or maintaining a correspondent account for or on behalf of Al-Huda Bank, an Iraqi bank that serves as a conduit for terrorist financing.

On January 31, 2024, FinCEN issued a finding and notice of proposed rulemaking (NPRM) that identified Al-Huda Bank as a foreign financial institution of primary money laundering concern. As described in the finding, Al-Huda Bank has for years exploited its access to U.S. dollars to support designated foreign terrorist organizations, including Iran's Islamic Revolutionary Guard Corps (IRGC) and IRGC-Quds Force, as well as Iran-aligned Iraqi militias Kata'ib Hizballah and Asa'ib Ahl al-Haq. Moreover, the chairman of Al-Huda Bank is complicit in Al-Huda Bank's illicit financial activities, including money laundering through front companies that conceal the true nature of and parties involved in illicit transactions, ultimately enabling the financing of terrorism.

FinCEN is taking this section 311 action to protect the United States financial system from Al-Huda Bank's illicit activity. Pursuant to this final rule, covered financial institutions are now prohibited from opening or maintaining correspondent accounts for or on behalf of Al-Huda Bank, and are required to take reasonable steps not to process transactions for the correspondent account of a foreign banking institution in the United States if such a transaction involves Al-Huda Bank, preventing indirect access by Al-Huda Bank to the United States financial system. This final rule also requires covered financial institutions to apply special due diligence to their foreign correspondent accounts that is reasonably designed to guard against their use to process transactions involving Al-Huda Bank.

What You Need to Do:

Informational; please share with BSA Officer and other affected team members.

FinCEN: Proposed Rule to Strengthen and Modernize Financial Institutions' AML/CFT Program (June 28, 2024)

Link

https://www.federalregister.gov/documents/2024/07/03/2024-14414/anti-money-laundering-and-countering-the-financing-of-terrorism-programs

Text

The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) announced a proposed rule to strengthen and modernize financial institutions' anti-money laundering and countering the financing of terrorism (AML/CFT) programs. While financial institutions have long maintained AML/CFT programs under existing regulations, this proposed rule would amend those regulations to explicitly require that such programs be effective, risk-based, and reasonably designed, enabling financial institutions to focus their resources and attention in a manner consistent with their risk profiles. Effective, risk-based, and reasonably designed AML/CFT programs are critical for protecting national security and the integrity of the U.S. financial system. The proposed amendments are based on changes to the Bank Secrecy Act (BSA) as enacted by the Anti-Money Laundering Act of 2020 (AML Act) and are a key component of Treasury's objective of building a more effective and risk-based AML/CFT regulatory and supervisory regime.

This proposed rule would:

- amend the existing program rules to explicitly require financial institutions to establish, implement, and maintain effective, risk-based, and reasonably designed AML/CFT programs with certain minimum components, including a mandatory risk assessment process;

- require financial institutions to review government-wide AML/CFT priorities and incorporate them, as appropriate, into risk-based programs, as well as provide for certain technical changes to program requirements; and
- promote clarity and consistency across FinCEN's program rules for different types of financial institutions.

The proposal also articulates certain broader considerations for an effective and risk-based AML/CFT framework as envisioned by the AML Act. For example, through its emphasis on risk-based AML/CFT programs, the proposed rule seeks to avoid one-size-fits-all approaches to customer risk that can lead to financial institutions declining to provide financial services to entire categories of customers. Today's proposal is consistent with a key recommendation in Treasury's De-risking Strategy, which recommended proposing regulations to require financial institutions to have reasonably designed and risk-based AML/CFT programs supervised on a risk basis and taking into consideration the effects of financial inclusion. Finally, the proposed rule would encourage financial institutions to modernize their AML/CFT programs where appropriate to responsibly innovate, while still managing illicit finance risks.

The proposal that FinCEN issued today was prepared in consultation with the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, and the National Credit Union Administration in order to collectively issue proposed amendments to their respective BSA compliance program rules for the institutions they supervise.

Written comments on FinCEN's proposed rule must be received on or before September 3, 2024.

Fact Sheet: Proposed Rule to Strengthen and Modernize Financial Institution AML/CFT Programs

Link

https://www.fincen.gov/sites/default/files/shared/Program-NPRM-FactSheet-508.pdf

Text

Today, the Financial Crimes Enforcement Network (FinCEN) issued a notice of proposed rulemaking (NPRM) to strengthen and modernize financial institutions' anti-money laundering and countering the financing of terrorism (AML/CFT) programs. While financial institutions have long maintained AML/CFT programs under existing regulations, this proposed rule (or "AML/CFT Program NPRM") would amend those regulations to expressly require that such programs be effective, risk-based, and reasonably designed, enabling financial institutions to focus their resources and attention in a manner consistent with their risk profiles. Effective, risk-based, and reasonably designed AML/CFT programs are critical for protecting national security and the integrity of the U.S. financial system. The proposed amendments are based on changes enacted by the Anti-Money Laundering (AML) Act of 2020 (AML Act) and are a key component of Treasury's objective of a more effective and risk-based AML/CFT regulatory and supervisory regime.

The following is a general overview of key elements of the AML/CFT Program NPRM. Please refer to the full NPRM for further details.

AML/CFT Program Requirements

The Bank Secrecy Act (BSA) requires financial institutions to establish AML/CFT programs that must include, at minimum, the following components: (1) the development of internal policies, procedures, and controls; (2) the designation of a compliance officer; (3) an ongoing employee training program; and (4) an independent audit function to test programs. The BSA and FinCEN's implementing regulations subject certain types of financial institutions to additional obligations, including provisions related to customer identification programs (CIP) and customer due diligence related to legal entity customers (CDD), among other requirements. The AML Act amended the BSA by, among other things, requiring several changes to the BSA's AML program requirements, including the insertion of "countering the financing of terrorism" (CFT) when describing AML program requirements. This proposed rule would adopt these changes.

The AML Act requires FinCEN and the appropriate Federal functional regulators to consider certain factors when prescribing minimum standards for AML/CFT programs and examining for compliance with those standards. For instance, in proposing this rule, FinCEN and Federal functional regulators must take into consideration that financial institutions are spending private compliance funds for a public and private benefit. FinCEN and Federal functional regulators must also take into consideration the AML Act's policy goal of extending financial services to the underbanked and facilitating their financial transactions while preventing criminal persons from abusing formal or informal financial services networks. Further, the BSA requires that FinCEN and Federal functional regulators consider that effective AML/CFT programs safeguard national security and generate significant public benefits, and that such programs should be reasonably designed to ensure compliance with the BSA and the regulations promulgated by FinCEN. Finally, the BSA notes that AML/CFT programs should be risk-based, including ensuring that more attention and resources of financial institutions should be directed toward higher-risk customers and activities, consistent with the risk profile of a financial institution, rather than toward lower-risk customers and activities. The proposed rule has taken these statutorily required factors into account.

AML/CFT Priorities

The AML Act provides FinCEN with an opportunity to reevaluate the existing requirements for financial institutions' AML/CFT programs as part of the Act's broader goals of strengthening and modernizing the U.S. AML/CFT regime. The AML Act comprehensively updated the BSA for the first time in decades, and it provided several changes to financial institutions' AML program requirements. Among the most prominent changes is the AML Act's mandate that FinCEN establish and make public government-wide AML/CFT Priorities, and to update them at least once every four years. The AML Act also requires FinCEN to issue regulations incorporating the AML/CFT Priorities into revised program rules. FinCEN issued the AML/CFT Priorities on June 30, 2021, and this AML/ CFT Program NPRM proposes to incorporate them into the program rules.

Effective, Risk-Based, and Reasonably Designed AML/CFT Programs

The AML Act notes that effective AML/CFT programs safeguard national security and generate significant public benefits by preventing the flow of illicit funds in the U.S. financial

system, and by assisting law enforcement and national security agencies with the identification and prosecution of persons attempting to launder money and undertake other illicit finance activity. The AML Act further provides that AML/CFT programs are to be risk-based and reasonably designed to ensure compliance with the BSA. As part of the implementation of the AML Act, FinCEN is proposing in the AML/CFT Program NPRM to amend existing program rules to explicitly require financial institutions to establish, implement, and maintain effective, risk-based, and reasonably designed AML/CFT programs. FinCEN intends for the proposed rule to enable financial institutions to use the risk assessment process to prioritize risks and focus their attention and resources in a manner consistent with the risk profile of each individual financial institution. Financial institutions would need to consider the total amount and nature of the resources available to identify, manage, and mitigate illicit finance activity risks. The importance of this consideration is reflected in the Purposes section of the AML Act and the proposed rule's focus on fostering innovation in combating financial crime.

The Risk Assessment Process

The proposed rule would require a financial institution's AML/CFT program to include a risk assessment process to better enable it to identify and understand its exposure to money laundering, terrorist financing, and other illicit finance activity risks. Under the proposed rule, financial institutions would be expected to use the results of their risk assessment process to develop risk-based internal policies, procedures, and controls in order to manage and mitigate risks, provide highly useful information to government authorities, and further the purposes of the BSA. Though many types of financial institutions currently have risk assessment processes despite the absence of a formal requirement, the proposed rule would put into regulation existing expectations and practices. Thus, the proposed rule standardizes the requirement for a risk assessment process across the different types of financial institutions subject to program rules.

Specifically, the proposed rule requires the risk assessment process to identify, evaluate, and document the financial institution's risks, including consideration of: (1) the AML/CFT Priorities, as appropriate; (2) the money laundering and terrorist financing (ML/TF) risks of the financial institution, based on a periodic evaluation of its business activities, including products, services, channels, customers, intermediaries, and geographic locations; and (3) reports filed by financial institutions pursuant to 31 CFR chapter X. The proposed rule also includes a provision that financial institutions periodically review and update their risk assessment process including, at a minimum, when there are material changes to their ML/TF risks.

Purpose Statement

The AML/CFT Program NPRM proposes to establish a new statement in FinCEN's regulations describing the purpose of the AML/CFT program requirement. This purpose statement would ensure that a financial institution implements an effective, risk-based, and reasonably designed AML/CFT program to identify, manage, and mitigate illicit finance activity risks that: complies with the BSA and the requirements and prohibitions of FinCEN's implementing regulations; focuses attention and resources in a manner consistent with the risk profile of the financial institution; may include consideration and evaluation of innovative approaches to meet its AML/CFT compliance obligations; provides highly useful reports or records to relevant government authorities; protects the financial system of the United States from criminal abuse; and safeguards the national security of the United States, including by preventing the flow of illicit funds in the financial system.

Other Changes to AML/CFT Programs

The AML/CFT Program NPRM proposes several other revisions to existing program requirements. For example, the proposed rule reflects the requirement in the BSA, as amended by the AML Act, that the duty to establish, maintain, and enforce a financial institution's AML/CFT program shall remain the responsibility of, and be performed by, persons in the United States who are accessible to, and subject to oversight and supervision by, the Secretary of the Treasury and the appropriate Federal functional regulator. Additionally, the proposed rule requires that an AML/CFT program be approved, and be subject to oversight, by a financial institution's board of directors or equivalent body. Further, the AML/CFT Program NPRM would make other revisions, mostly of a technical nature, to modernize the program rules and promote clarification and consistency.

Broader Considerations: Addressing De-risking, Encouraging Innovation, and Supporting Feedback Loops

The proposed rule also further articulates certain broader considerations for an effective and risk-based AML/CFT framework as envisioned by the AML Act. For example, as required by the BSA, FinCEN has considered the goal of extending financial services to the underbanked and facilitating financial transactions while preventing criminal persons from abusing formal or informal financial services networks. Through its emphasis on risk-based AML/CFT programs, the proposed rule seeks to avoid one-size-fits-all approaches to customer risk that can lead to financial institutions declining to provide financial services to entire categories of customers.

Additionally, one of the AML Act's purposes is to "encourage technological innovation and the adoption of new technology by financial institutions to more effectively counter money laundering and the financing of terrorism." The proposed rule would provide financial institutions with the ability to modernize their AML/CFT programs with responsible innovation while still managing illicit finance activity risks. Specifically, the NPRM includes a provision that a financial institution's internal policies, procedures, and controls may provide for its consideration, evaluation, and, as warranted by the institution's risk profile and AML/CFT program, implementation of innovative approaches to meet BSA compliance obligations.

FinCEN also intends for the proposed rule to work in concert with other sections of the AML Act, including sections 6103 (FinCEN Exchange), 6107 (Establishment of FinCEN Domestic Liaisons), and 6206 (Sharing of threat pattern and trend information). Together, the proposed rule and these sections would facilitate a focus on the AML/CFT Priorities and their incorporation into risk-based programs, which in turn would feed into critical feedback loops. Various feedback loops currently exist between the U.S. government and financial institutions, though prior to the AML Act, they have been limited in scope, frequency, and the type of feedback shared. The AML Act and the proposed rule provide a starting point for more robust feedback loops among FinCEN, law enforcement, financial regulators, and financial institutions.

The Role of the Federal Banking Agencies

The proposal that FinCEN is issuing today was prepared in consultation with the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, and the Office of the Comptroller of the Currency in order to collectively issue proposed amendments to their respective BSA compliance program rules for

the institutions they supervise.

Next Steps

The AML Act envisions significant reforms to the U.S. AML/CFT regime, and the proposed amendments in the AML/CFT Program NPRM would set a critical foundation for potential future changes in the AML/CFT framework as part of the multi-step, multi-year implementation of the AML Act. With the AML/CFT Program NPRM, FinCEN is communicating its commitment to the AML Act's purposes of modernizing the AML/CFT regime, encouraging innovation to more effectively counter ML/TF, advancing law enforcement and national security objectives, and further safeguarding the U.S. financial system from illicit activity.

For Further Information

Financial institutions should send questions or comments regarding the contents of this fact sheet to the FinCEN Regulatory Support Section at frc@fincen.gov.

What You Need to Do:

Informational; please share with BSA Officer and other affected team members.

Appraisal Bias

HUD, FHA: New Appraisal Bias Protections (May 1, 2024)

Link

Appraisal Review and Reconsideration of Value Updates (hud.gov)

Text

The **U.S. Department of Housing and Urban Development** (HUD) and the **Federal Housing Administration** (FHA) announced a new policy on May 1, 2024 that will enable mortgage borrowers to request a re-assessment of the appraised value of their property if they believe that the appraisal was inaccurate or biased.

The Reconsideration of Value (ROV) policy represents months of collaboration with the **Federal Housing Finance Agency** (FHFA) to develop an aligned approach for both FHA-insured mortgages and those purchased or guaranteed by **Fannie Mae** and **Freddie Mac**.

Applying to all FHA single-family forward and reverse mortgage programs, the new Mortgagee Letter (ML) enhances current ROV policy while adding additional clarified statements for appraisal reviews. These include improvements to the process by which borrowers may request an ROV if they identify a problem with the appraisal.

The guidance also requires lenders to include a borrower-initiated ROV process meeting certain minimum requirements, including delivery of disclosures to borrowers at loan application and upon delivery of the appraisal with instructions on how to request an ROV.

The new guidance is effective for FHA case numbers assigned on or after Sept. 2, 2024, and the policy clarifications are expected to be added to HUD's Single Family 4000.1 Handbook at a later date.

FHA's new policy requires lenders to disclose to borrowers that they may request a reconsideration of value with instructions that explain the process, including what information will be required from a borrower and the expected [ROV] processing times. These disclosures must be provided at both the time of mortgage application and at the presentation of the appraisal.

New requirements for lenders include:

- that underwriters be trained to identify and remedy appraisal deficiencies, including racial and ethnic bias;
- requirements for lenders when receiving, processing, and communicating the status of the reconsideration of value requests initiated by a borrower;
- new standards for lender quality control of appraisal reviews and reconsiderations of value; and
- new standards for appraisers to respond to requests from lenders for a [ROV] review.

What You Need to Do

Please share with affected team members. Read Mortgagee Letter (ML) 2024-07 using the Link provided above. The provisions of the ML may be implemented immediately but must be implemented for FHA case numbers assigned on or after September 2, 2024. The provisions of the ML apply to all FHA Single Family Title II forward and Home Equity Conversion Mortgage (HECM) programs.

Y&A will be sending an e-mail to CBC participants asking what they have done / will be doing about the appraisal bias rule. Y&A will sort through the responses and publish whatever information is received in the Q4 2024 Reg Update.

Young & Associates, Inc: Email Request from Bill Elliott (July 5, 2024)

Link

https://www.ffiec.gov/press/PDF/FFIEC_Statement_on_Exam_Principles_Related_to_Valuation_Bias.pdf

Text

In the most recent Regulatory Update (Q2 2024), there was a section that discussed a new requirement that banks assure that no discrimination on a prohibited basis occurs in appraisals (see Link, above). We are hearing that regulators are bringing this up in exams, even though it is just a few months old.

What You Need to Do

For this CBC (Q3 2024), we asked you to provide information regarding what decisions your bank has made on this issue, and what implementation has taken place. The responses received are below. Note that several CBC members had opinions on the subject, and that information is below. All specific identifying information has been removed. You will note that considerably less than the 307 banks in the program responded.

What Are You Doing for Appraisal Bias?

Note: The responses are in no particular order.

Response 1

We added an anti- discrimination section to our appraisal policy. We also broke out a section in policy entitled "Reconsideration of Value" to delineate a specific policy on this issue.

We also added similar anti-discrimination wording to our annual appraiser engagement letters we have appraisers on our approved list sign annually. We also added 2 appraisal discrimination questions to our appraisal review document to have our internal appraisal reviewers be looking for discrimination.

All lenders were sent this information me to assure everyone that is involved in approving a mortgage is aware

Response 2

We are currently working on policy revisions to incorporate this. We're also going to implement a new disclosure informing borrowers of the ability to request reconsideration of value. Interested to hear what others are doing!

Response 3

We added a "reconsideration of value" procedure to our Appraisal Policy and have a ECOA & UDAAP training sheet for our appraisers for vendor management in 2023. I'd like to note that in a congressional hearing on this topic in November 2023 I was watching, one of the speakers mentioned that this 1/3 of 1% of the appraisals they reviewed contained "unfavorable language". I think 1 or 2 very public cases are punishing everyone.

Response 4

We utilize a third-party AMC for that function, and we will work with them to ensure that they update their processes internally for this additional expectation. As if community bankers did not already wear enough hats, now we get to be the morality police for appraisers too. When will they let us be the morality police for the boneheads in Washington too? I'm on board for that.

Response 5

Here is what we have implemented so far:

- Created an ROV (reconsideration of value) form for our applicants to use upon request
- Added language in our Lending Policy that the ROV form exists and will be provided upon request
- Provided training to appropriate staff regarding the ROV form and how to handle appraisal complaints (same channel as complaints as described in our Compliance Policy)

Response 6

Here is the information that I have for our bank regarding discrimination/bias/ROV in residential lending:

- The Feb, 2024 statement on examination principles has not been thoroughly reviewed yet but we have implemented an ROV process/procedure.
- In June, 2023 the Board of Directors was educated on the topic of Appraisal Bias and Reconsideration of Value (ROV) via a Spotlight on Compliance document. We use a Spotlight to educate the Board on various topics throughout the year.
- Consumer Complaint Procedures - we have added appraisals/ROV to drop down list as one of the commonly cited "reasons for complaint" and are tracking appraisal issues according to our complaint procedures.
    - Consumer Complaint procedures were updated to include ROV as one of the complaint methods along with direct contact, CRA's social media, etc. and with an Addendum that details appraisal issues and steps that will be taken. We are not currently selling out loans on the secondary market so I only added a footnote regarding where to find that information.
- The 3rd party individual that reviews our appraisals has been provided with sign on information for an ABA webinar that lending management viewed in May but he has not viewed it yet.
- I've requested the appraisal discrimination/bias/ROV be included in the Appraisal policy when it is approved by the Board in September.
- We just went through and FDIC Compliance/CRA exam in April and the following were asked:
    - In the pre-exam questionnaire – under the ECOA/Fair Housing Act section – we were asked "Does the bank have a reconsideration of value process when any type of property valuation is obtained for a residential real estate transaction?"
    - In the CIDR request list they asked the following:
        - Describe the bank's compliance management system relating to appraisals or other property valuation methods, including any training, monitoring or audit processes. Provide details about what is included in such reviews, who performs the reviews, the timing and frequency of reviews, and how the reviews include fair lending considerations. To the extent applicable, this should also include any description of the bank's efforts to monitor the activities of third parties involved in the appraisal process. Note: Appraisal-related requests under this area pertain to compliance efforts under ECOA and FHA. These requests do not pertain to the following: Title XI, Part 323 of the FDIC regulations; ECOA Section 1002.14; TILA Section 1026.35(c); or TILA Section 1026.42."
        - Describe the bank's process for identifying and resolving appraisal or other property valuation-related inquiries or complaints, including the circumstances under which a reconsideration of value or second appraisal or valuation are ordered. Describe this process for both complaints received by the bank and any third-parties involved in the appraisal process.

- There were a few other appraisal related questions from the FDIC but they did not pertain to this.

Response 7

We have only begun creating procedures on reconsideration of value and will also implement a new form and mention this in our loan policy.

Response 8

My team has a meeting scheduled for July 31st to discuss what changes need to be made at our bank, so I don't have much to contribute to the discussion. However, I am curious what exams this is being brought up in? We are preparing for our next DFI Safety & Soundness exam this fall and my executives will want to know if it's likely to be brought up at that time.

Response 9

At this time we are working on the secondary market requirements for appraisals and also appraisal bias. At this time my plan is to incorporate a question into our appraisal review however I am open to other suggestions based on what others are hearing.

Response 10

Selecting and Engaging an Appraiser and Use of an Appraisal Management Company

In the *Interagency Appraisal and Evaluation Guidelines* provides for "appraiser independence" in respect to the person *ordering, performing, and reviewing* an appraisals or evaluation of collateral value. This statement applies both to residential and commercial transactions. The agencies state that a regulated financial institution should ensure that independence from the loan production and loan approval process is maintained when selecting appraisers, ordering appraisals and reviewing appraisals.

Our banks selects appraisers from the approved appraiser panels for both commercial and residential assignments based on the technical competence of the appraiser and the appraiser's knowledge of the market where the collateral is located. In all cases the selection of the appraiser will include the following:

- Appraisers will be engaged using the bank's standard Engagement Letter. The engagement letter outlines the bank's expectations. The appraisal engagement will be between Thumb Bank & Trust and the appraiser with the appraisal addressed to the ban.
- The individual selected to perform an appraisal shall not have direct or indirect interest, financial or otherwise, in the property or the transaction, as evidenced by the appraisal certification.
- An appraiser used in the preparation of an appraisal report must agree to render such reports in accordance with USPAP and the bank's policies and standards.

Acceptable Communications

Necessary communications between the appraiser and bank staff regarding the appraisal assignment will be conducted through the Appraisal Review officer or their designee so that independence is maintained. The following interaction may also be necessary from time to time:

- To consider addition information about the subject or comparable properties
- To provide additional supporting information about the basis of valuation
- To correct factual errors

Communication of predetermined, minimum, expected or qualifying estimate of value, loan amount or target loan to value is considered inappropriate.

Independence, education, expertise, experience and competency requirements

Independence- all assignment and review engagements are coordinated by the Appraisal Review Officer, a dis-interested third party. Any perceived threat to impose constraints on or influence the valuation process in general will be reported to the Chief Lending Officer.

Education, expertise, experience and competency- all review personnel and those positions involved in ordering and monitoring appraisal process are continually subjected to appraisal quality and process improvement discussion and seminars. We are is committed to continual process improvement.

Development and Monitoring of Approved Appraisers List

The Appraisal Review Officer is responsible for reviewing the qualifications of all prospective appraisers. Individual appraisers, not appraisal firms, shall be considered for placement on the bank's approved appraisal list. The bank may accept an appraisal prepared by a member of an appraisal firm not on the bank's approved appraiser list if another member of the firm who is on the list also signs and takes responsibility for the appraisal. At a minimum, the Appraisal Officer will review and approve the following before recommending the appraiser for inclusion on the bank's approved appraiser panel:

- A resume of the appraiser's educational background, professional training, experience and references;
- A resume of the appraiser's experience detailing the types of appraisals he or she has performed;
- Proof of current license or certification by the appropriate state authority and inclusion on the AQB's national appraiser registry.

Upon completing the review, the Appraisal Review Officer will maintain the list of names of qualified appraisers. The names of approved appraisers will be added to the bank's List of Approved Appraisers. The Appraisal Officer has the authority to remove appraisers from the approved list.

Response 11

In light of the increased focus on discrimination in appraisals, management is working to: enhance appraisal reviews to include looking for discriminatory/bias language, developing robust ROV procedures that take possible discrimination/bias into account, and enhancing denial file reviews and complaint data reviews for mentions of appraisals/value

Response 12

We have not implemented any new procedures at this time. Our appraisals are reviewed by a third-party auditor. We have a rotation process for selecting our appraisers and the ability to omit an appraiser from the rotation if there are concerns with their practices.

Response 13

We've shared the information with the proper department but have not made any formal changes as of yet.

Response 14

We have not made any changes to our program at this point – our OCC exam just began today so I'll let you know if they bring it up. We already have a Board-approved appraisal policy & procedures to ensure appraiser qualifications including verifying the status of their license and any disciplinary actions on record, ongoing monitoring of their continued USPAP certification, appraisal reviews are conducted which include evaluation of the reasonableness of comps used and certification of adherence to USPAP standards.