Regulatory Update

Community Bankers for Compliance

4th Quarter 2023

This publication is designed to provide information in regard to the subject matter covered.

It is provided with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional service. If legal advice or other expert assistance is required, the services of a professional competent in the area of special need should be sought.

Instructors for the CBC Program

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

Bill Elliott has over 40 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.

Sharon Bond, CRCM, Consultant, Young & Associates, Inc.

Sharon Bond is a consultant in the compliance department at Young & Associates, Inc. where she specializes in Consumer Compliance. Sharon works on a variety of compliance-related issues, including leading compliance seminars, conducting compliance reviews for all areas of compliance, conducting in-house training, and writing compliance articles and training materials. With over 30 years of industry experience, she has a strong background in mortgage lending and in federal consumer compliance laws and regulations. Sharon was an Associate National Bank Examiner with the Office of the Comptroller of the Currency (OCC) for five years. She holds the designation of Certified Regulatory Compliance Manager (CRCM) and the Six Sigma Qualtec Black Belt certifications.

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

Dale Neiss is a compliance consultant with Young & Associates, Inc. With over 30 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: Summer 2023 Supervisory Highlights (July 26, 2023)

Link

https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/cfpb_supervisory-highlights_issue-30_2023-07.pdf

Text

Since its inception, the Consumer Financial Protection Bureau's (CFPB) Supervision program has assessed supervised institutions' compliance with Federal consumer financial law and taken supervisory action against institutions that have violated it. This includes institutions engaged in unfair, deceptive, or abusive acts or practices (UDAAPs) prohibited by the Consumer Financial Protection Act of 2010 (CFPA). In April 2023, the CFPB issued a policy statement on abusive acts or practices to summarize the existing precedent, provide an analytical framework for identifying abusive conduct, and to offer some guiding principles.

This edition of Supervisory Highlights notes recent supervisory findings of abusive acts or practices supervised institutions engaged in across multiple product lines. Examiners also continue to find that supervised institutions are engaging in prohibited unfair and deceptive acts or practices. The CFPB will continue to supervise for, and enforce against, practices that may violate Federal consumer financial law, harm consumers, and impede competition.

Most supervised institutions rely on technology solutions to run their businesses and offer or provide consumer financial products or services. Supervision assesses information technology utilized by supervised entities, and information technology controls, that may impact compliance with Federal consumer financial law or risk to consumers. Examiners have identified several violations of Federal consumer financial law that were caused in whole or in part by insufficient information technology controls. This edition includes, for the first time, findings from the CFPB's Supervision information technology program.

A key aspect of the CFPB supervision program is benefitting supervised institutions by identifying compliance issues before they become significant. The supervision process is confidential in nature. This confidentiality promotes candid communication between supervised institutions and CFPB supervisory personnel concerning compliance and related matters.

The findings included in this report cover examinations in the areas of auto origination, auto servicing, consumer reporting, debt collection, deposits, fair lending, information technology, mortgage origination, mortgage servicing, payday and small dollar lending, and remittances that were completed from July 1, 2022, to March 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

Auto Origination

The CFPB assessed the auto finance origination operations of several supervised institutions for compliance with applicable Federal consumer financial laws and to assess whether institutions have engaged in UDAAPs prohibited by the CFPA.

Deceptive marketing of auto loans

Examiners found that supervised institutions engaged in the deceptive marketing of auto loans when they used advertisements that pictured cars that were significantly larger, more expensive, and newer than the advertised loan offers were good for. 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.

Examiners found that the representations made in these advertisements were likely to mislead consumers, as the "net impression" to consumers was that the advertisements applied to a subset of cars to which they did not actually apply. Examiners further concluded that it was reasonable for consumers to believe that the advertised terms applied to a class of vehicles similar to the cars pictured in the ads. These representations were material as information about the central characteristics of a product or service—such as costs, benefits, and/or restrictions on the use or availability—are presumed to be material. Here, the promotional offers advertised were significantly more restricted than a consumer may have realized. In response to these findings, the institutions have stopped using the deceptive advertisements and have enhanced monitoring of marketing materials and advertisements across all product lines.

Auto Servicing

Examiners identified three unfair or abusive acts or practices at auto servicers related to charging interest on inflated loan balances, cancelling automatic payments without sufficient notice, and collection practices after repossession.

Collecting interest on fraudulent loan charges

When supervised institutions purchase retail installment contracts from auto dealers, dealers generally provide a document listing the options included on the vehicle. Some dealers fraudulently included in the document options that are not actually present on the vehicle, for example by listing undercoating that the vehicle does not actually have. This artificially inflates the value of the collateral, which may make it easier for the dealer to find funding for the contract from indirect lenders.

Examiners found that servicers engaged in unfair and abusive acts or practices by collecting and retaining interest borrowers paid on automobile loans that included options that were not in fact included in the collateral, leading to improperly inflated loan amounts. Examiners found that after initial loan processing, servicers attempted to contact consumers to verify that options listed by the dealer are in fact on the vehicle; consumers rarely identified

discrepancies. In the event consumers identified discrepancies, servicers reduced the amounts that they paid dealers by the amount of the missing options. But servicers did not reduce the amount that consumers owed on the loan agreements and continued to charge interest tied to financing of the nonexistent options. Similarly, after repossession servicers compared the options actually present on the vehicle to the information originally provided by the dealer and, where the options were not actually included, obtained refunds from dealers that were applied to the deficiency balances. But the servicers did not refund consumers for the interest charged on the illusory options.

The CFPA defines an unfair act or practice as an act or practice that: (1) that causes or is likely to cause substantial injury to consumers; (2) which is not reasonably avoidable by consumers, and (3) is not outweighed by countervailing benefits to consumers or to competition. Examiners found that servicers engaged in unfair acts or practices when they collected interest on the nonexistent options. Examiners found that consumers suffered substantial injury when they paid excess interest resulting from improperly inflated loan amounts. Consumers could not reasonably avoid the injury because they had no reason to anticipate that dealers would fraudulently include nonexistent options and that the consumers would be charged interest based on the inflated loan amount. And even if consumers attempted to validate the options included, most consumers are not able to tell—merely by sight—the options included on a car, many of which may be hidden under the hood or otherwise not readily visible. And the injury is not outweighed by countervailing benefits to consumers or competition.

Examiners also found that the servicers engaged in abusive acts or practices. An act or practice is abusive if it: (1) materially interferes with the ability of a consumer to understand a term or condition of a consumer financial product or service; or (2) takes unreasonable advantage of: a lack of understanding on the part of the consumer of the material risks, costs, or conditions of the product or service; the inability of the consumer to protect the interest of the consumer in selecting or using a consumer financial product or service; or the reasonable reliance by the consumer on a covered person to act in the best interest of the consumer.

Here examiners concluded that the servicers' practices were abusive because they took unreasonable advantage of consumers' inability to protect their interests in the selection or use of the product by charging interest on loan balances that were improperly inflated because of the illusory options, which benefited the servicer to the detriment of consumers. Servicers were aware that some percentage of their loans had inflated balances and nevertheless collected excess interest on these amounts while seeking and obtaining refunds on the missing options. At the time of loan funding, consumers were unable to protect their own interests; it was impractical for them to challenge the practice because they did not know that certain options were missing. After repossession, servicers continued to take advantage of consumers' inability to protect their interests where they protected themselves by obtaining refunds from dealers for the value of options the collateral vehicles did not actually have but did not refund the excess interest amounts consumers had paid based on these inflated loan balances.

In response to these findings, Supervision directed the servicers to cease the practice.

Canceling automatic payments without sufficient notice

Examiners found that servicers engaged in unfair acts or practices by suspending recurring automated clearing house (ACH) payments prior to consumers' final payment without sufficiently notifying consumers that the final payment must be made manually. Consumers could enroll in automatic payments by completing a written electronic funds transfer

authorization. The authorizations contained a small print disclosure that servicers would not automatically withdraw the final payment; servicers did not provide any additional communication to consumers before the final payment was required. Many consumers enrolled in these automatic payments for a period of years and relied on the automatic payments. But servicers cancelled the final withdrawal and did not debit the final payment, resulting in missed payments and late fee assessment by servicers. Consumers suffered substantial injury when servicers failed to provide adequate notice that they would not debit the final payment, including the late fees servicers charged consumers when consumers missed these payments. Consumers could not reasonably avoid this injury because they believed their payments would be processed automatically and the only disclosure that the payment would be cancelled was written in fine print in the initial enrollment paperwork. And the injury is not outweighed by countervailing benefits to consumers or competition.

In response to these findings, servicers remediated consumers and revised their policies and procedures.

Requiring consumers to pay other debts to redeem vehicles

Some vehicle financing contracts contain clauses allowing servicers to use the vehicle to secure other unrelated unsecured debts consumers owe to the company, such as credit card debt; this is referred to as cross-collateralization. Examiners found that after servicers repossessed vehicles, they accelerated the amount due on the vehicle finance contract and also accelerated any other amounts the consumer owed to the entity. When consumers called to recover the vehicles, the servicers required consumers to pay the full amount on all accelerated debts, which included both debt for the vehicle and other debts.

Examiners found that servicers engaged in unfair and abusive acts or practices by engaging in the blanket practice of cross-collateralizing loans and requiring consumers to pay other debts to redeem their repossessed vehicles.

Accelerating and demanding repayment on other debts before returning repossessed vehicles was unfair. It caused substantial injury to consumers because consumers were required to pay accelerated and cross-collateralized amounts across multiple loans or lose their vehicles. Consumers could not reasonably avoid the harm caused by this practice. While servicers occasionally allowed consumers to pay lesser amounts, they did so only if consumers objected or argued about the debt and consumers were not meaningfully made aware that arguing about the cross-collateralization could result in a lesser payment amount. And even if the consumer objected, representatives still used the cross-collateral provisions as a coercive collection tactic. A blanket practice of cross-collateralizing and demanding repayment does not benefit consumers and the harm outweighs any countervailing benefits to consumers or competition.

This practice was abusive because it also took unreasonable advantage of a lack of understanding of consumers of the material risks, costs, or conditions of their loan agreements. When consumers sought to reinstate their loans after repossession, servicers utilized contractual remedies to accelerate all debts owed to them which resulted in a significant monetary advantage to servicers while imposing a corresponding degree of economic harm on the consumer. These practices also inflicted significant emotional and psychological distress. The advantage gained by the servicers was unreasonable in the ordinary case of vehicle repossession. And consumers lacked an understanding of the material risks, costs, or conditions of the specific contractual remedies allowing for cross-collateralization at issue in the relevant loans.

In response to these findings, servicers remediated consumers and revised policies and procedures.

Consumer Reporting

Companies that regularly assemble or evaluate information about consumers for the purpose of providing consumer reports to third parties are "consumer reporting companies" (CRCs). These companies, along with the entities—such as banks, loan servicers, and others—that furnish information to the CRCs for inclusion in consumer reports, play a vital role in the availability of credit and have a significant role to play in the fair and accurate reporting of credit information. They are subject to several requirements under the Fair Credit Reporting Act (FCRA) and its implementing regulation, Regulation V, including the requirement to reasonably investigate disputes and to furnish data subject to the relevant accuracy requirements. In recent reviews, examiners found deficiencies in CRCs' compliance with FCRA permissible purpose-related policy and procedure requirements and furnisher compliance with FCRA and Regulation V dispute investigation requirements.

CRC duty to maintain reasonable policies and procedures designed to limit furnishing consumer reports to persons with permissible purpose(s)

The FCRA requires that CRCs maintain reasonable procedures designed to limit the furnishing of consumer reports to persons with at least one of the permissible purposes enumerated under Section 604(a) of the FCRA. In recent reviews of CRCs, examiners found that CRCs' procedures relating to ensuring end users of consumer reports have a requisite permissible purpose failed to comply with this obligation because the CRCs' procedures posed an unreasonable risk of improperly disclosing consumer reports to persons without a permissible purpose. For example, examiners identified multiple deficiencies in the CRCs' procedures, such as failing to maintain an adequate process for re-assessing end users' permissible purpose(s) where indicia of improper consumer report use by an end user is present. This created heightened risk of improper consumer report disclosures. In some instances, examiners found that such deficiencies resulted in CRCs furnishing consumer reports to end users despite having reasonable grounds to believe the end users did not have a requisite permissible purpose.

In response to these findings, CRCs are revising policies and procedures for, and their oversight of, onboarding end users and periodically re-assessing end users' permissible purpose(s). CRCs also are revising processes relating to the monitoring of end users, including the identification of end users exhibiting indicia of impermissible consumer report use.

Furnisher duty to review policies and procedures and update them as necessary to ensure their continued effectiveness

Examiners found that furnishers are violating the Regulation V duty to periodically review their policies and procedures concerning the accuracy and integrity of furnished information and update them as necessary to ensure their continued effectiveness. Specifically, in recent reviews of auto furnishers, examiners found that furnishers failed to review and update policies and procedures after implementing substantial changes to their dispute handling processes. For example, furnishers changed software systems for use in the investigation of disputes but maintained policies and procedures that referenced only systems no longer in use, inhibiting the continued effectiveness of those policies and procedures. In response to these

findings, furnishers are updating their policies and procedures to reflect current systems and training staff to use them in handling disputes.

Furnisher duty to conduct reasonable investigations of direct disputes

Examiners are continuing to find that furnishers are violating the Regulation V duty to conduct a reasonable investigation of direct disputes. In recent reviews of mortgage furnishers, examiners found the furnishers failed to conduct any investigations of direct disputes that were received at an address provided by the furnishers to CRCs and set forth on consumer reports. Rather than investigate direct disputes sent to these qualifying addresses under Regulation V, the furnishers responded to the disputes by instructing the consumers to re-send their direct disputes to certain other addresses of the furnishers and only investigated the disputes to the extent the consumers re-sent them per these instructions. In response to these findings, furnishers are updating their policies and procedures to ensure that they conduct reasonable investigations of direct disputes that are sent to addresses provided by the furnishers to CRCs and set forth on consumer reports.

Furnisher duty to notify consumers that a dispute is frivolous or irrelevant

Examiners are continuing to find that furnishers are violating the Regulation V duty to provide consumers with notices regarding frivolous or irrelevant disputes. In recent reviews of third-party debt collector furnishers, examiners found that furnishers failed to send any notice to consumers whose direct disputes they determined were frivolous or irrelevant. For example, when furnishers determined that disputes sent by consumers were duplicative of prior disputes, the furnishers did not investigate the disputes nor send notices to consumers setting forth the reasons for their determination and the information the consumers needed to submit for the furnishers to investigate the disputed information. In response to these findings, furnishers are establishing policies and procedures to identify and respond to frivolous or irrelevant disputes, including sending a letter to the consumer notifying the consumer of the determination that a dispute is frivolous or irrelevant and identifying the additional information needed to investigate the consumer's dispute.

Furnisher duty to inform consumers of information needed to investigate frivolous or irrelevant disputes

Examiners are continuing to find that furnishers are violating their Regulation V duty, after making a determination that a direct dispute is frivolous or irrelevant, to include in their notices to consumers the reasons for that determination and to identify any information required to investigate the disputed information. In recent reviews of mortgage furnishers, examiners found that furnishers sent frivolous or irrelevant notices to consumers that failed to accurately convey what information the consumers needed to submit for the furnishers to investigate the disputed information. For example, furnishers sent consumers a frivolous notification stating that consumers must provide their entire unredacted credit report for the furnishers to investigate the dispute, even though an entire unredacted credit report was not required for the investigation and an excerpt of the relevant portion of the credit report would have sufficed. In response to these findings, furnishers are updating the content of their frivolous or irrelevant notices to eliminate the language requesting an entire unredacted credit report as a prerequisite for investigation.

Furnishers' failure to provide adequate address-disclosures for notices

Section 623(a)(1)(A) of the FCRA requires that a furnisher must not furnish to any CRC any information relating to a consumer if the furnisher knows or has reasonable cause to believe that the information is inaccurate. A furnisher is not subject to Section 623(a)(1)(A) if the furnisher clearly and conspicuously specifies to consumers an address at which consumers may notify the furnisher that information it furnished is inaccurate. The FCRA does not require a furnisher to specify such an address. If a furnisher clearly and conspicuously specifies such an address, it is not subject to Section 623(a)(1)(A) but must comply with Section 623(a)(1)(B) of the FCRA, which provides that a furnisher shall not furnish information relating to a consumer to a CRC if it has been notified by the consumer, at the address specified for such notices, that certain information is inaccurate and such information is, in fact, inaccurate. A furnisher that specifies an address may also be subject to Section 623(a)(2) of the FCRA if it determines that information it has furnished is not complete or accurate and fails to notify the CRC and provide corrections.

Examiners are continuing to find that furnishers are not clearly and conspicuously specifying to consumers an address for notices at which a consumer may notify the furnisher that information is inaccurate. In reviews of third-party debt collection furnishers, examiners found that the only notice or dispute address furnishers provided to consumers was an address included on debt validation notices for the purpose of disputing the validity of a debt. Examiners found that the debt validation notices did not specify to consumers an address for, or otherwise specify that the debt validity dispute address may also be used for, notices relating to inaccurately furnished consumer report information. As a result, examiners found that the furnishers have not met the requirement in Section 623(a)(1)(C) of the FCRA to not be subject to Section 623(a)(1)(A) and therefore are subject to the stricter prohibition under Section 623(a)(1)(A) of the FCRA against furnishing information the furnishers know or have reasonable cause to believe is inaccurate.

Debt Collection

The CFPB has supervisory authority to examine certain institutions that engage in consumer debt collection activities, including very large depository institutions, nonbanks that are larger participants in the consumer debt collection market, and nonbanks that are service providers to certain covered persons. Recent examinations of larger participant debt collectors identified violations of the Fair Debt Collection Practices Act (FDCPA) as well as the CFPA.

Unlawful attempts to collect medical debt

Examiners found that debt collectors continued collection attempts for work-related medical debt after receiving sufficient information to render the debt uncollectible under state worker's compensation law absent written evidence to the contrary, which the collector did not obtain from its client. The collectors made multiple calls over several years, during which they implied that the consumer owed the debt and asserted that the ambulance ride that gave rise to the debt originated from the consumer's home, despite evidence in their files that it originated from the consumer's workplace. Examiners found that, through these practices, the debt collectors violated the FDCPA by collecting an amount not permitted by law or agreement, by falsely representing the character, amount, or legal status of a debt, by engaging in conduct which had the natural consequence of harassing, oppressing, or abusing the consumer, and by using false, deceptive, or misleading representations in connection with the collection of a debt.

In response to these findings, Supervision directed the debt collectors to establish and maintain adequate collection policies, procedures, and training to include specific limitations on circumstances under which the collectors may contact consumers in connection with pending workers' compensation claims; enhancing call monitoring to include a review of accounts with a pending workers' compensation claim; and ensuring accounts are monitored for pending workers' compensation claims and collection attempts on such accounts are ceased.

Deceptive representations about interest payments

Examiners found that debt collectors advised consumers that if they paid the balance in full by a date certain, any interest assessed on the debt would be reversed. The debt collectors then failed to credit the consumers' accounts with the accrued additional interest, resulting in the consumers paying more than the agreed upon amount. Examiners found this practice to be deceptive in violation of the CFPA. In response to these findings, Supervision directed the debt collectors to remediate all consumers who had overpaid.

Deposits

The CFPB continues to examine financial institutions to assess whether they have engaged in UDAAPs prohibited by the CFPA. The CFPB also continues its examinations of supervised institutions for compliance with Regulation E, which implements the Electronic Fund Transfer Act (EFTA). The CFPB also examines for compliance with other relevant statutes and regulations, including Regulation DD, which implements the Truth in Savings Act.

Unfair line of credit usage and fees

The CFPA prohibits any "covered person" from "engaging in any unfair, deceptive, or abusive act or practice."

Examiners found unfair acts or practices due to institutions' assessment of both nonsufficient funds (NSF) and line of credit transfer fees on the same transaction. The institutions offered a line of credit program that consumers could opt-in to. If a consumer's checking account did not have sufficient funds to pay for a transaction, the institutions would transfer funds from the line of credit to cover the transaction and assess a line of credit transfer fee, as well as interest on the amount of credit extended. In some instances, the line of credit might not have sufficient funds to cover the transaction, in which case the institutions would deny the transaction and assess an NSF fee on the denied transaction. As the transaction was declined, no funds from the line of credit would be transferred to pay the transaction. But, if there were insufficient funds in the consumer's checking account to pay the NSF fee and that NSF fee overdrew the consumer's account, the institutions would automatically transfer funds from the line of credit to the consumer's checking account and assess a line of credit transfer fee.

Supervision found the institutions' practice of assessing both the NSF and the line of credit transfer fee on the same transaction is an unfair act or practice. These acts or practices caused or were likely to cause substantial injury in the form of two fees being assessed on the same denied transaction. Consumers who enrolled in the line of credit program were charged two fees instead of the single fee charged to those who were not enrolled, even though in both cases the transaction was returned unpaid. A consumer could not reasonably avoid this substantial injury as the consumer had no notice of the potential for double fees or ability to avoid the double fees in this automated process and would not reasonably expect that enrolling in a

program meant to prevent overdraft and decrease fees related to denied transactions would instead increase them. These acts or practices did not provide benefits to consumers or competition.

The supervised institutions believed they had safeguards in place to not assess NSF fees and line of credit fees on the same transaction. Specifically, they programmed their systems to not assess both of these fees on the same day. The way the institutions' systems posted NSF fees, however, meant that the NSF and line of credit fees were incurred on different days, even though they were part of the same transaction. Thus, the safeguard was inadequate. In response to these findings, the institutions committed to system changes and remediated $113,358 to 4,147 consumers. The system change implemented by the supervised institutions was to avoid the issue altogether by entirely eliminating NSF fees for unpaid transactions.

Fair Lending

The CFPB's fair lending supervision program assesses compliance with the Equal Credit Opportunity Act (ECOA) and its implementing regulation, Regulation B, as well as the Home Mortgage Disclosure Act (HMDA) and its implementing regulation, Regulation C, at institutions subject to the CFPB's supervisory authority. ECOA prohibits a creditor from discriminating against any applicant, with respect to any aspect of a credit transaction, on the basis of race, sex, color, religion, national origin, sex (including sexual orientation and gender identity), marital status, or age (provided the applicant has the capacity to contract), because all or part of the applicant's income derives from any public assistance program, or because the applicant has in good faith exercised any right under the Consumer Credit Protection Act.

During recent examinations, Examiners found lenders violated ECOA and Regulation B.

Pricing discrimination

In the Fall 2021 issue of *Supervisory Highlights*, the CFPB discussed findings that mortgage lenders violated ECOA and Regulation B by discriminating against African American and female borrowers in the granting of pricing exceptions based upon competitive offers from other institutions. Since then, Supervision conducted additional examinations assessing mortgage lenders' compliance with ECOA and Regulation B with respect to the granting of pricing exceptions based on competitive offers from other institutions. The CFPB again found that mortgage lenders violated ECOA and Regulation B by discriminating in the incidence of granting pricing exceptions across a range of ECOA-protected characteristics, including race, national origin, sex, or age.

Examiners observed that certain lenders maintained policies and procedures that permitted the granting of pricing exceptions to consumers, including pricing exceptions for competitive offers. Generally, a pricing exception is when a lender makes exceptions to its established credit standards. For example, a lender may lower a rate to match a competitor's offer and retain the consumer. Examiners identified lenders with statistically significant disparities for the incidence of pricing exceptions at differential rates on a prohibited basis compared to similarly situated borrowers. Weaknesses in the lenders' policies and procedures with respect to pricing exceptions for competitive offers, the failure of mortgage loan officers to follow those policies and procedures, the lenders' lack of oversight and control over their mortgage loan officers' discretion in connection with and use of such exceptions, or managements' failure to take appropriate corrective action risks contributed to the observed disparities in the incidence of granting pricing exceptions. Examiners did not identify evidence

of legitimate, nondiscriminatory reasons that explained the disparities observed in the statistical analysis.

In several instances, examiners identified policies and procedures that were not designed to effectively mitigate ECOA and Regulation B violations or manage associated risks of harm to consumers. Some policies permitted mortgage loan officers to request a pricing exception by submitting a request into the loan origination system without requiring that the request be substantiated by documentation. While those requests were subject to managerial review, there were no guidelines for the bases for approval or denial of the exception request or the amount of the exception. Other policies had limited documentation requirements—and sometimes no documentation requirements for pricing exceptions below a certain threshold. This meant that the lenders could not effectively monitor whether the pricing exception request was initiated by the consumer and/or supported by a competitive offer to the consumer. Other policies granted some loan officers pricing exception authority up to certain thresholds without the need for competitive offer documentation or management approval. As a result, the lenders did not flag those discretionary discounts as pricing exceptions and did not monitor them. Some policies had more robust documentation and approval requirements. But those institutions did not effectively monitor interactions between loan officers and consumers to ensure that the policies were followed and that the loan officer was not coaching certain consumers and not others regarding the competitive match process. In other instances, examiners determined that loan officers were not properly documenting the initiation source of the concession request nor were they retaining and documenting competitors' pricing information in borrowers' files as required by the lender policy.

Examiners also identified weaknesses in training programs. Some lenders did not have training that explicitly addressed fair lending risks associated with pricing exceptions, including the risks of providing different levels of assistance to customers, on prohibited bases, in connection with a customer's request for a price exception. Other training programs did not cover pricing exceptions risk for employees who have discretionary pricing authority.

Finally, examiners concluded that management and board oversight at lenders was not sufficient to identify and address risk of harm to consumers from the lender's pricing exceptions practices. Similarly, examiners observed that some lenders failed to take corrective action based on their statistical observations of disparities in pricing exceptions. Some lenders failed to document whether additional investigation into observed disparities was warranted, review the causes of such disparities, or consider actions that might reduce such disparities.

In response to these findings, the CFPB directed lenders to, among other things: enhance or implement pricing exception policies and procedures to mitigate fair lending risks, including enhancing documentation standards and requiring clear exception criteria; enhance or implement policies requiring the retention of documentation for all pricing exceptions, including document regarding whether the pricing exception request was initiated by the consumer; develop and implement a monitoring and audit program to effectively identify and mitigate potential disparities and/or fair lending risks associated with the pricing exception approval process; or to identify and remediate harmed consumers.

Discriminatory lending restrictions

The CFPB recently reviewed lending restrictions in underwriting policies and procedures at several lenders to evaluate fair lending risks and to assess compliance with ECOA and Regulation B. The reviews focused on lending restrictions relating to how those lenders handled the treatment of applicants' criminal records and whether the lenders properly

treated income derived from public assistance.

Regarding prior contact with the criminal justice system, both national data and the history of discrimination in the justice system suggest that restrictions on lending based on criminal history are, in many circumstances, likely to have a disparate impact based on race and national origin. Thus, the use of criminal history in credit decisioning may create a heightened risk of violating ECOA and Regulation B.

The CFPB's review identified risky policies and procedures at several institutions for several areas of credit, including mortgage origination, auto lending, and credit cards, but most notably within small business lending. A common thread in the CFPB review was that the discovery of criminal records prompted enhanced or second-level underwriting review. However, policies and procedures at several institutions did not provide detail regarding how that review should be conducted, creating fair lending risk around how the reviewing official exercises discretion. There were variations amongst the policies and procedures as to how the lender identified criminal records and which violations or charges triggered further review or denial. For example, some lenders generally denied credit when it identified applicants with felony convictions for financial crimes but did not deny credit for arrests or non-felony convictions. Other lenders treated criminal indictments, fraud cases, sexual offenses, and industry bans as significant risks. But without clear guidelines and well-defined standards designed to meet legitimate business needs, lenders risked violating ECOA and Regulation B by applying these underwriting restrictions in a manner that could discriminate on a prohibited basis.

With respect to the proper treatment of public assistance income in underwriting, ECOA and Regulation B prohibit discrimination against applicants, with respect to any aspect of a credit transaction, because all or part of the applicant's income derives from any public assistance program. Examiners identified lenders whose policies and procedures excluded income derived from certain public assistance programs or imposed stricter standards on income derived from public assistance programs. Lenders maintained a written policy that expressly prohibited underwriters from considering Home Assistance Payments provided by the Section 8 Housing Choice Voucher Homeownership Program. Lenders participated in mortgage lending programs that provided consumers with a benefit in the form of a mortgage credit certificate but did not treat those benefits as income under their underwriting standards. Some lenders maintained a policy with a six-year continuity-of-income requirement for applicants relying primarily on public assistance income that was stricter than the three-year requirements applicable to other applicants' income.

In response to these findings, the CFPB directed lenders to review, identify, and provide relief to any applicant negatively affected by these policies. Lenders were also directed to revise and implement policies and procedures and enhance related systems to ensure public assistance income is evaluated under standards applicable to other sources of income.

Information Technology

The CFPB's Supervision program evaluates information technology controls at supervised institutions that may impact compliance with Federal consumer financial law or implicate risk to consumers. The CFPB assesses the effectiveness of information technology controls in detecting and preventing data breaches and cyberattacks. For example, inadequate security for sensitive consumer information, weak password management controls, untimely software updates or failing to implement multi-factor authentication or a reasonable equivalent could cause or contribute to violations of law including the prohibition against engaging in UDAAPs.

Examiners found that institutions engaged in unfair acts or practices prohibited by the CFPA by failing to implement adequate information technology controls.

Failing to implement adequate information technology security controls

Examiners found that institutions engaged in unfair acts or practices by failing to implement adequate information technology security controls that could have prevented or mitigated cyberattacks. More specifically, the institutions' password management policies for certain online accounts were weak, the entities failed to establish adequate controls in connection with log-in attempts, and the same entities also did not adequately implement multi-factor authentication or a reasonable equivalent for consumer accounts.

The entities' lack of adequate information technology security controls caused substantial harm to consumers when bad actors accessed almost 8,000 consumer bank accounts and made fraudulent withdrawals in the sum of at least $800,000. Consumers were also injured because they had to devote significant time and resources to dealing with the impacts of the incident. For example, consumers had to contact the institutions to file disputes to determine why funds were missing from their accounts and then wait to be reimbursed by the institutions. Consumers may have had to spend additional time enrolling in credit monitoring services, identity theft protection services or changing their log-in credentials.

The impacted consumers could not reasonably avoid the injury caused by the institutions' inadequate information technology security controls. Consumers do not have control over certain aspects of an institutions' security features, such as how many log-in attempts an institution allows before locking an account or the number of transactions it labels suspicious, requiring additional verification. Similarly, only the institutions can implement measures to mitigate or prevent cyberattacks such as employing controls or tools to block automated malicious software (botnet) activity or ensuring sufficient authentication protocols are in place such as multi-factor authentication or an alternative of equivalent strength. Consumers do not have control over these security measures and were unable to reasonably avoid the injury caused by the cyberattacks. The injury to consumers outweighs any countervailing benefits, such as avoiding the cost of implementing information technology controls necessary to prevent these types of attacks.

In response to these findings, the institutions are implementing multi-factor authentication, or a reasonable equivalent, enhancing password management practices and implementing adequate controls for failed log-in attempts to prevent/mitigate unauthorized access to consumer accounts. Additionally, the institutions are providing remediation to impacted consumers.

Mortgage Origination

The CFPB assessed mortgage origination operations of several supervised institutions for compliance with applicable Federal consumer financial laws including Regulation Z.

Loan originator compensation: Differentiations based on product type

Regulation Z generally prohibits compensating mortgage loan originators in an amount that is based on the terms of a transaction. It defines a term of a transaction as "any right or obligation of the parties to a credit transaction." And it provides that a determination of whether compensation is "based on" a term of a transaction is made based on objective facts

and circumstances indicating that compensation would have been different if a transaction term had been different. Accordingly, in the preamble to the CFPB's 2013 Loan Originator Final Rule, the CFPB clarified that it is "not permissible to differentiate compensation based on credit product type, since products are simply a bundle of particular terms."

As part of their business model, institutions brokered-out certain mortgage products not offered in-house. For example, the institutions used outside lenders for reverse mortgage originations, but had their own in-house cash-out refinance mortgage product. Examiners determined that the institutions used a compensation plan that allowed a loan originator who originated both brokered-out and in-house loans to receive a different level of compensation for the brokered-out loans versus in-house loans. By compensating differently for loan product types that were not offered in-house, the entities violated Regulation Z by basing compensation on the terms of a transaction. In response to these findings, the entities have since revised their loan originator compensation plans to comply with Regulation Z.

Loan disclosures: Failure to reflect the terms of the legal obligation on disclosures

Regulation Z requires that disclosures "shall reflect the terms of the legal obligation between the parties." In most cases, disclosures should reflect the terms to which both the consumer and creditor are legally bound at the outset of a transaction.

Examiners found that the standard adjustable-rate promissory note used by an institution stated that the result of the margin plus the current index should be rounded up or down to the nearest one-eighth of one percentage point. However, examiners discovered that the institutions' loan origination system was not programmed to round. Thus, the fully indexed rate that the entity calculated and provided on their disclosures was calculated contrary to the promissory note for the loan. Consequently, the supervised institutions failed to reflect the terms of the legal obligation on disclosures in violation of Regulation Z. In response to these findings, the supervised institutions reconfigured their loan origination system to round according to the promissory note.

Mortgage Servicing

Examiners identified UDAAP and regulatory violations at mortgage servicers, including violations during the loss mitigation and servicing transfer processes, as well as payment posting violations.

Loss mitigation timing violations

If a servicer receives a complete application more than 37 days before a scheduled foreclosure sale, then Regulation X requires servicers to evaluate the complete loss mitigation applications within 30 days of receipt and provide written notices to borrowers stating which loss mitigation options, if any, are available. Examiners found that some servicers violated Regulation X when they failed to evaluate complete applications within 30 days of receipt. Relatedly, some servicers evaluated the application within 30 days but failed to provide the required notice to borrowers within 30 days as required. In response to these findings, servicers improved policies and implemented additional training.

Additionally, examiners found that servicers engaged in an unfair act or practice when they delayed processing borrower requests to enroll in loss mitigation options, including COVID-19 pandemic-related forbearance extensions, based on incomplete applications. These

delays varied in length, including delays up to six months. Borrowers were substantially injured because they suffered one or more of the following harms: prolonged delinquency, late fees, default notices, and lost time and resources addressing servicer delays. Borrowers also experienced negative credit reporting because of the servicers' delays, resulting in a risk of damage to their credit that may have materialized into financial injury. Borrowers could not reasonably avoid injury because servicers controlled the processing of applications, and borrowers reasonably expected servicers to enroll them in the options they applied for. And the injury to consumers was not outweighed by benefits to consumers or competition.

In response to these findings, servicers ceased the practice and developed improved policies and procedures.

Misrepresenting loss mitigation application response times

Examiners found that servicers engaged in deceptive acts or practices when they informed consumers, orally and in written notices, that they would evaluate their complete loss mitigation applications within 30 days, but then moved toward foreclosure without completing the evaluations. Because the servicers received the complete loss mitigation applications 37 days or less before foreclosure, Regulation X did not require the servicers to evaluate the application within 30 days. But the servicers informed consumers in written and oral communications that they would evaluate borrowers' complete loss mitigation applications within 30 days, and these representations created the overall net impression that foreclosure would not occur until the servicers rendered decisions on the applications. The borrowers reasonably interpreted these representations to mean that they would receive decisions on the applications, and potentially a period of time to take other actions if the applications were denied, prior to foreclosure. Finally, the servicers' representations were material, as they prompted the borrowers to wait for notification concerning a possible loan modification and discouraged the borrowers from taking additional steps to prepare for foreclosure.

In response to these findings, servicers ceased the practice and developed improved policies and procedures.

Assigning continuity of contact personnel

Under Regulation X, servicers are required to establish continuity of contact with delinquent consumers by maintaining policies and procedures to assign personnel to delinquent borrowers by, at the latest, the 45th day of delinquency. These personnel should be made available to answer delinquent borrowers' questions via telephone, and the servicer shall maintain policies and procedures that are reasonably designed to ensure these personnel can perform certain functions. These include providing accurate information about loss mitigation and timely retrieving written information provided by the borrower to the servicer in connection with a loss mitigation application.

Examiners found that servicers violated Regulation X by failing to maintain adequate continuity of contact procedures. Servicers did not maintain policies and procedures that were reasonably designed to ensure that personnel were made available to borrowers via telephone and provided timely live responses if borrowers were unable to reach continuity of contact personnel; the servicers routinely failed to return phone calls from borrowers. And when consumers did speak with personnel, the personnel failed to provide accurate information about loss mitigation options that were available. Additionally, servicers' systems did not allow the assigned personnel to retrieve, in a timely manner, written information that the consumer

had already provided in connection with their loss mitigation applications, causing assigned personnel to ask for information already in the servicers' possession.

In response to these findings, servicers updated their servicing platforms, developed new monitoring reports, implemented additional trainings, and revised policies and procedures.

Spanish language acknowledgement notices missing information

Regulation X requires servicers, in most circumstances, to provide borrowers with a written acknowledgment notice within 5 days of receipt of a loss mitigation application. This notice must contain a statement that the borrower should consider contacting servicers of any other mortgage secured by the same property to discuss loss mitigation options. Examiners found that servicers violated Regulation X by failing to include this required language on Spanish language application acknowledgment notices. In contrast, servicers included this language on English language acknowledgment notices sent to English speaking consumers. In response to these findings, servicers updated their letter templates.

Failure to provide critical loss mitigation information

Examiners found that servicers violated Regulation X and Regulation Z by failing to provide specific required information in several circumstances:

- Specific reasons for denial when they sent notices that included vague denial reasons, such as informing consumers that they did not meet the eligibility requirements for the program;
- Correct payment and duration information for forbearance; and
- Information in periodic statements about loss mitigation programs, such as forbearance, to which consumers had agreed.

In response to these findings, servicers updated their letter templates and enhanced monitoring.

Failure to credit payment sent to prior servicer after transfer

After a transfer of servicing, Regulation X requires that, during the 60-day period beginning on the effective date of transfer, servicers not treat payments sent to the transferor servicer as late if the transferor servicer receives them on or before the due date. Examiners found that servicers treated payments received by the transferor servicer during the 60-day period, but not transmitted by the transferor to the transferee until after the 60-day period, as late. This violated Regulation X because the transferor had received the payment within the 60-day period beginning on the effective date of the transfer. In response to these findings servicers remediated consumers and updated policies, procedures, training, and internal controls.

Failure to maintain policies and procedures reasonably designed to identify missing information after a transfer

Regulation X requires servicers to maintain policies and procedures that are reasonably designed to achieve the objectives in 12 CFR 1024.38(b). Commentary to Regulation X clarifies that "procedures" refers to the actual practices followed by the servicer. Under Regulation X,

transferee servicers are required to maintain policies and procedures to identify necessary documents and information that may not have been included in a servicing transfer and obtain such information from the transferor servicer.

Examiners found that some servicers violated Regulation X when they failed to maintain policies and procedures reasonably designed to achieve the objective of facilitating transfer of information during servicing transfers. For example, servicers' policies and procedures were not reasonably designed because they failed to obtain copies of the security instruments, or any documents reestablishing the security instrument, to establish the lien securing the mortgage loans after servicing transfers. In response to these findings, servicers updated their policies and procedures and implemented new training.

Payday and Small-Dollar Lending

During examinations of payday and small-dollar lenders, Supervision identified unfair, deceptive, and abusive acts or practices and violations of Regulation Z. Supervision also identified risks associated with the Military Lending Act.

Unreasonable limitations on collection communications

Examiners found that lenders engaged in abusive and deceptive acts or practices in connection with short-term, small-dollar loans, by including language in loan agreements purporting to prohibit consumers from revoking their consent for the lender to call, text, or e-mail the consumers. The agreements stated, for example, that consumers, "cannot revoke this consent to call, text, or email about your existing loan" and that "[n]one of our employees are authorized to receive a verbal revocation of this authorization." Lenders that engage in unreasonable collections communications may violate the CFPA's prohibition against UDAAP. By implying that consumers could not take action to limit unreasonable collections communications, this practice was abusive because it took unreasonable advantage of the consumers' inabilities to protect their interests in selecting or using a consumer financial product or service by limiting such collections communications. The practice was also deceptive because it misled or was likely to mislead consumers acting reasonably as to a material fact, i.e., whether or not they could protect themselves by limiting unreasonable communications by phone, text, or email, and whether the lenders had an obligation to honor such requests. The practice was further abusive and deceptive under the above analyses because, contrary to the language of the loan agreements, the lenders' procedures did in fact require the lenders' representatives to allow consumers to revoke consent to communications.

In response to these findings, Supervision directed the lenders to revise the contract language to cease misleading consumers about their ability to limit collections calls, texts, and emails to reasonable channels, locations, and times, and to cease taking unreasonable advantage of consumers' inabilities to protect themselves against unreasonable or unlawful collection communications.

False collection threats

Examiners found that supervised institutions made false collection threats related to litigation, garnishment, and late fees, each of which constituted deceptive acts or practices in violation of the CFPA. The lenders sent letters to delinquent payday loan borrowers in certain states, stating that the supervised institutions "may pursue any legal remedies available to us" unless the consumer contacted the institution to discuss the delinquency. The

representations misled or were likely to mislead borrowers into reasonably believing that the supervised institutions might take legal action against the consumer to collect the debt if the consumer did not make timely payment. It would be reasonable for consumers to interpret a threat to pursue "any legal remedies available to us" to include the legal remedy of a lawsuit or other similar civil action. The supervised institutions, however, never pursued such legal action to collect on payday loans in these states. The representations were material because threats of possible legal action could have an impact on a consumer's decision regarding whether and when to make payment. In response to these findings, Supervision directed the institutions to stop engaging in the deceptive conduct.

Examiners also found that lenders engaged in deceptive acts or practice by making false threats related to garnishment in collections communications. Lenders used the term "garnishment" in communications with consumers when referring to voluntary wage deduction process. These representations misled or were likely to mislead reasonable consumers by giving the false impression they would be subject to an involuntary legal garnishment process if they did not make payment. In fact, consumers could revoke voluntary wage deduction consent at will under the terms of the loan agreement and prevent deductions from occurring. Consumers acting reasonably would believe that the lenders express references to the possibility of garnishment accurately reflected what might happen absent the consumers making payment. The representations were material because they may have affected a consumer's decision regarding whether and when to make payment and whether to revoke their consent to the voluntary wage deduction process. In response to these findings, the entities were required to stop engaging in the deceptive conduct.

In addition, examiners found that periodic statements provided to borrowers falsely stated, "if we do not receive your minimum payment by the date listed above, you may have to pay a $25 late fee." Such representations misled or were likely to mislead borrowers into reasonably believing that they could be charged late fees, when in fact lenders did not assess late fees in connection with the product. The representations were material because they were likely to affect consumers' decisions about whether and when to make payments. In response to these findings, Supervision directed the lenders to stop engaging in the deceptive conduct.

Unauthorized wage deductions

Examiners found that lenders engaged in unfair acts or practices with respect to consumers who signed voluntary wage deduction agreements by sending demand notices to consumers' employers that incorrectly conveyed that the employer was required to remit to the lenders from the consumer's wages the full amount of the consumer's loan balance. In fact, the consumer had agreed to permit the lenders only to seek a wage deduction in the amount of the individual scheduled payment due. The lenders then collected wages from the consumers' employers in amounts exceeding the single payment authorized by the consumer. This wage collection practice caused substantial injury to consumers who incurred monetary injury by having amounts deducted from their wages in excess of what they had authorized. The consumers could not have reasonably avoided the injury, which was caused by the lenders seeking and obtaining wage deductions in excess of those authorized by the consumers. The benefits to the lenders of collecting unauthorized amounts do not outweigh the injuries to the consumers in the form of lost wages. In response to these findings, Supervision directed lenders to stop engaging in the practice and provide remediation to impacted borrowers.

Misrepresentations regarding the impact of payment of debt in collections

Examiners found that lenders engaged in deceptive acts or practices when they misrepresented to borrowers the impact that payment or nonpayment of debts in collection may have on the sale of the debt to a debt buyer and the subsequent impact on the borrower's credit reports. The lenders made representations about debt sale, credit reporting practices, and corresponding effects on consumer creditworthiness that misled or were likely to mislead the consumer. Their agents asserted or implied that making a payment would prevent referral to a third-party debt buyer and a negative credit impact. However, these agents had no basis to predict the consumer's credit situation or a potential debt buyer's furnishing practices, the lender's contracts with debt buyer prohibited furnishing to a CRC, and the debt was not in fact sold. It was reasonable for a consumer experiencing repayment difficulty to interpret the representations to mean that not making a payment would cause a third party to subsequently report adverse credit information and worsen their creditworthiness. The representations were material because they were likely to affect the consumer's choices or conduct regarding the loan. In response to these findings, Supervision directed the entities to stop engaging in the deceptive conduct.

Risk of harm to consumers protected by the Military Lending Act

Examiners found that installment lenders created a risk of harm to borrowers protected by the Military Lending Act by, before engaging in loan transactions, and contrary to their policies, failing to confirm that several thousand borrowers were not covered borrowers under the Military Lending Act as implemented by Department of Defense regulations. These risks included potentially, originating loans to covered borrowers at rates and terms impermissible under the Military Lending Act; not providing covered borrowers with required disclosures; including in loan agreements prohibited mandatory arbitration clauses; and failing to limit certain types of repeat or extended borrowing. In response to these findings, Supervision directed lenders to change their practices to prevent these risks.

Failure to retain evidence of compliance with disclosure requirements under Regulation Z

Examiners found that lenders failed to retain for two years evidence that they delivered clear and conspicuous closed-end loan disclosures in writing before consummation of the transaction, in a form that consumers may keep, in violation of the record-retention provision of Regulation Z, and creating a risk of a violation of the general disclosure requirements of Regulation Z. Copies of disclosures in loan files did not include evidence of when or how lenders delivered disclosures to borrowers. And lenders were unable to produce evidence that, for electronically signed contracts, disclosures were delivered to consumers in a form they may keep before loan consummation. Lenders' compliance procedures did not require delivery of loan disclosures to consumers in a form they may keep before consummation. In response to these findings, Supervision directed lenders to update compliance management systems to ensure clear and conspicuous disclosures are provided in writing in a form the consumer may keep before consummation and evidence of compliance is retained, consistent with Regulation Z, for all disclosure channels, including electronic or keypad.

Remittances

The CFPB evaluated both depository and non-depository institutions for compliance with the Electronic Funds Transfer Act (EFTA) and its implementing Regulation E, including Subpart B (Remittance Rule).

Failure to develop policies and procedures to ensure compliance with the Remittance Rule's error resolution requirements

The Remittance Rule states that a remittance transfer provider shall develop and maintain written policies and procedures that are designed to ensure compliance with the error resolution requirements applicable to remittance transfers. Some institutions did not develop written policies and procedures designed to ensure compliance. This issue was noted in prior editions of *Supervisory Highlights* and continues to be an issue with institutions.

For example, some institutions used their anti-money laundering compliance policy in lieu of a specific policy tailored to the Remittance Rule requirements. The anti-money laundering policy and procedure included some basics, like identifying some covered Remittance Rule errors and the basic timeframes remittance providers had to investigate and resolve error notices. But they were not substitutes for Remittance Rule policies. They did not provide detailed guidance to employees on how to distinguish notices of error, the handling of which are subject to specific Remittance Rule requirements, from other complaints. They did not make clear employees should provide notifications that are required by the Remittance Rule to consumers when the institutions determined an error, no error, or a different error occurred. The policies also did not alert employees as to the remedies available to consumers under the Remittance Rule and articulated remedies different than those required by the Remittance Rule.

Other institutions provided policies that indicated the institutions knew of the Remittance Rule and its requirements, and had manuals to cover Remittance Rule compliance. However, these institutions did not develop procedures that would put these policies into effect. Specifically, the manuals did not provide adequate guidance to employees to resolve error notices in a consistent and compliant manner. Recitation of Remittance Rule requirements without greater detail on how to effectuate compliance does not ensure compliance as the Remittance Rule requires.

In response to these findings, institutions updated their policies and procedures during or after the conclusion of the examinations.

Supervisory Program Developments

Omitted.

Remedial Actions

Omitted

What You Need to Do

There are quite a few topics covered in this issue of Supervisory Highlights; please review and share with team members as deemed appropriate.

FDIC: 2023 Risk Review (August 14, 2023)

Link

https://www.fdic.gov/analysis/risk-review/2023-risk-review.html

Text

The Federal Deposit Insurance Corporation (FDIC) published its *2023 Risk Review*. The report summarizes conditions in the U.S. economy, financial markets, and banking industry.

The 2023 Risk Review provides a comprehensive summary of key developments and risks in the U.S. banking system, as in prior reports, and includes a new section focused on crypto-asset risk. The report focuses on the effects of key risks on community banks in particular, as the FDIC is the primary federal regulator for the majority of community banks in the U.S. banking system.

The FDIC's Risk Review is an annual publication and based on year-end banking data from the prior year. This year's expanded report incorporates data and insights related to the recent stress to the banking sector through first quarter 2023. FDIC intends to publish its next Risk Review in the spring of 2024.

Section 1 is an executive summary.

Omitted.

Section 2 is an overview of economic, financial market, and banking industry conditions.

Omitted.

Sections 3 through 7 include analysis of the key credit, market, operational, crypto-asset, and climate-related financial risks facing banks.

Selected sections are below

Section 5 – Operational Risk

If a bank does not know the customer with whom a bank is conducting business, the U.S. financial system is more susceptible to money laundering, terrorist financing, and other illicit financial activity risks.

Banks implement CDD policies, procedures, and processes to assess and mitigate risks associated with customers and the products and services offered by the bank. Still, the inability to know the beneficial owner of accounts maintained at U.S. financial institutions

presents risk to the U.S. financial system. In 2016, the United States implemented the beneficial ownership rule requiring financial institutions to identify and verify beneficial owners of legal entity customers when a new account is opened. This approach will change once the Corporate Transparency Act (CTA) is fully implemented. The CTA will require certain companies to disclose to FinCEN their beneficial ownership information when they are formed (or for non-U.S. companies, when they register with a state to do business in the United States); they will also be required to report changes in beneficial owners. Beneficial ownership information helps address the risk within the United States, whereby criminals have historically been able to take advantage of the lack of uniform laws and regulations pertaining to the disclosure of an entity's beneficial owners. These revisions are expected to help facilitate law enforcement investigations and make it more difficult for illicit actors to hide behind corporate entities registered in the United States or foreign entities registered to do business in the United States.

Bank reliance on third parties to perform AML/ CFT compliance services or act as an intermediary between the bank and its customers may be a source of risk.

Third parties used by a bank may not be subject to AML/CFT laws and regulations. Excessive use of third-party relationships can limit bank staff's knowledge of customer account activity and impede the ability to verify the identity of a customer or beneficial owner of a legal entity customer, perform CDD procedures, or identify the beneficiary or recipient of a financial transaction, product, or service

The dynamic nature of sanctions regulations increases the risk that banks process transactions for a sanctioned party.

Financial authorities and governments use economic and trade sanctions based on foreign policy and national security goals against targeted individuals and entities such as foreign countries, regimes, terrorists, international narcotics traffickers, and those engaged in certain activities such as the proliferation of weapons of mass destruction or transnational organized crime. Since Russia's invasion of Ukraine, the Office of Foreign Assets Control (OFAC) and the Department of State issued approximately 1,500 new and 750 amended sanctions (i.e., changes to sanctions programs). Inadequate interdiction software implementation, ineffective supplemental processes (manual or automated), unknown gaps in sanctions screening systems, and untimely updates to a bank's interdiction software increase the risk of processing transactions for a sanctioned party. The FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security (BIS) issued joint alerts urging banks to be vigilant against efforts by individuals or entities to evade BIS export controls implemented in connection with the Russian Federation's invasion of Ukraine.

Section 6 – Crypto-Asset Risk

The crypto-asset sector experienced significant market volatility in 2022, exposing several vulnerabilities.

In 2022, growth in the crypto-asset industry corresponded with an increasing interest by some banks to engage in crypto-asset activities.

Crypto-assets present novel and complex risks that are difficult to fully assess.

Part of the difficulty in assessing these risks arises from the dynamic nature of crypto-assets, the crypto marketplace, and the rapid pace of innovation. Some of the key risks associated with crypto-assets and crypto-asset sector participants include those related to fraud, legal uncertainties, misleading or inaccurate representations and disclosures, risk management practices exhibiting a lack of maturity and robustness, and platform and other operational vulnerabilities. Possible contagion risk within the crypto-asset sector resulting from interconnections among certain crypto-asset participants may present concentration risks for banks with exposure to the crypto-asset sector. Susceptibility of stablecoins to run risk can create the potential for deposit outflows for banks that hold stablecoin reserves.

The FDIC and other banking regulators have taken several steps in light of these emerging risks.

The FDIC has generally been aware of some banks' interest in crypto-asset-related activities through its normal supervision process. However, as this interest has accelerated, the FDIC determined that more information was needed to better understand the risks associated with these activities. Hence in April 2022, the FDIC issued Financial Institution Letter (FIL) 016-2022, which asks FDIC-supervised institutions to notify the FDIC of the crypto-related activities in which they are engaged in or intend to engage in. This FIL notes various crypto-related activities, including acting as crypto-asset custodians; maintaining stablecoin reserves; issuing crypto and other digital assets; acting as market makers or exchange or redemption agents; participating in blockchain and distributed ledger-based settlement or payment systems, including performing node functions; and related activities such as finder activities and lending. This list is not all inclusive and does not mean that the activity is permissible for FDIC-supervised institutions. These institutions were asked to provide necessary information that would allow the FDIC to assess the safety and soundness, consumer protection, and financial stability implications of such activities.

While not specific to crypto-assets, the FDIC finalized a rule on May 17, 2022, to help address instances in which firms misrepresent the availability of deposit insurance in violation of the law. On July 29, 2022, the FDIC issued a fact sheet to the public on FDIC deposit insurance and crypto companies and an advisory to FDIC-insured institutions on deposit insurance and dealings with crypto companies. Both documents address risks, concerns, and risk management and governance considerations related to misrepresentations and misconceptions about deposit insurance coverage in the context of crypto-assets. Since 2022, the FDIC has taken action against more than 85 entities that were misrepresenting the nature, extent, or availability of deposit insurance. In some instances, these firms had made misleading claims in connection with crypto-assets. For example, on August 19, 2022, the FDIC issued letters to five companies that had made false representations stating or implying that crypto-assets were eligible for FDIC insurance, demanding that they and their officers, directors, and employees cease and desist from making false and misleading statements about FDIC deposit insurance. Also, on December 13, 2022, the FDIC Board of Directors issued for public comment a proposed rule to amend its regulations on use of the official FDIC sign and to clarify the FDIC regulation regarding misrepresentations of deposit insurance.

More recently in January 2023, the FDIC, the Federal Reserve, and the Office of the Comptroller of the Currency (OCC) released a joint statement on crypto-asset risks to banking organizations. The statement reminds banking organizations that they should ensure that crypto-asset-related activities can be performed in a safe and sound manner, are legally permissible, and comply with applicable laws and regulations, including those designed to protect consumers (such as fair lending laws and prohibitions against unfair, deceptive, or

abusive acts or practices). Also, in February 2023, the FDIC, Federal Reserve, and OCC issued a Joint Statement on Liquidity Risks to Banking Organizations Resulting from Crypto-Asset Market Vulnerabilities on the liquidity risks to banking organizations presented by certain sources of funding from crypto-asset-related entities. This statement highlights key liquidity risks associated with crypto-assets and crypto-asset sector participants that banking organizations should be aware of. In particular, certain sources of funding from crypto-asset-related entities may pose heightened liquidity risks to banking organizations due to the unpredictability of the scale and timing of deposit inflows and outflows. The statement reminds banking organizations to apply existing risk management principles and provides examples of practices that could be effective. The agencies also continue to emphasize that banking organizations are neither prohibited nor discouraged from providing banking services to customers of any specific class or type, as permitted by law or regulation.

The FDIC, in coordination with the other federal banking agencies, continues to closely monitor crypto-asset-related exposures of banking organizations. As warranted, the FDIC will issue additional statements related to engagement by banking organizations in crypto-asset-related activities. The FDIC also has developed processes to engage in robust supervisory discussions with banking organizations regarding proposed and existing crypto-asset-related activities.

Section 7 – Climate-Related Financial Risk

The FDIC is in the early stages of understanding and addressing financial risks posed by climate change and intends to expand efforts in a thoughtful and measured approach that emphasizes collaboration with other supervisors and industry.

The FDIC is working with domestic and international financial regulatory counterparts to better understand and address climate-related financial risks. The FDIC is also working with banking industry stakeholders to maintain a meaningful dialogue on climate-related risks and to support institutions as they develop plans to identify, monitor, and manage these risks.

To enhance the understanding of climate-related financial risks, the FDIC in 2022 established an internal cross-disciplinary working group to assess the safety and soundness and financial stability considerations associated with climate-related financial risks and to develop broad understanding of climate-related financial risk in all of its forms. The FDIC is also coordinating with interagency peers and is participating on the Financial Stability Oversight Council's Climate-Related Financial Risk Committee. Further, as climate change is a global issue, the FDIC joined the Network of Central Banks and Supervisors for Greening the Financial System to foster collaboration and share best practices for addressing climate-related financial risk globally.

The FDIC recognizes that risk management practices in this area are evolving and will continue to encourage banks to consider climate-related financial risk in a manner that allows them to prudently meet the financial services needs of their communities.

As an initial step to promote a consistent understanding of effective management of this emerging risk, in March 2022 the FDIC issued a proposed Statement of Principles for Climate-Related Financial Risk Management for Large Financial Institutions. The principles provide

a high-level framework for the safe and sound management of exposures to climate-related financial risk and are intended to support efforts by large financial institutions to focus on key aspects of climate-related financial risk management. The draft principles are substantially similar to the principles issued by the Office of the Comptroller of the Currency (OCC) in December 2021 and the Federal Reserve Board in December 2022. After reviewing comments received on the proposed principles, the FDIC intends to coordinate with the OCC and Federal Reserve in issuing any final guidance.

What You Need to Do

The primary areas of focus in this publication are: operational risk, crypto-asset risk, and climate-related financial risk. Please review and share with team members as deemed appropriate.

FDIC: Banker Engagement Site (BES) for Consumer Compliance and CRA Examination Activities (September 5, 2023)

Link

https://www.fdic.gov/news/financial-institution-letters/2023/fil23049.html

Text

In September 2023, the Federal Deposit Insurance Corporation (FDIC) is launching a new Banker Engagement Site (BES) through FDIC*connect*. BES provides a secure and efficient portal to exchange documents, information, and communications for consumer compliance and Community Reinvestment Act (CRA) examinations. Specifically, BES provides a financial institution's authorized staff the ability to communicate with FDIC examination staff and to respond to the information and document requests made throughout the supervisory process.

Highlights:

The FDIC is introducing BES as the primary tool for exchanging examination planning and other information for Division of Depositor and Consumer Protection (DCP) consumer compliance and CRA activities.

BES offers new functionality to improve the banker experience in pre-examination process and improves efficiencies through the following features:

- The ability for bank users to collaborate with the FDIC's examination team when responding to information and document requests;
- The capability to submit questions and comments to the examination team;
- The ability to view submitted responses and documents;
- The capability to associate responses with specific requests;

- The ability to manage the bank's user roles and permissions;
- The availability of informative user guides and training resources;
- Contact information for the examination team;
- Access to the pre-examination planning response provided for the previous examination; and
- An ability to opt-out of using BES (institutions will be provided an alternative method to respond to pre-examination planning requests and to exchange information).

The FDIC's existing tool to exchange examination information, the Enterprise File Exchange (EFX), will continue to be used when the pre-planning for consumer compliance and CRA activity initiated prior to the availability of BES and also may be utilized in some additional circumstances. The FDIC's examination management will inform financial institutions, during their initial pre-examination contact, of the application that will be used for their examination during the transition to BES. BES is designed to support the consumer compliance examination process and is not planned for the use in other FDIC examinations, such as safety and soundness examinations. For such activities where BES is not used, institutions should continue to use EFX and reference FIL-63-2019.

BES is integrated with the FDIC's identity access system via FDIC*connect* for user authentication. External users must be registered with FDIC*connect* to benefit from the enhanced capability provided by BES. External users will continue to be authenticated using a secure two-factor authentication process.

What You Need to Do

For information only – FDIC-supervised Fis.

FRB: Compliance Spotlight – Supervisory Observations on Representment Fees (September 22, 2023)

Link

file:///C:/Users/dneiss/Downloads/CCOI22023-compliance-spotlight-representment-fees%20(1).pdf

Text

Background and Observations

Through supervisory examinations, the Federal Reserve recently analyzed the practice of imposing fees on represented transactions at several supervised institutions for compliance with applicable federal consumer financial laws.

As background, a representment occurs when, after a bank declines to pay a debit transaction from a consumer's checking account because of insufficient funds, the merchant presents that same transaction again to the bank for payment. Examiners identified more than one institution that charged a nonsufficient funds (NSF) fee when a transaction was first presented and declined and also charged additional NSF fees each time the same transaction was represented and declined.

At more than one supervised institution, examiners cited the assessment of NSF fees on represented transactions as an unfair practice in violation of Section 5 of the Federal Trade Commission (FTC) Act, which prohibits unfair or deceptive acts or practices (UDAP), based on the following findings:

- The assessment of NSF fees on represented transactions resulted in a substantial injury in the form of monetary harm that affected a large number of consumers.
- Consumers were not in a position to reasonably avoid this harm because:
    - once the bank had declined to pay a transaction because of insufficient funds, the merchant controlled the number and timing of representment; and
    - the bank determined whether it paid or declined the represented transaction, and whether it assessed an NSF fee on the represented transaction.
- NSF fees on represented transactions were retained by the bank and did not provide benefits to consumers or competition that outweighed the consumer harm.

Managing Risks

Examiners identified the following methods that institutions had effectively used to mitigate UDAP risk related to the assessment of fees on represented transactions:

- Institutions refrained from assessing an NSF fee on a represented transaction after the bank assessed an NSF fee on the transaction when it was initially presented for payment.
- Institutions that relied on a third party for their systems monitored the third party's system settings for compliance with applicable laws and regulations, including the prohibition on UDAPs. Examiners also found it helpful when institutions informed their Federal Reserve contact if a third party was unable to comply with their directions relating to representments.
- Institutions took steps to ensure that the information provided to consumers about represented transactions was accurate and consistent with the bank's policy and any systems limitations.

This list is based on supervisory observations to date and does not impose any legal obligations on banks. Other methods may also assist banks in managing their UDAP risks.

What You Need to Do

FRB perspective on representment fees; review the "managing risks" and incorporate into policy and procedures if applicable and relevant.

FDIC: Public Campaign to Raise Awareness About Deposit Insurance (October 11, 2023)

Link

https://www.fdic.gov/news/press-releases/2023/pr23083.html

Text

To increase the public's awareness of deposit insurance and how it can protect people's money in the event of a bank's failure, the Federal Deposit Insurance Corporation (FDIC) launched a national campaign, "Know Your Risk. Protect Your Money." The consumer-focused campaign aims to reach those who may have lower confidence in the U.S. banking system or who are unbanked, as well as those who use mobile payment systems, alternative banking services and financial products that may appear to be FDIC-insured but are not.

Following three regional bank failures earlier this year, a Gallup poll found nearly half of Americans surveyed are worried about the safety of their money deposited into banks and other financial institutions. This uncertainty also suggests a significant percentage of those surveyed are unaware money deposited into an FDIC-insured bank is protected up to at least $250,000. More than 99 percent of deposit accounts in the U.S. today are under this deposit insurance coverage limit and are fully protected by the FDIC. Since the FDIC's creation 90 years ago, no depositor has lost a penny of their insured deposits.

The FDIC has also observed an increasing number of instances online where firms or individuals have misused the FDIC's name or logo, or have made false or misleading representations about deposit insurance, raising confusion among consumers about the insurability of nonbanks and crypto-assets. To determine if an institution is FDIC-insured, you can ask a representative of the institution, look for the FDIC sign at the institution, or use the FDIC's BankFind tool. Learn more about FDIC deposit insurance and which financial products are covered.

The FDIC's public awareness campaign features a piggy bank, which is commonly associated with money and personal savings, placed in potentially risky situations. Recognizing that many Americans may be putting their money at risk, the advertisements emphasize, "Know Your Risk. Protect Your Money." The campaign consists of digital display ads, including web banners, as well as search engine marketing and sponsored social media that connect consumers to deposit insurance information and resources on the FDIC's website in English and Spanish. The digital campaign will run through November and will resume in January 2024 with the start of traditional tax filing season and when many consumers receive refund payments.

For more information or to access campaign resources and toolkits, please visit FDIC.gov/news/campaigns/know-your-risk and follow on social media at #IsYourMoneyInsured.

What You Need to Do

All FDIC-insured FIs should consider participating in this campaign.

CFPB: Advisory Opinion – Consumer Financial Protection Act (October 11, 2023)

Link

https://files.consumerfinance.gov/f/documents/cfpb-1034c-advisory-opinion-2023_10.pdf

Text

The Consumer Financial Protection Bureau (CFPB) issued an advisory opinion regarding a provision enacted by Congress which generally prohibits large banks and credit unions from imposing unreasonable obstacles on customers, such as charging excessive fees, for basic information about their own accounts. Under a 2010 federal law, large banks and credit unions must provide complete and accurate account information when requested by accountholders. As many large banks shift away from a relationship banking model that prioritizes high levels of customer service, today's advisory opinion clarifies that people are entitled to get the basic information they need without having to pay junk fees.

In the run up to the 2008 financial crisis, large banks, along with other financial institutions, failed to ensure consumers had access to full details about their accounts. As millions of homeowners struggled to pay their mortgages, many were unable to even determine which companies held their loans. When Congress instituted financial reforms in the Consumer Financial Protection Act, it included a provision in Section 1034(c) requiring large banks and credit unions – those with more than $10 billion in assets – to provide account information that is in their control or possession, when it is requested by customers.

When large financial institutions charge fees to respond to those requests, they impede customers from obtaining the essential information they are entitled to under federal law. From its market monitoring and the public's comments about large banks' customer service, the CFPB is aware that some large banks charge customers for basic information that is critical to fix problems with their bank account or to manage their finances.

Banks give many different names to these fees. Today's guidance explains how the CFPB will administer the legal requirement for large banks when it comes to customer service, including how the CFPB will evaluate fees imposed on customers for making reasonable requests, such as seeking original account agreements or information about recurring withdrawals from an account.

The CFPB does not intend to seek monetary relief for potential violations of Section 1034(c) that occur prior to February 1, 2024.

The CFPB has been pursuing a number of initiatives to preserve relationship banking in the United States and to ensure that consumers can obtain adequate customer service. Earlier this year, the CFPB published an analysis on financial institution use of customer service chatbots powered by artificial intelligence.

Consumers can submit complaints about junk fees and about financial products and services by visiting the CFPB's website or by calling (855) 411-CFPB (2372).

Employees who believe their companies have violated federal consumer financial protection laws, including by charging consumers unlawful fees, are encouraged to send information about

what they know to whistleblower@cfpb.gov. To learn more about reporting potential industry misconduct, visit the CFPB's website.

What You Need to Do

This AO pertains to large banks and credit unions – those with more than $10 billion in assets – requiring them to provide account information that is in their control or possession, when it is requested by customers. Regardless of your assets size, please review the information and share with appropriate team members. Note also the following: employees who believe their companies have violated federal consumer financial protection laws, including by charging consumers unlawful fees, are encouraged to send information about what they know to whistleblower@cfpb.gov.

CFPB: Supervisory Highlights – Junk Fees Update (October 11, 2023)

Link

https://files.consumerfinance.gov/f/documents/cfpb_supervisory_highlights_junk_fees-update-special-ed_2023-09.pdf

Text

Supervisory Observations

Deposits

In recent examinations of depository institutions and service providers, Supervision has reviewed certain fees related to deposit accounts to assess whether supervised entities have engaged in any unfair, deceptive, or abusive acts or practices (UDAAPs) prohibited by the Consumer Financial Protection Act of 2010 (CFPA). Examiners have focused on NSF and overdraft fees in particular and have reviewed statement fees and surprise depositor fees as well. Examiners also have engaged in follow-up work regarding pandemic relief benefits.

Assessing multiple NSF fees for the same transaction

Supervision continued examinations of institutions to review for UDAAPs in connection with charging consumers NSF fees, especially with respect to "re-presentments." A re-presentment occurs when, after declining a transaction because of insufficient funds and assessing an NSF fee for the transaction, the consumer's account-holding institution returns the transaction to the merchant's depository institution, and the merchant presents the same transaction to the consumer's account-holding institution for payment again. In some instances, when the consumer's account remains insufficient to pay for the transaction upon re-presentment, the consumer's account-holding institution again returns the transaction to the merchant and

assesses another NSF fee for the transaction, without providing consumers a reasonable opportunity to prevent another fee after the first failed presentment attempt. Absent restrictions on the assessment of NSF fees by the consumer's account-holding institution, this cycle can occur multiple times, and consumers may be charged multiple fees for a single transaction.

Core processor practices

Core processors provide critical deposit, payment, and data processing services to many supervised institutions, and the system functionality that these entities develop drives many fee practices, including NSF fee practices. Supervision has examined core processors in their capacity as service providers to covered persons providing deposit services.

Examiners concluded that, in the offering and providing of core service platforms, core processors engaged in an unfair act or practice by contributing to the assessment of unfair NSF fees on re-presented items. An act or practice is unfair when: (1) it causes or is likely to cause substantial injury to consumers; (2) the injury is not reasonably avoidable by consumers; and (3) the injury is not outweighed by countervailing benefits to consumers or to competition. Consumers incurred substantial injury in the form of the relevant re-presentment NSF fees. Consumers were also at increased risk of incurring additional fees on subsequent transactions caused by the re-presentment NSF fees, which lowered consumers' account balances. Injurious fees were foreseeable in light of the system limitations, as the core processor platforms did not allow financial institutions to refrain from charging more than one NSF fee per item without discontinuing NSF fees altogether or manually waiving individual fees. These fees were not reasonably avoidable by consumers, where consumers did not have a meaningful opportunity to prevent another fee after the first failed representment attempt. The consumer injury at issue was not outweighed by countervailing benefits to consumers or competition.

To address these findings, the core processors enhanced the systems they provide to financial institutions to facilitate their implementation of policies to eliminate NSF re-presentment fees. Additionally, Supervision intends to review the practices of financial institutions seeking payment from the consumer's financial institution, often called Originating Depository Financial Institutions, to ensure that represented transactions are coded properly to enable systems to identify the relevant transactions efficiently as well as refrain from charging NSF fees on those transactions.

Supervised institutions' practices

In other examinations, Supervision found that financial institutions engaged in unfair acts or practices by charging consumers re-presentment NSF fees without affording the consumer a meaningful opportunity to prevent another fee after the first failed representment attempt. The assessment of re-presentment NSF fees caused substantial monetary injury to consumers, totaling tens of millions of dollars that will be refunded to consumers because of examinations during this time period. These injuries were not reasonably avoidable by consumers, regardless of disclosures in account-opening documents, because consumers did not have a reasonable opportunity to prevent another fee after the first failed presentment attempt. And the injuries were not outweighed by countervailing benefits to consumers or competition.

Consistent with the CFPB's longtime position regarding responsible business conduct, institutions proactively developed plans to remediate consumers for assessed re-presentment NSF fees. However, some financial institutions used incomplete reports that only captured certain re-presentment NSF fees charged to consumers. Examiners found that these reports captured

consumer accounts that were charged NSF fees on checks only, or on both checks and ACH transactions. Yet they omitted consumer accounts that were assessed NSF fees solely on ACH transactions. After examiners identified this issue, institutions reviewed their remediation methodologies to ensure coverage of both ACH and check re-presentments.

In total, institutions are refunding over $22 million to consumers in response to Supervision directives since CFPB initiated this set of work in 2022. Additionally, the vast majority of institutions reported plans to stop charging NSF fees altogether.

Unfair unanticipated overdraft fees

Supervision continued to cite unfair acts or practices at institutions that charged consumers for unfair unanticipated overdraft fees, such as Authorize-Positive Settle-Negative (APSN) overdraft fees, during this time period. APSN overdraft fees occur when financial institutions assess overdraft fees for debit card or ATM transactions where the consumer had a sufficient available balance at the time the consumer authorized the transaction, but given the delay between authorization and settlement the consumer's account balance is insufficient at the time of settlement. This change in balance can occur for many reasons, such as intervening authorizations resulting in holds, settlement of other transactions, timing of presentment of the transaction for settlement, and other complex practices relating to transaction processing order. Supervision's recent matters have built on work described in Winter 2023 Supervisory Highlights, and the CFPB previously discussed this practice in Consumer Financial Protection Circular 2022-06, Unanticipated Overdraft Fee Assessment Practices.

Across its examinations, Supervision has identified tens of millions of dollars in injury to thousands of consumers that occurred whether supervised institutions used the consumer's available or ledger balance for fee decisioning. Consumers could not reasonably avoid the substantial injury, irrespective of account opening disclosures. The consumer injury was not outweighed by countervailing benefits to consumers or competition. To remedy the violation, these institutions ceased charging APSN overdraft fees, and will conduct a lookback and issue remediation to injured consumers.

In total, financial institutions are refunding over $98 million to consumers since this work began in 2022. In recent examinations, and consistent with Supervision's earlier work, supervised institutions that had reported to examiners that they engaged in APSN overdraft fee practices now report that they will stop doing so.

Supervisory data requests on overdraft, NSF and other overdraft-related fees

As part of the CFPB's ongoing supervisory monitoring related to overdraft practices, Supervision obtained data from several institutions related to fees assessed over the course of 2022, including per item overdraft and NSF fees, sustained overdraft fees, and transfer fees (collectively, "overdraft-related fees"). Supervision also obtained account-level and transaction-level data from several institutions regarding overdraft fees assessed over a one-month period on non-recurring debit card and ATM transactions. Some of the key observations gleaned from the data are discussed below. Please note that the discussion below does not present all of the CFPB's observations or data obtained and that the CFPB's analysis of data provided by institutions is ongoing.

Overdraft coverage and fee amounts per overdraft transaction

During the time periods reviewed, the relevant institutions charged per-item overdraft fees that ranged from $15 per item to $36 per item. The amount of overdraft coverage provided for consumer transactions on which these fees were charged often was disproportionately small. For example, in these data sets, the median amount of overdraft coverage extended on one-time debit card and ATM transactions ranged from $14 to $30. In fact, the percentage of transactions for which the amount of overdraft coverage provided was less than the relevant per-item overdraft fee ranged from 32% to 74% across institutions.

Incident and distribution of overdraft, NSF and other overdraft-related fees

Supervision obtained institution-level data segmented by certain account characteristics, including: opt-in status, i.e. accounts opted-in to overdraft services for one-time debit card and ATM transactions ("opted-in accounts") versus accounts not opted-in to such overdraft services ("not opted-in accounts"), and average account balance, i.e. accounts with an average balance at or less than $500 ("lower balance accounts") versus accounts with an average balance greater than $500 ("higher balance accounts"). Across all institutions monitored, most accountholders do not incur overdraft-related fees. This data set also showed that overdraft-related fees constituted the majority of the total deposit account fees that consumers incurred and an even greater proportion of the total fees assessed to lower balance accounts and opted-in accounts.

In 2022, in this data set, overdraft and NSF fees comprised 53% of all fees that the institutions charged to consumer checking accounts and nearly three-quarters of all fees charged to lower balance accounts and opted-in accounts. Not surprisingly then, while accountholders overall each paid approximately $65 per year in overdraft and NSF fees on average, opted-in accounts and lower balance accountholders paid over $165 and $220 in overdraft and NSF fees on average per year, respectively. A relatively small fraction of bank customers had a lower average balance but paid the majority of overdraft and NSF fees which is consistent with findings in prior research conducted by the CFPB. Indeed, across all institutions in aggregate, one-fifth of accounts were lower-balance accounts, but these accounts paid 68% of per-item overdraft fees assessed and 77% of the per-item NSF fees assessed. In fact, for at least one institution, over half of per-item overdraft fees assessed and over one-third of per-item NSF fees assessed were charged to lower balance, opted-in accounts even though only five percent of the institution's accounts fell into this category.

Data on the frequency of overdraft transactions and fees showed that the number of overdraft transactions and fees varies substantially with opt-in status. Accounts that overdraft most frequently (12 or more overdraft fees per year) were nearly five times as prevalent among opted-in accounts compared to not opted-in accounts.

Account closure and charge-offs attributable to overdraft transactions and overdraft-related fees

Supervision also obtained data on account closure attributable to unpaid negative balances and overdraft transactions and the amount of charged-off negative balances attributable to overdraft transactions (excluding fees). With respect to account closure, Supervision found that, across all institutions, most accounts were closed involuntarily and half of such accounts were closed due to an unpaid negative balance attributable to overdraft transactions and overdraft-related fees.

In aggregate, losses to institutions in the form of charge-offs were evenly split between opted in accounts and not opted in accounts. Although overdraft transactions initiated by lower balance accounts were more likely to be charged-off, the average amount charged-off per lower balance account was roughly equal to the amount charged-off per higher balance account and was actually lower at some institutions. Notably, overdraft-related fees themselves generally constituted one-third of the total amount of negative balances charged-off. In fact, overdraft-related fees constituted as much as two-thirds of the total amount of all overdraft charge-offs by at least one institution.

Unfair statement fees

When supervised institutions send account statements to customers that provide information about their deposit accounts during the month, they generally deliver these statements to consumers in paper form, through the U.S. mail, unless consumers elect to receive the statements in verified and secure electronic form, whether by email or through the institution's website or its mobile application.

In recent examinations, Supervision observed that institutions charged fees for the printing and delivery of paper statements, including additional fees when they mailed a statement that was returned undelivered. Supervision found that, in certain instances, institutions did not print or attempt to deliver paper statements but continued to assess paper statement fees and returned mail fees each month.

Supervision found that institutions engaged in an unfair act or practice by assessing paper statement fees and returned mail fees for paper statements they did not attempt to print and deliver. Assessing such delivery-related statement fees for undelivered statements caused substantial injury to consumers. Indeed, in one instance, a senior citizen discovered that her account was almost entirely depleted because an account statement had been returned undelivered five years prior and the institution had been assessing statement fees each month since. Consumers could not reasonably avoid this injury because they had no reason to anticipate that such fees would be assessed. The injury was also not outweighed by countervailing benefits to consumers or competition because assessing delivery-related fees for undelivered statements provides no benefit to consumers and does not actually compensate institutions for any costs incurred.

In response to these findings, the institutions stopped assessing paper statements and returned mail fees for paper statements they did not attempt to deliver and will refund the millions of dollars in such fees that were charged to hundreds of thousands of consumers.

Surprise depositor fees

Surprise depositor fees, also known as returned deposit item fees, are fees assessed to consumers when an institution returns as unprocessed a check that the consumer attempted to deposit into his or her checking account. An institution might return a check for several reasons, including insufficient funds in the originator's account, a stop payment order, or problems with the information on the check.

In October 2022, the CFPB issued a compliance bulletin stating that it is likely an unfair act or practice for an institution to have a blanket policy of charging return deposit item fees anytime that a check is returned unpaid, irrespective of the circumstances or patterns of behavior on the account. The CFPB stated that these fees cause substantial monetary injury for each returned

item, which consumers likely cannot reasonably avoid because they lack information about and control over whether a check will clear. And it may be difficult to show that this injury from blanket return deposit item policies is outweighed by countervailing benefits to consumers or to competition.

In recent examinations, Supervision has evaluated the returned deposit item fee practices at a number of institutions. Most of the examined institutions have advised the CFPB that they have eliminated returned deposit item fees entirely. Others have stated that they are in the process of doing so. As previewed in the October 2022 bulletin, Supervision has not sought to obtain monetary relief for return deposit item fees assessed prior to November 1, 2023. But Supervision will continue to monitor the relevant practices for compliance with the law and may direct remediation from institutions that continue charging unfair returned deposit item fees.

Treatment of pandemic relief benefits

As described in past editions of Supervisory Highlights, Supervision conducted examination work to evaluate how financial institutions handled pandemic relief benefits deposited into consumer accounts. Specifically, the CFPB performed a broad assessment centered on whether consumers may have lost access to pandemic relief benefits, namely Economic Impact Payments and unemployment insurance benefits, as a result of financial institutions' garnishment or setoff practices. Further follow-up reviews identified many supervised institutions that risked committing an unfair act or practice in violation of the CFPA in connection with their treatment of pandemic relief benefits which resulted in consumers being charged improper fees.

In response to these findings, the institutions (1) refunded protected Economic Impact Payments improperly taken from consumers to set off fees or amounts owed to the institution; (2) refunded garnishment-related fees assessed to consumers for improper garnishment of Economic Impact Payments; and (3) reviewed, updated, and implemented policies and procedures to ensure the institution complies with applicable state and territorial protections regarding its setoff and garnishment practices.

To date, Supervision has identified over $1 million in consumer injury in response to these examination findings, with institutions providing redress to over 6,000 consumers. Thus far, supervised institutions have provided redress of approximately $685,000 to consumers for improper setoff of Economic Impact Payments and approximately $315,000 for improper garnishment-related fees. Most supervised institutions have reported making substantial changes to their policies and procedures to prevent this type of consumer injury in the future.

Auto Servicing

Examiners also reviewed fee practices in connection with auto loans. Through this work, Supervision continues to identify unfair acts or practices related to auto servicers' handling of refunds of add-on products after loans terminate early. Specifically, some servicers failed to ensure consumers received refunds, while others did so but miscalculated the refund amounts.

When consumers purchase an automobile, auto dealers and finance companies offer optional, add-on products that consumers can purchase. Auto dealers and finance companies often charge consumers for the entire cost of any add-on products at origination, adding the cost of the add-on product as a lump sum to the total amount financed. As a result, consumers typically make payments on these products throughout the loan term, even if the product expires earlier.

Overcharging for add-on products after early loan termination

Examiners have continued to review servicer practices related to add-on product charges where loans terminated early through payoff or repossession. When loans terminate early, certain products no longer offer any possible benefit to consumers; whether a product offers a benefit depends on the type of product and reason for early termination. For example, many vehicle service contracts continue to provide possible benefits to consumers after early payoff but not after repossession, while a credit product (such as Guaranteed Asset Protection (GAP) or credit-life insurance) will not offer any possible benefits after either early payoff or repossession.

Examiners found auto servicers engaged in unfair acts or practices because consumers suffered substantial injury when servicers failed to ensure they received refunds for add-on products following early loan termination; consumers were essentially required to pay for services they could no longer use, as the relevant products (including vehicle service contracts, GAP, or credit-life insurance) terminated either when the loan contract was terminated or provided no possible benefits after the consumer lost use of the vehicle. Consumers could not reasonably avoid the injury because they had no control over the servicers' refund processing actions. When servicers present consumers with payoff amounts, deficiency balances, or refunds, consumers may have no reason to know that the amounts include unearned add-on product costs. And reasonable consumers might not apply for refunds themselves because they may be unaware that the contract provided that they could do so. Examiners concluded that the injury was not outweighed by any countervailing benefits to consumers or competition.

In response to these findings, servicers are remediating impacted consumers more than $20 million and implementing processes to ensure consumers receive refunds for add-on products that no longer offer any possible benefit to consumers.

Miscalculating refunds for add-on products after early loan termination

Examiners also have continued to identify problems with the calculation of unearned fee amounts after loan termination. Examiners found that servicers engaged in unfair acts or practices when they used miscalculated add-on product refund amounts after loans terminated early. These servicers had a policy to obtain add-on product refunds and relied on service providers to calculate the refund amounts. The service providers miscalculated the refunds due, either because they used the wrong amount for the price of the add-on product or because they deducted fees (such as cancellation fees) that were not authorized under the add-on product contract; the servicers then used these miscalculated refund amounts.

Examiners found that servicers engaged in an unfair act or practice when they used miscalculated add-on product refund amounts after loans terminated early. Using miscalculated refund amounts caused, or was likely to cause, substantial injury because servicers either communicated inaccurately higher deficiency balances or provided smaller refunds than warranted after early loan termination. Consumers could not reasonably avoid the injury because they were not involved in the servicers' calculation process, and it is reasonable for consumers to assume that the calculations are accurate. And the injury was not outweighed by countervailing benefits to consumers or competition.

In response to these findings, servicers are remediating impacted consumers and improving monitoring of service providers.

Remittances

Examiners also review activities of remittance transfer providers to ensure that fees are disclosed and charged consistent with Subpart B of Regulation E (the Remittance Rule). These examinations found that certain providers have violated regulations by failing to appropriately disclose fees or failing to refund fees, in certain circumstances, because of an error.

The Remittance Rule requires that remittance transfer providers disclose any transfer fees imposed by the provider. Recent examinations have found that remittance providers have failed to disclose fees imposed by their agents at the time of the transfer, in violation of 12 CFR 1005.31(b)(1)(ii). This reduced the total wire amount the recipients received as compared to the amount that had been disclosed. Additionally, in the case of an error for failure to make funds available to a designated recipient by the date of availability, the Remittance Rule states that if a remittance transfer provider determines an error occurred, the provider shall refund to the sender any fees imposed, and to the extent not prohibited by law, taxes collected on the remittance transfer. Examiners found that certain providers failed to correct errors by refunding to the sender fees imposed on the remittance transfer, within the specified time frame, where the recipients did not receive the transfers by the promised date, in violation of 12 CFR 1005.33(c)(2)(ii)(B). In response to these findings, supervised institutions implemented corrective action to prevent future violations and provided remediation to consumers charged fees in violation of regulatory requirements.

*****

What You Need to Do

More about "junk fees" and other UDAP issues. Please review and share with appropriate team members.

Lending Issues

FFIEC: 2023 Census Flat File and 2023 Median Family Income Report (August 10, 2023)

Link

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

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

Text

FFIEC Census Flat Files

The FFIEC Census flat files are a convenient method of accessing and analyzing the FFIEC census data that are used to create the HMDA and CRA Aggregate and Disclosure Reports. They contain over 1,000 fields of census data and are updated annually to reflect changes to MSA/MD boundaries announced by the Office of Management and Budget (OMB) and CRA Distressed/ Underserved Census Tracts as announced by the Federal banking regulatory agencies.

For years prior to 2019, these files are also included as part of a Windows application. The Windows application allows users to generate reports that can be exported in Excel, PDF, and text formats. From 2019 on, the user must download the flat files to generate their own reports.

For 2022, the FFIEC plans to release the various FFIEC Census products in three parts as the data become available. The first release was March 30, 2022; a second release in August updated the flat file with ACS fields; and a final release is expected in 2023 after the Demographic and Housing Characteristics (DHC) files are released by Census.

For 2023, the initial flat file release in August does not include demographic data for the four island areas. This data will be included in a second flat file release coming later in 2023.

FFIEC Median Family Income Report

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 for HMDA reporters.

CFPB: 2024 Filing Instruction Guide (FIG) and Supplemental Guide for Quarterly Filers (September 7, 2023)

Link

FIG:

https://s3.amazonaws.com/cfpb-hmda-public/prod/help/2024-hmda-fig.pdf

Supplemental Guide for Quarterly Filers:

https://s3.amazonaws.com/cfpb-hmda-public/prod/help/supplemental-guide-for-quarterly-filers-for-2024.pdf

Text

2024 Filing Instruction Guide (FIG)

The 2024 Filing Instructions Guide (FIG) is a compendium of resources to help you file annual HMDA data collected in 2024 with the Consumer Financial Protection Bureau (Bureau). These resources are further detailed throughout the document in individual sections.

NOTE: There are no significant changes to the submission process for data collected in 2024 and reported in 2025.

Supplemental Guide for Quarterly Filers

Omitted.

What You Need to Do:

Informational for HMDA reporters.

CFPB: 2022 Mortgage Market Activity and Trends (September 27, 2023)

Link

https://files.consumerfinance.gov/f/documents/cfpb_data-point-mortgage-market-activity-trends_report_2023-09.pdf

Text

The Consumer Financial Protection Bureau (CFPB) released its annual report on residential mortgage lending activity and trends. In 2022, mortgage applications and originations declined markedly from the prior year, while rates, fees, discount points, and other costs increased. Overall affordability declined significantly, with borrowers spending more of their income on mortgage payments and lenders more often denying applications for insufficient income. Most refinances during the reported period were cash-out refinances, and, in a reversal of recent trends, the median credit score of refinance borrowers declined below the median credit score of purchase borrowers. As in years past, independent lenders continued to dominate home mortgage lending, with the exception of home equity lines of credit.

Key findings from this year's analysis include:

- **Borrowers paid much more in costs and fees:** When taking out a mortgage, borrowers often pay certain costs and fees. These costs rose 22% from 2021 to $5,954. A higher percentage of borrowers (50.2%) paid discount points in 2022 than in any other year since data collection in this area began, including than in 2021 (32.1%). The median borrower paid $2,370 for discount points in 2022.

- **Cash-out refinances comprised majority of refinance originations:** In 2021, the number of refinances was 8.3 million. Today's report shows that number dropped to 2.2 million in 2022, a 73.2% reduction. Most of the refinances were cash-out refinance loans originated by independent lenders. Cash-out refinances can increase the risk of foreclosure as they typically have higher interest rates, higher monthly payments, and higher balances than other refinances, and can result in unsecured debt, such as credit card debt, becoming secured by the home.

- **Home-equity lines of credit rose:** Though they did not comprise the majority of refinances, home-equity lines of credit were the only form of refinancing to see a rise from 2021. While independent lenders dominate the cash-out refinancing market, depository institutions offered the majority of the 1.27 million home-equity lines of credit in 2022. Home-equity lines of credit tend to have lower interest rates, monthly payments, and foreclosure risks than cash-out refinances.

- **Average monthly mortgage payments increased more than 46%:** Driven by the rise in mortgage interest rates, the average monthly payment for borrowers taking out a conventional conforming 30-year fixed-rate mortgage (excluding taxes and insurance) rose from $1,400 in December 2021 to $2,045 in December 2022 – a 46.1% increase. The median interest rate for a 30-year fixed-rate mortgage at the end of 2022 was 6.5%.

- **Overall, Hispanic and Black borrowers experienced worse outcomes:** Black and Hispanic borrowers were denied loans at higher rates, received smaller loans, were charged higher interest rates, and paid more in upfront fees than white and Asian borrowers. For example, in 2022, the median interest rate for Black and Hispanic borrowers was above 5%, while the median rate was below 5% for white and Asian borrowers.

- **Lenders increasingly denied applicants for insufficient income:** Lenders denied loan applications due to insufficient income at higher rates than at any point since that data was first collected and reported in 2018. More than 50% of mortgage denials for Asian applicants were due to insufficient income. The same was true for around 45% of denials for Black and Hispanic applicants, and around 40% of denials for white applicants. Denials due to insufficient income were below 40% for all four groups in 2018.

Since 1975, the Home Mortgage Disclosure Act has required financial institutions to collect and make public certain loan-level information on mortgage applications and originations. In 2011, Congress transferred responsibilities for implementing the Act from the Federal Reserve Board of Governors to the CFPB. Since then, the CFPB has worked to improve public access to the data, including through an annual report analyzing the information received.

This is the fifth year that the data reflect changes implemented by the 2015 HMDA rule, which implemented statutory changes in the Consumer Financial Protection Act and provided greater information to the public about home mortgage lending.

What You Need to Do:

Informational for mortgage lenders and/or HMDA reporters.

CFPB: Small Business Lending Rule (July 31, 2023)

Link

https://files.consumerfinance.gov/f/documents/cfpb_pi_order_texas_bankers.pdf

Text

On July 31, 2023, the U.S. District Court for the Southern District of Texas ordered the CFPB not to implement or enforce the small business lending rule against plaintiffs in *Texas Bankers Ass'n, et al. v. CFPB*, *et al.*, No. 7:23-cv-00144, and their members. That order, a copy of which is available using the link above, stays all deadlines for compliance with the small business lending rule for plaintiffs in that case and their members.

What You Need to Do:

The existing deadlines for compliance (Oct 1, 2024, April 1, 2025, Jan 1, 2026) will be delayed. More information to come.

CFPB: Filing Instructions Guide for Small Business Lending Data (August 17, 2023)

Link

https://www.consumerfinance.gov/data-research/small-business-lending/filing-instructions-guide/

Text

The CFPB released an update to the Filing Instructions Guide for Small Business Lending Data.

The updates include:

- Reordering certain demographic information codes to better correlate with Home Mortgage Disclosure Act data, per request from industry,

- Minor wording clarifications to the pricing information data point, and
- Minor administrative updates to the validation IDs.

The changes were also incorporated into the Small Business Lending Rule Data Points Chart.

Details about these changes to the Filing Instructions Guide can be found in the Small Business Lending Data Updates page, available at:

www.consumerfinance.gov/data-research/small-business-lending/small-business-lending-data-updates/

You can access the updated Small Business Lending Rule Data Points Chart here:

www.consumerfinance.gov/compliance/compliance-resources/small-business-lending-resources/small-business-lending-collection-and-reporting-requirements/

What You Need to Do:

Informational for SBL data reporters.

CFPB: Correction to Agency Contact Information (August 25, 2023)

Link

https://www.govinfo.gov/content/pkg/FR-2023-08-25/pdf/2023-18240.pdf

Text

On March 20, 2023, the Consumer Financial Protection Bureau (Bureau or CFPB) published the "Agency Contact Information" final rule in the *Federal Register*. The Bureau has identified clerical errors in that final rule. These errors are found in the Federal agency contact information that must be provided with Equal Credit Opportunity Act adverse action notices in appendix A to Regulation B.

PART 1002—EQUAL CREDIT OPPORTUNITY ACT (REGULATION B)

Appendix A to Part 1002—Federal Agencies To Be Listed in Adverse Action Notices

The following list indicates the Federal agency or agencies that should be listed in notices provided by creditors pursuant to § 1002.9(b)(1). Any questions concerning a particular creditor may be directed to such agencies. This list is not intended to describe agencies' enforcement authority for ECOA and Regulation B. Terms that are not defined in the Federal Deposit Insurance Act (12 U.S.C. 1813(s)) shall have the meaning given to them in the International Banking Act of 1978 (12 U.S.C. 3101).

1. ***Banks, savings associations, and credit unions with total assets of over $10 billion and their affiliates:*** Bureau of Consumer Financial Protection, 1700 G Street NW, Washington, DC 20552. Such affiliates that are not banks, savings associations, or credit unions also should list, in addition to the Bureau: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580.

2. To the extent not included in item 1 above:

a. ***National Banks, Federal savings associations, and Federal branches and Federal agencies of foreign banks:*** Office of the Comptroller of the Currency, Customer Assistance Group, P.O. Box 53570, Houston, TX 77052.

b. ***State member banks, branches and agencies of foreign banks (other than Federal branches, Federal agencies, and insured State branches of foreign banks), commercial lending companies owned or controlled by foreign banks, and organizations operating under section 25 or 25A of the Federal Reserve Act:*** Federal Reserve Consumer Help Center, P.O. Box 1200, Minneapolis, MN 55480.

c. ***Nonmember Insured Banks, Insured State Branches of Foreign Banks, and Insured State Savings Associations:*** Division of Depositor and Consumer Protection, National Center for Consumer and Depositor Assistance, Federal Deposit Insurance Corporation, 1100 Walnut Street, Box #11, Kansas City, MO 64106.

d. *Federal Credit Unions:* Omitted.

*****

What You Need to Do:

Once again, review the supervisory address on your Notice of Action Taken for accuracy.

CFPB: Small Business Lending Rule – Updated FAQs (September 14, 2023)

Link

https://www.consumerfinance.gov/compliance/compliance-resources/small-business-lending-resources/small-business-lending-collection-and-reporting-requirements/small-business-lending-rule-faqs/

Text

The CFPB updated the FAQs regarding the small business lending rule.

Topics include:

- Institutional coverage
- Covered credit transactions
- Small businesses
- Firewall
- Record retention

What You Need to Do:
Informational FAQs regarding the SBL Rule.

CFPB: Adverse Action Notification Requirements & Proper Use of Sample Forms (September 19, 2023)

Link

https://www.consumerfinance.gov/compliance/circulars/circular-2023-03-adverse-action-notification-requirements-and-the-proper-use-of-the-cfpbs-sample-forms-provided-in-regulation-b/

Text

The Consumer Financial Protection Bureau (CFPB) issued guidance about certain legal requirements that lenders must adhere to when using artificial intelligence and other complex models. The guidance describes how lenders must use specific and accurate reasons when taking adverse actions against consumers. This means that creditors cannot simply use CFPB sample adverse action forms and checklists if they do not reflect the actual reason for the denial of credit or a change of credit conditions. This requirement is especially important with the growth of advanced algorithms and personal consumer data in credit underwriting. Explaining the reasons for adverse actions help improve consumers' chances for future credit, and protect consumers from illegal discrimination.

Consumer Financial Protection Circular 2023-03

Question presented

When using artificial intelligence or complex credit models, may creditors rely on the checklist of reasons provided in CFPB sample forms for adverse action notices even when those sample

reasons do not accurately or specifically identify the reasons for the adverse action?

Response

No, creditors may not rely on the checklist of reasons provided in the sample forms (currently codified in Regulation B) to satisfy their obligations under ECOA if those reasons do not specifically and accurately indicate the principal reason(s) for the adverse action. Nor, as a general matter, may creditors rely on overly broad or vague reasons to the extent that they obscure the specific and accurate reasons relied upon.

Analysis

The Equal Credit Opportunity Act (ECOA), implemented by Regulation B, makes it unlawful for any creditor to discriminate against any applicant with respect to any aspect of a credit transaction on the basis of race, color, religion, national origin, sex (including sexual orientation and gender identity), marital status, age (provided the applicant has the capacity to contract), because all or part of the applicant's income derives from any public assistance program, or because the applicant has in good faith exercised any right under the Consumer Credit Protection Act. ECOA and Regulation B require that, when taking adverse action against an applicant, a creditor must provide the applicant with a statement of reasons for the action taken. This statement of reasons must be "specific" and indicate the "principal reason(s) for the adverse action;" moreover, the specific reasons disclosed must "relate to and accurately describe the factors actually considered or scored by a creditor." Adverse action notice requirements promote fairness and equal opportunity for consumers engaged in credit transactions, by serving as a tool to prevent and identify discrimination through the requirement that creditors must affirmatively explain their decisions. In addition, such notices provide consumers with a key educational tool allowing them to understand the reasons for a creditor's action and take steps to improve their credit status or rectify mistakes made by creditors.

The CFPB provides sample forms (currently codified in Regulation B) that creditors may use to satisfy their adverse action notification requirements, if appropriate. These forms include a checklist of sample reasons for adverse action which "creditors most commonly consider," as well as an open-ended field for creditors to provide other reasons not listed. The sample forms are used by creditors to satisfy certain adverse action notice requirements under ECOA and the Fair Credit Reporting Act (FCRA), though the statutory obligations under each remain distinct. While the sample forms provide examples of commonly considered reasons for taking adverse action, "[t]he sample forms are illustrative and may not be appropriate for all creditors." Reliance on the checklist of reasons provided in the sample forms will satisfy a creditor's adverse action notification requirements only if the reasons disclosed are specific and indicate the principal reason(s) for the adverse action taken.

Some creditors use complex algorithms involving "artificial intelligence" and other predictive decision-making technologies in their underwriting models. These complex algorithms sometimes rely on data that are harvested from consumer surveillance or data not typically found in a consumer's credit file or credit application. The CFPB has underscored the harm that can result from consumer surveillance and the risk to consumers that these data may pose. Some of these data may not intuitively relate to the likelihood that a consumer will repay a loan. The CFPB and the prudential regulators have previously noted that these data may create additional consumer protection risk. This Circular addresses adverse action notice requirements under ECOA and

Regulation B; financial institutions also must ensure their use of data and advanced technologies fully complies with other legal requirements, such as the prohibition against illegal discrimination. The CFPB, along with the Department of Justice and other enforcement agencies, have pledged to vigorously use the agencies' collective authorities to protect individuals' rights regardless of whether legal violations occur through traditional means or advanced technologies.

Under ECOA and Regulation B a creditor must provide an applicant with a statement of specific reason(s) for an adverse action; these reasons must "relate to and *accurately* describe the factors *actually* considered or scored by a creditor." A creditor therefore may not rely solely on the unmodified checklist of reasons in the sample forms provided by the CFPB if the reasons provided on the sample forms do not reflect the principal reason(s) for the adverse action. As explained in Regulation B, "if the reasons listed on the forms are not the factors actually used, a creditor will not satisfy the notice requirement by simply checking the closest identifiable factor listed." Rather, the sample forms merely provide an illustrative and non-exclusive list. Thus, if the principal reason(s) a creditor actually relies on is not accurately reflected in the checklist of reasons in the sample forms, it is the duty of the creditor—if it chooses to use the sample forms—to either modify the form or check "other" and include the appropriate explanation, so that the applicant against whom adverse action is taken receives a statement of reasons that is specific and indicates the principal reason(s) for the action taken. Creditors that simply select the closest, but nevertheless inaccurate, identifiable factors from the checklist of sample reasons are not in compliance with the law. Creditors may not evade this requirement, even if the factors actually considered or scored by the creditor may be surprising to consumers, as may be the case when a creditor relies on complex algorithms that, for instance, consider data that are not typically found in a consumer's credit file or credit application.

Because it is unlawful for a creditor to fail to provide a statement of *specific* reasons for the action taken, a creditor will not be in compliance with the law by disclosing reasons that are overly broad, vague, or otherwise fail to inform the applicant of the specific and principal reason(s) for an adverse action. Just as an accurate description of the factors actually considered or scored by a creditor is critical to ensuring compliant adverse action notifications, sufficient specificity is also required. Such specificity is necessary to ensure consumer understanding is not hindered by explanations that obfuscate the principal reason(s) for the adverse action taken. For instance, Regulation B provides the example that a creditor should disclose "insufficient bank references" and not "insufficient credit references," which is listed on the CFPB's sample form, if the creditor considers only references from banks and other depository institutions and not from other institutions.

Specificity is particularly important when creditors utilize complex algorithms. Consumers may not anticipate that certain data gathered outside of their application or credit file and fed into an algorithmic decision-making model may be a principal reason in a credit decision, particularly if the data are not intuitively related to their finances or financial capacity. As noted in the Official Commentary to Regulation B, a creditor must "disclose the actual reasons for denial . . . even if the relationship of that factor to predicting creditworthiness may not be clear to the applicant." For instance, if a complex algorithm results in a denial of a credit application due to an applicant's chosen profession, a statement that the applicant had "insufficient projected income" or "income insufficient for amount of credit requested" would likely fail to meet the creditor's legal obligations. Even if the creditor believed that the reason for the adverse action was broadly related to future income or earning potential, providing such a reason likely would not satisfy its duty to provide the specific reason(s) for adverse action. Concerns regarding specificity may also arise when creditors take adverse action against consumers with existing credit lines. For example, if a creditor decides to lower the limit on, or close altogether, a consumer's credit line based on behavioral data, such as the type of establishment at which a consumer shops or the

type of goods purchased, it would likely be insufficient for the creditor to simply state "purchasing history" or "disfavored business patronage" as the principal reason for adverse action. Instead, the creditor would likely need to disclose more specific details about the consumer's purchasing history or patronage that led to the reduction or closure, such as the type of establishment, the location of the business, the type of goods purchased, or other relevant considerations, as appropriate.

As discussed in an Advisory Opinion, these requirements under ECOA extend to adverse actions taken in connection with existing credit accounts (*i.e.*, an account termination or an unfavorable change in the terms of an account that does not affect all or substantially all of a class of the creditor's accounts), as well as new applications for credit. The CFPB has also made clear that adverse action notice requirements apply equally to all credit decisions, regardless of whether the technology used to make them involves complex or "black-box" algorithmic models, or other technology that creditors may not understand sufficiently to meet their legal obligations. As data use and credit models continue to evolve, creditors have an obligation to ensure that these models comply with existing consumer protection laws.

What You Need to Do:

If your FI uses artificial intelligence (AI), or other complex models, please review and share with appropriate team members.

CFPB/DOJ: Joint Statement on Fair Lending and Credit Opportunities for Noncitizen Borrowers (October 12, 2023)

Link

https://files.consumerfinance.gov/f/documents/cfpb-joint-statement-on-fair-lending-and-credit-opportunities-for-noncitizen-b_jA2oRDf.pdf

Text

The Consumer Financial Protection Bureau and Department of Justice (collectively, the agencies) jointly issue this statement to assist creditors and borrowers in understanding the potential civil rights implications of a creditor's consideration of an individual's immigration status under the Equal Credit Opportunity Act (ECOA).

ECOA does not expressly prohibit consideration of immigration status, and as explained further below, a creditor may consider an applicant's immigration status when necessary to ascertain the creditor's rights regarding repayment. However, creditors should be aware that unnecessary or overbroad reliance on immigration status in the credit decisioning process, including when that reliance is based on bias, may run afoul of ECOA's antidiscrimination provisions and could also violate other laws.

ECOA and Regulation B

The agencies are charged with enforcing the antidiscrimination provisions of ECOA, requirements that are essential for ensuring fair, competitive and nondiscriminatory lending markets. ECOA prohibits discrimination by a creditor in any aspect of a credit transaction, on the basis of race, color, religion, national origin, sex (including sexual orientation and gender identity), marital status, age, an applicant's receipt of public assistance, or the good faith exercise of an applicant's rights under the Consumer Credit Protection Act. 15 U.S.C. § 1691. Discouraging applications for credit on a prohibited basis is also prohibited.

ECOA is implemented by regulations found at 12 C.F.R. part 1002, commonly known as "Regulation B." ECOA and Regulation B apply to all types of credit, including both personal credit and business credit. Among other things, Regulation B sets forth "rules concerning evaluation of applications" for credit. 12 C.F.R. §1002.6. Under Regulation B, creditors shall not consider race, color, religion, national origin, or sex in any aspect of a credit transaction. 12 C.F.R. § 1002.6(b)(9). Subject to that restriction, "a creditor may consider any information obtained, so long as the information is not used to discriminate against an applicant on a prohibited basis." 12 C.F.R. 1002.6(a).

Thus, while ECOA and Regulation B do not expressly prohibit consideration of immigration status, they do prohibit creditors from using immigration status to discriminate on the basis of national origin, race, or any other protected characteristic. Regulation B notably provides that a "creditor may consider [an] applicant's immigration status or status as a permanent resident of the United States, and any additional information that may be necessary to ascertain the creditor's rights and remedies regarding repayment." 12 C.F.R. § 1002.6(b)(7). Regulation B does not, however, provide a safe harbor for all consideration of immigration status.

Issues Related to ECOA, Regulation B and Noncitizen Borrowers

While Regulation B describes certain conditions under which creditors may consider immigration status, creditors should remain cognizant that ECOA and Regulation B expressly forbid discrimination on the basis of certain protected characteristics, including race and national origin. Immigration status may broadly overlap with or, in certain circumstances, serve as a proxy for these protected characteristics. Creditors should therefore be aware that if their consideration of immigration status is not "necessary to ascertain the creditor's rights and remedies regarding repayment" and it results in discrimination on a prohibited basis, it violates ECOA and Regulation B.

Accordingly, creditors must ensure that they do not run afoul of ECOA's nondiscrimination provisions when considering immigration status. As a general matter, creditors should evaluate whether their reliance on immigration status, citizenship status, or "alienage" (i.e., an individual's status as a non-citizen) is necessary or unnecessary to ascertain their rights or remedies regarding repayment. To the extent that a creditor is relying on immigration status for a reason other than determining its rights or remedies for repayment, and the creditor cannot show that such reliance is necessary to meet other binding legal obligations, such as restrictions on dealings with citizens of particular countries, 12 C.F.R. pt. 1002, Supp I. ¶ 2(z)-2, the creditor may risk engaging in unlawful discrimination, including on the basis of race or national origin, in violation of ECOA and Regulation B.

For example, if a creditor has a blanket policy of refusing to consider applications from certain groups of noncitizens regardless of the credit qualifications of individual borrowers within that group, that policy may risk violating ECOA and Regulation B. This risk could arise because some

individuals within those groups may have sufficient credit scores or other individual circumstances that may resolve concerns about the creditor's rights and remedies regarding repayment.

In addition, the overbroad consideration of certain criteria – such as how long a consumer has had a Social Security Number – may implicate or serve as a proxy for citizenship or immigration status, which in turn, may implicate a protected characteristic under ECOA like national origin or race. Such overbroad policies may harm applicants with these protected characteristics without being necessary to ascertain the creditor's rights and remedies for repayment or to meet other binding legal obligations. 12 C.F.R. § 1002.6(b)(7); 12 C.F.R. pt. 1002, Supp I. 2(z)-2. Any claims that such policies are necessary to preserve the creditor's rights and remedies regarding repayment or to meet other binding legal obligations should be supported by evidence and cannot be a pretext for discrimination.

Similarly, if a creditor requires documentation, identification, or in-person applications only from certain groups of noncitizens, and this requirement is not necessary for assessing the creditor's ability to obtain repayment or fulfilling the creditors' legal obligations, that policy may violate ECOA and Regulation B by harming applicants on the basis of national origin or race.

In addition to potential violations of ECOA and Regulation B, creditors should be mindful of their obligations under 42 U.S.C. § 1981 (Section 1981). Section 1981 provides, in relevant part, that "all persons within the jurisdiction of the United States shall have the same right in every State and Territory to make and enforce contracts . . . as is enjoyed by white citizens[,]" 42 U.S.C. § 1981(a), and has long been construed to prohibit discrimination based on alienage. To the extent that a creditor's consideration of immigration status would violate Section 1981, courts have made clear that the limited consideration of immigration status that is permissible under ECOA and Regulation B does not conflict with Section 1981, creditors must therefore comply with both statutes. Indeed, far from conflicting, courts have observed that ECOA's prohibition of national origin discrimination and Section 1981's prohibitions complement one another and that discrimination that arises from overbroad restrictions on lending to noncitizens may violate either or both statutes.

Conclusion

ECOA and other laws protect consumers and help ensure fair lending and credit opportunities for qualified borrowers. Creditors should be mindful of those obligations as they relate to noncitizen borrowers and ensure that credit decisions are based on non-discriminatory criteria.

What You Need to Do:

Be aware that unnecessary or overbroad reliance on immigration status in the credit decisioning process, including when that reliance is based on bias, may run afoul of ECOA's antidiscrimination provisions and could also violate other laws. Review policy and train as appropriate.

CFPB: Final Rule – Annual Threshold Adjustments (Credit Cards, HOEPA, and Qualified Mortgages) (September 18, 2023)

Link

https://www.federalregister.gov/documents/2023/09/21/2023-20476/truth-in-lending-regulation-z-annual-threshold-adjustments-credit-cards-hoepa-and-qualified

Text

The Consumer Financial Protection Bureau (CFPB) issued this final rule amending the official interpretations for Regulation Z, which implements the Truth in Lending Act (TILA). The CFPB is required to calculate annually the dollar amounts for several provisions in Regulation Z; this final rule reviews the dollar amounts for provisions implementing TILA and amendments to TILA, including under the Credit Card Accountability Responsibility and Disclosure Act of 2009 (CARD Act), the Home Ownership and Equity Protection Act of 1994 (HOEPA), and the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act). The CFPB is adjusting these amounts, where appropriate, based on the annual percentage change reflected in the Consumer Price Index (CPI) in effect on June 1, 2023.

This final rule is effective January 1, 2024.

CARD Act Change - Minimum Interest Charge Disclosure Thresholds (Open End Credit) § 1026.6(b)(2)(iii) and 1026.60(b)(3)

The threshold that triggers requirements to disclose minimum interest charges will **remain unchanged at $1.00** in 2024.

CARD Act Change - Safe Harbor Penalty Fees (Open End Credit) § 1026.52(b)(1)(ii)(A) and (B)

Currently, § 1026.52(b)(1)(ii) sets forth a safe harbor of $30 generally for a late payment, except that it sets forth a safe harbor of $41 for each subsequent late payment within the next six billing cycles.

The Consumer Financial Protection Bureau (Bureau) proposed, on February 1, 2023, to amend Regulation Z, which implements the Truth in Lending Act (TILA), to better ensure that the late fees charged on credit card accounts are "reasonable and proportional" to the late payment as required under TILA.

The proposal would (1) lower the safe harbor dollar amount for late fees to $8 and eliminate a

higher safe harbor dollar amount for late fees for subsequent violations of the same type; (2) provide that the current provision that provides for annual inflation adjustments for the safe harbor dollar amounts would not apply to the late fee safe harbor amount; and (3) provide that late fee amounts must not exceed 25 percent of the required payment.

The comment period closed May 3, 2023; a final rule has not yet been published.

Dodd-Frank Act ATR and QM Annual Threshold Adjustments

For HOEPA loans, the adjusted **total loan amount threshold for high-cost mortgages in 2024 will be $26,092.** The adjusted **points and fees dollar trigger for high-cost mortgages in 2024 will be $1,305.**

For the general rule to determine consumers' ability to repay mortgage loans, the maximum thresholds for total points and fees for qualified mortgages in 2024 will be 3 percent of the total loan amount for a loan greater than or equal to $130,461; $3,914 for a loan amount greater than or equal to $78,277 but less than $130,461; 5 percent of the total loan amount for a loan greater than or equal to $26,092 but less than $78,277; $1,305 for a loan amount greater than or equal to $16,308 but less than $26,092; and 8 percent of the total loan amount for a loan amount less than $16,308.

The chart below shows the history of the changes; the acronym TLA means Total Loan Amount. The adjustments are effective January 1, 2024.

2014 Loan Amount	2014 Maximum Points and Fees	2022 Loan Amount	2022 Maximum Points and Fees	2023 Loan Amount	2023 Maximum Points and Fees	2024 Loan Amount	2024 Maximum Points and Fees
$100,000 and higher	3% of TLA	$114,847 and higher	3% of TLA	$124,331 and higher	3% of TLA	$130,461 and higher	3% of TLA
$60,000 to $99,999.99	$3,000	$68,908 to $114,846.99	$3,445	$74,599 to $124,330.99	$3,730	$78,277 to $130,460.99	$3,914
$20,000 to $59,999.99	5% of TLA	$22,969 to $68,907.99	5% of TLA	$24,866 to $74,598.99	5% of TLA	$26,092 to $78,276.99	5% of TLA
$12,500 to $19,999.99	$1,000	$14,356 to $22,968.99	$1,148	$15,541 to $24,865.99	$1,243	$16,308 to $26,091.99	$1,305
Under $12,500	8% of TLA	Under $14,356	8% of TLA	Under $15,541	8% of TLA	Under $16,308	8% of TLA

HOEPA Annual Threshold Adjustments

The adjustments are effective January 1, 2024; the acronym TLA means Total Loan Amount.

2014 Loan Amount	2014 Maximum Points and Fees	2022 Loan Amount	2022 Maximum Points and Fees	2023 Loan Amount	2023 Maximum Points and Fees	2024 Loan Amount	2024 Maximum Points and Fees
$20,000 and higher	5% of TLA	$22,969 and higher	5% of TLA	$24,866 and higher	5% of TLA	$26,092 and higher	5% of TLA
Under $20,000	8% of TLA or $1,000, whichever is lower	Under $22,969	8% of TLA or $1,148, whichever is lower	Under $24,866	8% of TLA or $1,243, whichever is lower	Under $26,092	8% of TLA or $1,305, whichever is lower

What You Need to Do:

Make all necessary changes for 2024. This may include policies, software, training materials, and any other location that this information is pertinent and resides within the banks procedures.

FDIC: Equal Housing Lending Poster Updates (August 31, 2023)

Link

https://www.fdic.gov/news/financial-institution-letters/2023/fil23047.htm

Text

FDIC-supervised institutions are required to maintain up-to-date Equal Housing Lender (EHL) posters in branches, as required by the Fair Housing Act. The FDIC recently amended some details of the posters, including updating the name of the office to which complaints should be addressed, as well as adding the web address of the FDIC's web-based complaint portal. FDIC-supervised institutions may obtain compliant posters from the FDIC Online Catalog through FDICconnect.

On April 23, 2023, the FDIC issued a Federal Register Notice to update and clarify the requirements for EHL posters that are required to be displayed in FDIC-supervised institutions. These changes were necessitated by a name change of the FDIC's entity that receives complaints, from the Consumer Response Center to the National Center for Consumer and Depositor Assistance (NCDA), and the introduction of the web address of the FDIC's web-based complaint portal.

FDIC-supervised institutions are required to update their EHL posters with the following name, address, and web address:

National Center for Consumer and Depositor Assistance

Federal Deposit Insurance Corporation

1100 Walnut Street, Box #11

Kansas City, MO 64106

https://ask.fdic.gov/fdicinformationandsupportcenter

The effective date for these changes was June 23, 2023. Financial institutions are reminded that the NCDA's address to physically mail complaints will be maintained at FDIC.gov, and EHL posters should reflect the correct address.

FDIC-supervised banks may, but are not required to, obtain posters from the FDIC Online Catalog. Institutions may also wish to create their own posters or use third-party providers. Institutions are expected to make good-faith efforts to update the EHL posters as soon as reasonably practicable.

To request copies of the EHL posters from the FDIC, financial institutions must be registered users of the FDICconnect (FCX) system and provisioned for the FDIC Online Catalog. The steps

for FCX users to obtain posters are as follows:

1. To access the FDIC Online Catalog, log into FCX Connect using your FCX Connect credentials.

2. Once you are logged in, you will be redirected to the Business Center Menu.

3. Select the "Ask and Order" link on the upper left side of the screen. The FDIC Online Catalog link will appear underneath.

4. Select the "FDIC Online Catalog Link" and you will be redirected to the FDIC Online Catalog log in screen.

5. Click on the "FDIC Connect Users Click Here" button and you will be redirected to the FDIC Online Catalog.

If you do not have access to FCX, you must first register. The FCX Team can also be reached by phone to answer registration questions through the FDIC Contact Center at 1-877-ASK-FDIC and selecting option #4 on the phone menu for FDICconnect.

What You Need to Do:

Informational for FDIC-supervised FIs. Take appropriate action as necessary.

CFPB: Freedom Mortgage and Realty Connect Penalized for Illegal Kickbacks (August 17, 2023)

Link

https://www.consumerfinance.gov/about-us/newsroom/cfpb-penalizes-freedom-mortgage-and-realty-connect-for-illegal-kickbacks/

Text

The Consumer Financial Protection Bureau (CFPB) took action against Freedom Mortgage Corporation (Freedom) for providing illegal incentives to real estate brokers and agents in exchange for mortgage loan referrals. Freedom provided real estate agents and brokers with numerous incentives — including cash payments, paid subscription services, and catered parties — with the understanding they would refer prospective homebuyers to Freedom for mortgage loans. This conduct violated the Real Estate Settlement Procedures Act and its implementing regulation. The CFPB is ordering Freedom to cease its illegal activities and pay $1.75 million into the CFPB's victim relief fund. The CFPB separately issued an order against a real estate brokerage firm, Realty Connect USA Long Island (Realty Connect), for accepting numerous illegal kickbacks from Freedom. Realty Connect will pay a $200,000 penalty and cease its unlawful conduct.

Freedom is a privately held nonbank mortgage loan originator and servicer headquartered in Boca Raton, Florida. In August 2021, Freedom transferred its traditional retail mortgage unit to its wholly owned subsidiary, RoundPoint Mortgage Servicing (RoundPoint). Freedom's RoundPoint subsidiary ceased traditional retail operations on or around August 2022. Realty Connect is a privately held real estate brokerage firm based in Suffolk County, New York.

The Real Estate Settlement Procedures Act helps reduce closing costs for homebuyers and increases competition in the marketplace by prohibiting mortgage loan originators from offering referral incentives and kickbacks to other companies in exchange for referring homebuyers.

The CFPB found Freedom and Realty Connect violated the Real Estate Settlement Procedures Act. The specific violations include:

- **Paying for referrals through illegal marketing service arrangements:** Freedom entered into marketing services agreements with over 40 real estate brokerages where Freedom made monthly payments totaling approximately $90,000 to brokerages in exchange for the brokerages' marketing services. However, Freedom used these marketing services agreements as a way to pay for mortgage referrals, rather than compensate the brokerages for marketing services they actually performed. Realty Connect received $6,000 per month from Freedom, but failed to perform many of the marketing tasks required under the agreement.

- **Offering premium subscription services free of charge:** Freedom gave real estate brokers and agents free access to valuable industry subscription services, which provided information concerning property reports, comparable sales, and foreclosure data. Freedom paid thousands of dollars per month for one of the subscription services, and Freedom provided access to over 2,000 agents for no cost. Freedom often required real estate agents and brokers to agree to be paired with a Freedom loan officer before Freedom would give them access to its subscription services. Since 2017, the real estate agents who received free access to these subscription services—including agents at both Realty Connect and other brokerages—made more than 1,000 mortgage referrals to Freedom.
- **Hosting and subsidizing company events and providing gifts:** Freedom hosted parties and other events for real estate agents and brokers, including events held exclusively for Realty Connect brokers and agents. Freedom paid for the food, beverages, alcohol, and entertainment. Freedom would also sometimes give free tickets to sporting events, charity galas, or other events where the agents and brokers would have otherwise needed to pay their own way. Freedom also denied requests for event sponsorship from real estate brokerages that did not refer mortgage business to Freedom's loan officers.

Enforcement Action

Under the Consumer Financial Protection Act (CFPA), the CFPB has the authority to take action against institutions violating consumer financial laws, including engaging in unfair, deceptive, or abusive acts or practices. The CFPB found that Freedom and Realty Connect violated the Real Estate Settlement Procedures Act by exchanging items of value in return for mortgage loan referrals.

The orders announced today require Freedom and Realty Connect to:

- **Cease illegal activities**: Freedom is prohibited from providing anything of value to other entities in exchange for mortgage referrals. Realty Connect is prohibited from accepting items of value in exchange for mortgage referrals.
- **Pay nearly $2 million in penalties**: Freedom will pay a $1.75 million penalty into the CFPB victims relief fund. Realty Connect will also pay a $200,000 civil money penalty.

Read the order against Freedom here:

https://www.consumerfinance.gov/enforcement/actions/freedom-mortgage-corporation-2023-respa/

Read the order against Realty Connect here:

https://www.consumerfinance.gov/enforcement/actions/realty-connect-usa-long-island-inc/

The CFPB has published a set of frequently asked questions on the Real Estate Settlement Procedures Act, including guidance on gifts and promotional activity, to help regulated entities understand their obligations under federal law.

Read the frequently asked questions here:

https://www.consumerfinance.gov/compliance/compliance-resources/mortgage-resources/real-estate-settlement-procedures-act/real-estate-settlement-procedures-act-faqs/

What You Need to Do:

Review of RESPA Section 8 violations; take note and share with appropriate team members.

FEMA: National Flood Insurance Program Reauthorization (September 30, 2023)

Link

https://www.fema.gov/flood-insurance/rules-legislation/congressional-reauthorization

Text

Congress must periodically renew the NFIP's statutory authority to operate. On September 30, 2023, the president signed legislation passed by Congress that extends the National Flood Insurance Program's (NFIP's) authorization to November 17, 2023.

Congress must now reauthorize the NFIP by no later than 11:59 p.m. on November 17, 2023.

What You Need to Do:
Be prepared for a lapse of reauthorization of the NFIP; refer to your specific supervisor agency guidance.

Depository Issues

There are no Depository Issues for this period.

Other Issues

CFPB/OCC: Action Against Bank of America (July 11, 2023)

Link

CFPB: https://www.consumerfinance.gov/about-us/newsroom/bank-of-america-for-illegally-charging-junk-fees-withholding-credit-card-rewards-opening-fake-accounts/

OCC: https://www.occ.gov/static/enforcement-actions/ea2023-019.pdf

Text

CFPB Takes Action Against Bank of America for Illegally Charging Junk Fees, Withholding Credit Card Rewards, and Opening Fake Accounts

Bank of America will pay more than $100 million to harmed consumers, and $150 million in penalties to CFPB and Office of the Comptroller of the Currency

The Consumer Financial Protection Bureau (CFPB) ordered Bank of America to pay more than $100 million to customers for systematically double-dipping on fees imposed on customers with insufficient funds in their account, withholding reward bonuses explicitly promised to credit card customers, and misappropriating sensitive personal information to open accounts without customer knowledge or authorization. The Office of the Comptroller of the Currency (OCC) also found that the bank's double-dipping on fees was illegal. Bank of America will pay a total of $90 million in penalties to the CFPB and $60 million in penalties to the OCC.

Bank of America is a global, systemically important bank serving 68 million people and small business clients, and has one of the largest coverages in consumer financial services in the country. As of March 31, 2023, the bank had $2.4 trillion in consolidated assets and $1.9 trillion in domestic deposits, which makes it the second- largest bank in the United States.

Bank of America harmed hundreds of thousands of consumers over a period of several years and across multiple product lines and services. Specifically, Bank of America:

- **Deployed a double-dipping scheme to harvest junk fees:** Bank of America had a policy of charging customers $35 after the bank declined a transaction because the customer did not have enough funds in their account. The CFPB's investigation found that Bank of America double-dipped by allowing fees to be repeatedly charged for the same transaction. Over a period of multiple years, Bank of America generated substantial additional revenue by illegally charging multiple $35 fees.
- **Withheld cash and points rewards on credit cards:** To compete with other credit card companies, Bank of America targeted individuals with special offers of cash and points when signing up for a credit card. Bank of America illegally withheld promised credit card account bonuses, such as cash rewards or bonus points, to tens of thousands of consumers. The bank failed to honor rewards promises for consumers who submitted in-person or over-

the-phone applications. The bank also denied sign-up bonuses to consumers due to the failure of Bank of America's business processes and systems.

- **Misused Sensitive Customer Information to Open Unauthorized Accounts**: From at least 2012, in order to reach now disbanded sales-based incentive goals and evaluation criteria, Bank of America employees illegally applied for and enrolled consumers in credit card accounts without consumers' knowledge or authorization. In those cases, Bank of America illegally used or obtained consumers' credit reports, without their permission, to complete applications. Because of Bank of America's actions, consumers were charged unjustified fees, suffered negative effects to their credit profiles, and had to spend time correcting errors.

This is not the first enforcement action Bank of America has faced for illegal activity in its consumer business. In 2014, the CFPB ordered Bank of America to pay $727 million in redress to its victims for illegal credit card practices. In May 2022, the CFPB ordered Bank of America to pay a $10 million civil penalty over unlawful garnishments and, later in 2022, the CFPB and OCC fined Bank of America $225 million and required it to pay hundreds of millions of dollars in redress to consumers for botched disbursement of state unemployment benefits at the height of the COVID-19 pandemic.

Enforcement Action

Under the Consumer Financial Protection Act, the CFPB has the authority to take action against institutions violating consumer financial protection laws. Bank of America's practices violated the Act's prohibition on unfair and deceptive acts or practices. Bank of America also violated the Fair Credit Reporting Act by using or obtaining consumer reports without a permissible purpose in connection with unauthorized credit cards, as well as the Truth in Lending Act and its implementing Regulation Z, by issuing credit cards to consumers without their knowledge or consent.

The CFPB's orders require Bank of America to:

- **Stop its repeat offenses**: Under the terms of today's orders, Bank of America must stop opening unauthorized accounts, and the bank must disclose material limitations on any rewards cards bonuses and provide bonuses as advertised. Additionally, while Bank of America has generally reduced its reliance on junk fees, the bank is also strictly prohibited from charging repeat non-sufficient funds fees in the future.

- **Pay redress to harmed consumers:** The orders require Bank of America to compensate consumers charged unlawful non-sufficient funds fees and who have not already been made whole by the bank, totaling approximately $80.4 million in consumer redress. The bank must also compensate consumers who incurred costs stemming from the unauthorized opening of new credit card accounts, and any customers improperly denied bonuses whom the bank has not already made whole. The bank previously paid around $23 million to consumers who were denied rewards bonuses.

- **Pay $90 million in penalties to the CFPB:** Bank of America will pay a $60 million penalty to the CFPB for charging repeat non-sufficient funds fees, and a $30 million penalty to the CFPB for its credit card rewards practices and for opening unauthorized accounts. The penalties will be deposited into the CFPB's victims relief fund. Separately, Bank of America will also pay a $60 million penalty to the OCC for its double-dipping fee practices.

OCC Assesses $60 Million Civil Money Penalty Against Bank of America Related to Bank's Overdraft Program

The Office of the Comptroller of the Currency (OCC) announced a $60 million civil money penalty against Bank of America, N.A., for violations of law relating to its practice of assessing multiple overdraft and insufficient funds fees against customers for a single transaction.

The OCC found that Bank of America charged customers tens of millions of dollars in fees on resubmitted transactions. In particular, the bank's practices violated Section 5 of the Federal Trade Commission Act, which prohibits unfair or deceptive acts or practices.

Generally, when a bank receives a check or automated clearing house (ACH) transaction for payment from a customer's deposit account, and the account has insufficient funds available for the payment, the bank may decline to pay the transaction and charge the customer an insufficient funds (NSF) fee. In some instances, third-party merchants resubmit, or represent, such checks or transactions for payment.

Upon representment, if the customer's account still had insufficient funds, Bank of America either charged an additional $35 NSF fee or paid the transaction and charged a $35 overdraft fee. The bank's disclosures did not clearly explain that multiple fees could result from the same transaction. Additionally, customers had no ability to know when or if a merchant would resubmit a transaction to the bank for payment and therefore could not reasonably avoid the assessment of multiple fees for the same transaction. In response to supervisory concerns, Bank of America has waived, refunded, or agreed to refund tens of millions of dollars to customers who were harmed by its practice of charging such fees.

The OCC's civil money penalty order is separate from, but coordinated with, the Consumer Financial Protection Bureau (CFPB), which announced a consent order against Bank of America. The CFPB ordered the bank to redress customers harmed by its practices.

What You Need to Do:

This time, it's Bank of America. Please review and be forewarned; share with appropriate team members.

FRB: Creation of Novel Activities Supervision Program (August 8, 2023)

Link

https://www.federalreserve.gov/supervisionreg/srletters/SR2307.htm

Text

The Federal Reserve has established a Novel Activities Supervision Program (Program) to enhance the supervision of novel activities conducted by banking organizations supervised by the Federal Reserve. The Program will focus on novel activities related to crypto-assets, distributed ledger technology (DLT), and complex, technology-driven partnerships with nonbanks to deliver financial services to customers. The Program will be risk-focused and complement existing supervisory processes, strengthening the oversight of novel activities conducted by supervised banking organizations.

Background

Financial innovation supported by new technologies can benefit the U.S. economy and U.S. consumers by spurring competition, reducing costs, creating products that better meet customer needs, and extending the reach of financial services and products to those typically underserved. Innovation can also lead to rapid change in individual banks or in the financial system and generate novel manifestations of risks that can materially impact the safety and soundness of banking organizations. Given the novelty of these activities, they may create unique questions around their permissibility, may not be sufficiently addressed by existing supervisory approaches, and may raise concerns for the broader financial system.

Novel Activities Supervision Program

The Federal Reserve established the Program to ensure that the risks associated with innovation are appropriately addressed. The Program will enhance the supervision of novel activities conducted by supervised banking organizations, with a focus on the following activities:

- ***Complex, technology-driven partnerships with non-banks to provide banking services*** – Partnerships where a non-bank serves as a provider of banking products and services to end customers, usually involving technologies like application programming interfaces (APIs) that provide automated access to the bank's infrastructure.
- ***Crypto-asset related activities*** – Activities such as crypto-asset custody, crypto-collateralized lending, facilitating crypto-asset trading, and engaging in stablecoin/dollar token issuance or distribution.

- ***Projects that use DLT with the potential for significant impact on the financial system*** – The exploration or use of DLT for various use cases such as issuance of dollar tokens and tokenization of securities or other assets.

- ***Concentrated provision of banking services to crypto-asset-related entities and fintechs*** – Banking organizations concentrated in providing traditional banking activities such as deposits, payments, and lending to crypto-asset-related entities and fintechs.

The Program will work in partnership with existing Federal Reserve supervisory teams to monitor and examine novel activities conducted by supervised banking organizations. Supervised entities engaging in novel activities will not be moved to a separate supervisory portfolio. Instead, the Program will work within existing supervisory portfolios and alongside existing supervisory teams. The Program will leverage current supervisory processes to the extent possible to maximize efficiency and minimize burden.

The Program will be risk-based, and the level and intensity of supervision will vary based on the level of engagement in novel activities by each supervised banking organization. The Federal Reserve will notify in writing those supervised banking organizations whose novel activities will be subject to examination through the Program. The Federal Reserve will periodically evaluate and update which banking organizations should be subject to the examination of novel activities through the Program, and banking organizations will be notified accordingly. In addition, as part of the Program, the Federal Reserve will routinely monitor supervised banking organizations that are exploring novel activities.

To help ensure the Program is informed by diverse perspectives and best practices in supervision and risk-management, it will be advised by a range of multidisciplinary leaders from around the Federal Reserve System. To stay abreast of emerging issues, technologies, and new products, the Program will engage broadly with external experts from academia and the banking, finance, and technology industries. The Program will incorporate insights and analysis from real-time data, market monitoring, horizontal exams, and proactive, intentional, and regular information exchange across portfolios, federal bank regulatory agencies, and other stakeholders.

Through this Program, the Federal Reserve will continue to build upon and enhance its technical expertise to better understand novel activities, the novel manifestations of risks of such activities, and appropriate controls to manage such risks. In addition to enhancing the supervision of risks associated with banking organizations engaging in novel activities, the Program will also inform the development of supervisory approaches and guidance for banking organizations engaging in novel activities, as warranted.

The Program will help ensure that regulation and supervision allow for innovations that improve access to and the delivery of financial services, while also safeguarding bank customers, banking organizations, and financial stability. The Program will also operate in keeping with the principle that banking organizations are neither prohibited nor discouraged from providing banking services to customers of any specific class or type, as permitted by law or regulation.

What You Need to Do:

Informational for FRB-supervised FIs; please review and share with appropriate team members if applicable.

FRB: Supervisory Nonobjection Process for State Member Banks Seeking to Engage in Certain Activities Involving Dollar Tokens (Aug 8, 2023)

Link

https://www.federalreserve.gov/supervisionreg/srletters/SR2308.htm

Text

This letter provides a description of the supervisory nonobjection process for state member banks seeking to engage in certain activities involving tokens denominated in national currencies and issued using distributed ledger technology or similar technologies to facilitate payments (dollar tokens).

Background

On January 27, 2023, the Board of Governors of the Federal Reserve System (Board) issued a Policy Statement on section 9(13) of the Federal Reserve Act (Policy Statement) clarifying that the Board generally presumes that it will exercise its discretion under section 9(13) of the Federal Reserve Act to limit state member banks and their subsidiaries to engaging as principal in only those activities that are permissible for national banks — in each case, subject to the terms, conditions, and limitations placed on national banks with respect to the activity — unless those activities are permissible for state banks by federal statute or under 12 CFR part 362.

In Interpretive Letter 1174, the Office of the Comptroller of the Currency (OCC) specifically recognized the authority of national banks to use distributed ledger technology or similar technologies to conduct payments activities as principal, including by issuing, holding, or transacting in dollar tokens. However, the OCC conditioned the legal permissibility of these activities on a national bank demonstrating, to the satisfaction of its supervisors, that it has in place controls to conduct the activity in a safe and sound manner.

Nonobjection Process for Dollar Token Activities

A state member bank seeking to engage in activities permitted for national banks under OCC Interpretive Letter 1174, including issuing, holding, or transacting in dollar tokens to facilitate payments, is required to demonstrate, to the satisfaction of Federal Reserve supervisors, that the bank has controls in place to conduct the activity in a safe and sound manner. To verify this requirement has been met, a state member bank should receive a written notification of supervisory nonobjection from the Federal Reserve before engaging in the proposed activities.

A state member bank seeking to engage in such dollar token activities, including for the purpose of testing, must notify its lead supervisory point of contact at the Federal Reserve of the bank's intention to engage in the proposed activity and should include a description of the proposed activity. Federal Reserve supervisory staff may follow up with the bank to seek additional information in order to better understand the proposal and the control framework that the state member bank has put in place. After receiving a written notification of supervisory nonobjection, state member banks will continue to be subject to supervisory review and

heightened monitoring of these activities.

To obtain a written notification of supervisory nonobjection, a state member bank should demonstrate that it has established appropriate risk management practices for the proposed activities, including having adequate systems in place to identify, measure, monitor, and control the risks of its activities, and the ability to do so on an ongoing basis. Federal Reserve staff will focus on the risks discussed in the preamble to the Policy Statement with respect to dollar tokens, including, but not limited to:

- **operational risks**, including those risks associated with the governance and oversight of the network; clarity of the roles, responsibilities, and liabilities of parties involved; and the transaction validation process (e.g., timing and finality of settlement of transactions, potential irreversibility of transactions, and the central authority of transaction records);
- **cybersecurity risks**, including risks associated with the network on which the dollar token is transacted, the use of smart contracts, and any use of open source code;
- **liquidity risks**, including the risk that the dollar token could experience substantial redemptions in a short period of time that would trigger rapid outflows of deposits;
- **illicit finance risks**, including risks relating to compliance with Bank Secrecy Act and Office of Foreign Asset Control requirements, which include requiring banking organizations to verify the identity of a customer, perform due diligence to understand the nature and purpose of the customer relationship, and perform ongoing monitoring to identify and report suspicious activity; and
- **consumer compliance risks**, including risks related to identifying and ensuring compliance with any consumer protection statutes and regulations that apply to the specific dollar token activity.

Federal Reserve staff will also assess whether the bank has demonstrated that it understands and will comply with laws that apply to the proposed activities.

What You Need to Do:

Informational for FRB-supervised FIs; please share with appropriate team members if applicable.

Bank Secrecy Act

FFIEC: Updates to the BSA/AML Examination Manual (August 2, 2023)

Link

https://bsaaml.ffiec.gov/

Text

The FFIEC members have reorganized some existing sections of the Manual to create new, individual sections based on specific regulations. Modifications to the six sections included in this release are detailed below. Sections have been deleted from the "Risks Associated with Money Laundering and Terrorist Financing" portion of the Manual. Concepts from the deleted sections are now included within related sections of "Assessing Compliance with BSA Regulatory Requirements." There were no changes to the regulatory requirements covered by these sections. The agencies made revisions to ensure language clearly distinguishes between mandatory regulatory requirements and considerations set forth in guidance or supervisory expectations. The updated sections provide further transparency into the BSA/AML examination process and do not establish new requirements. The FFIEC revised the sections in close collaboration with Treasury's Financial Crimes Enforcement Network.

Revised Section: Special Information Sharing Procedures to Deter Money Laundering and Terrorist Activity

Updated and retitled the previous *Information Sharing* section to align with the regulations at 31 CFR 1010.520 and 31 CFR 1010.540. **See below for the complete section.**

Revised Section: Due Diligence Programs for Private Banking Accounts

Updated and combined the previous Private Banking Due Diligence Program (Non-US Persons) and Private Banking sections and retitled to align with the regulation at 31 CFR 1010.620. **See below for the complete section.**

Revised Section: Due Diligence Programs for Correspondent Accounts for Foreign Financial Institutions

Updated and combined the previous Foreign Correspondent Account Recordkeeping, Reporting and Due Diligence section and Correspondent Accounts (Foreign) sections and retitled to align with the regulation at 31 CFR 1010.610. **See Y&A website for complete section.**

New Section: Prohibition on Correspondent Accounts for Foreign Shell Banks; Records Concerning Owners of Foreign Banks and Agents for Service of Legal Process

Created a new stand-alone section from the previous Foreign Correspondent Account Recordkeeping, Reporting, and Due Diligence section and titled it to align with the regulation at 31 CFR 1010.630. **See Y&A website for the complete section.**

New Section: Summons or Subpoena of Foreign Bank Records; Termination of Correspondent Relationship; Records Concerning Owners of Foreign Banks and Agents for Service of Legal Process

Created a new stand-alone section from the previous Foreign Correspondent Account Recordkeeping, Reporting, and Due Diligence section and titled it to align with the regulation at 31 CFR 1010.670. **See Y&A website for the complete section.**

New Section: Reporting Obligations on Foreign Bank Relationships with Iranian-Linked Financial Institutions

Created new stand-alone section from the existing Foreign Correspondent Account Recordkeeping, Reporting, and Due Diligence section and titled it to align with the regulation at 31 CFR 1060.300. **See Y&A website for the complete section.**

What You Need to Do:
Two sections below; four sections on Y&A website.

SPECIAL INFORMATION SHARING PROCEDURES TO DETER MONEY LAUNDERING AND TERRORIST ACTIVITY

Objective: *Assess the bank's compliance with the Bank Secrecy Act (BSA) regulatory requirements for special information sharing procedures to deter money laundering (ML) and terrorist activity (Section 314 information requests).*

Regulatory Requirements for Special Information Sharing Procedures to Deter Money Laundering and Terrorist Activity

This section outlines the regulatory requirements for banks in 31 CFR Chapter X regarding special information sharing procedures to deter money laundering (ML) and terrorist activity. Specifically, it covers:

- 31 CFR 1010.520
- 31 CFR 1010.540

The regulations discussed in this section implement Section 314 of the USA PATRIOT Act. These regulations establish procedures for the facilitation of information sharing between government agencies and financial institutions, and voluntary information sharing among financial institutions, to deter ML and terrorist activity.

Information Sharing Between Government Agencies and Financial Institutions — Section 314(a) of the USA PATRIOT Act

A federal, state, local, or foreign law enforcement agency investigating ML or terrorist activity may request that the Financial Crimes Enforcement Network (FinCEN) solicit, on the investigating agency's behalf, certain information from banks and other financial institutions or a group of financial institutions. The law enforcement agency must provide a written certification to FinCEN that, at a minimum, states that each individual, entity, or organization about which the law enforcement agency is seeking information is engaged in, or is reasonably suspected based on credible evidence of engaging in, ML or terrorist activity. The law enforcement agency must provide enough specific identifiers, such as a date of birth, address, and taxpayer identification number, to permit a bank or other financial institution to differentiate between common or similar names; and identify one person at the agency who can be contacted with any questions relating to the request. Upon receiving the requisite certification from the requesting law enforcement agency, FinCEN may require a bank to search its records to determine whether it maintains or has maintained accounts for, or has engaged in transactions with, any specified individual, entity, or organization.

Search and Reporting Requirements

FinCEN posts Section 314(a) subject lists through its web-based Secure Information Sharing System (SISS). FinCEN's Frequently Asked Questions Concerning the 314(a) Process (FinCEN's 314(a) FAQs) are available to banks designated as 314(a) participants.

A bank should designate, via their primary federal supervisory agency, one or more persons to be the points of contact (POCs) for receiving information requests from FinCEN. Instructions for updating 314(a) POC information can be found on the SISS, as well as FinCEN's public website. Every two weeks, or more frequently if an emergency request is transmitted, the bank's designated POCs receive notification from FinCEN that new case information has been posted on the SISS. The POCs can access the Section 314(a) subject list and download the files in various formats for searching.

Upon receiving a Section 314(a) information request from FinCEN, a bank must expeditiously search its records to determine whether it maintains or has maintained any account for, or has engaged in any transaction with, each individual, entity, or organization named in FinCEN's request. Except as otherwise provided in the Section 314(a) information request, a bank is only required to search its records for any current account maintained for a named suspect; any account maintained for a named suspect during the preceding 12 months; any transaction conducted by, or on behalf of, a named suspect during the preceding six months that is required under law or regulation to be recorded by the bank or is recorded and maintained electronically by the bank; or any transmittal of funds conducted in which a named suspect was either a transmitter or a recipient during the preceding six months that is required under law or regulation to be recorded by the bank or is recorded and maintained electronically by the bank.

FinCEN's 314(a) FAQs recommend that banks provide Section 314(a) information requests to each domestic subsidiary and affiliate that offers accounts or services that would be subject to Section 314(a) search parameters. However, these searches are not required unless the domestic subsidiary or affiliate meets the statutory definition of a financial institution subject to the requirements of 31 CFR 1010.520. If a bank forwards a Section 314(a) information request to a subsidiary or affiliate and matches are found, the matches should be reported by the bank. The Section 314(a) subject lists cannot be shared with any foreign office, branch, or affiliate, unless

the request specifically states otherwise.

The bank must report any positive matches to FinCEN (via the SISS) within 14 days from the date of posting or in the time frame specified in FinCEN's request. Because this information is valuable to law enforcement, a bank may choose to provide information in addition to a confirmation of a positive match in the comment section of the bank's response.

If a bank identifies an account or transaction identified with any individual, entity, or organization named in a request from FinCEN, the bank must report the following information to FinCEN:

- The name of such individual, entity, or organization;
- The account number of each such account, or in the case of a transaction, the date and type of each such transaction; and
- Any Social Security number, taxpayer identification number, passport number, date of birth, address, or other similar identifying information provided by the individual, entity, or organization when each such account was opened, or each such transaction was conducted.

A bank may provide the Section 314(a) subject lists to a third-party service provider or vendor to perform or facilitate record searches as long as the bank takes the necessary steps, using an agreement or procedures, to ensure that the third party safeguards and maintains the confidentiality of the information. A bank cannot provide direct access to the SISS to a third-party vendor.

According to FinCEN's 314(a) FAQs, if a bank fails to perform or complete searches on one or more Section 314(a) information requests received during the previous 12 months, the bank must immediately obtain these prior requests from FinCEN and perform a retroactive search of the bank's records. The bank is not required to perform retroactive searches in connection with Section 314(a) information requests that were transmitted more than 12 months before the date upon which it discovers that it failed to perform or complete the requested search. Additionally, in performing retroactive searches, a bank is not required to search records created after the date of the original information request.

Use Restrictions and Confidentiality

Section 314(a) subject lists contain parties that are reasonably suspected, based on credible evidence, of engaging in ML or terrorist acts. Section 314(a) subject lists are not updated or corrected if an investigation is dropped, a prosecution is declined, or a subject is exonerated. Section 314(a) subject lists contain sensitive and confidential information, and the regulation restricts the use of the information provided in a Section 314(a) information request. A bank may only use the information to report the required information to FinCEN, to determine whether to establish or maintain an account or engage in a transaction, or to assist with Bank Secrecy Act (BSA)/anti-money laundering (AML) regulatory compliance, such as the filing of suspicious activity reports (SARs). The FinCEN 314(a) FAQs state that banks should not use the fact that parties are identified in Section 314(a) information requests as the sole basis for determining whether to open or maintain an account for named subjects. Furthermore, banks are not required to file a SAR solely because accounts or transactions involving Section 314(a) subjects are identified. The filing of SARs as a result of Section 314(a) information requests should be in accordance with suspicious activity reporting regulations and the bank's policies and procedures. Refer to the Assessing Compliance with BSA Regulatory Requirements - Suspicious Activity

Reporting section of this Manual for more information.

A bank cannot disclose to any person, other than FinCEN, the bank's primary banking regulator, or the law enforcement agency on whose behalf FinCEN is requesting information, the fact that FinCEN has requested or has obtained information under Section 314(a).

Each bank must maintain adequate procedures to protect the security and confidentiality of Section 314(a) information requests from FinCEN. Application of procedures that the bank has already established to protect its customers' nonpublic personal information, in compliance with Section 501 of the Gramm–Leach–Bliley Act and implementing regulations, will be deemed sufficient to protect 314(a) information requests.

Documentation

Although banks are not required to maintain records related to Section 314(a) information requests, FinCEN's 314(a) FAQs recommend that banks maintain records to demonstrate that all required searches have been performed and positive matches reported. Banks may obtain an activity report in the SISS, which provides download and response history. Banks may also choose to keep a manual log of Section 314(a) information requests received and of any positive matches identified and reported to FinCEN. If a bank elects to maintain copies of the Section 314(a) information requests, the bank must maintain the information in a secure and confidential manner.

FinCEN regularly updates a list of recent Section 314(a) search transmissions, including information on the date of transmission, tracking number, and number of subjects listed in the transmission. Banks may review this list to verify that Section 314(a) information requests have been received.

Voluntary Information Sharing Among Financial Institutions — Section 314(b) of the USA PATRIOT Act

Notice and Verification Requirements

Section 314(b) of the USA PATRIOT Act and its implementing regulations permit banks, other financial institutions, and associations of financial institutions, located in the United States, to transmit, receive, or otherwise share information with any other financial institution or association of financial institutions regarding individuals, entities, organizations, and countries for purposes of identifying, and where appropriate, reporting activities that the financial institution or association suspects may involve possible ML or terrorist activity. Banks that choose to voluntarily participate in information sharing under Section 314(b) must file a notice with FinCEN through the SISS. A notice to share information is effective for one year, beginning on the date of the notice, and requires the bank to designate at least one point of contact for receiving and providing information. To continue to engage in the sharing of information after the end of the one-year period, a bank must submit a new notice.

Banks may establish policies and procedures that designate more than one person with the authority to participate in Section 314(b) information sharing. Additionally, prior to sharing information, a bank must take reasonable steps to verify that the other financial institution (or association of financial institutions) with which it intends to share information has also submitted

the required notice to FinCEN. To facilitate the identification of Section 314(b) program participants, FinCEN provides participating banks with access to a list of other participating financial institutions.

Use and Security of Information

A bank that receives information from a financial institution or association of financial institutions related to a Section 314(b) request must limit the use of the information. Such information must not be used for any purpose other than identifying and, where appropriate, reporting on ML or terrorist activities; determining whether to establish or maintain an account, or to engage in a transaction; or assisting the bank in complying with any requirements of Chapter X.

Each bank that voluntarily engages in the sharing of information must maintain adequate procedures to protect the security and confidentiality of the information. Application of procedures that the bank has already established to protect its customers' nonpublic personal information, in compliance with Section 501 of the Gramm–Leach–Bliley Act, will be deemed sufficient to protect 314(b) information requests.

Section 314(b) provides specific protection from liability under U.S. (federal and state) law. A financial institution will be protected under this safe harbor provision if it:

- Notifies FinCEN of its intent to engage in information sharing;
- Verifies that the other financial institution (or association of financial institutions) has submitted the required notice to FinCEN to engage in information sharing;
- Shares information only for permissible purposes; and
- Maintains adequate procedures to protect the security and confidentiality of the information received pursuant to information sharing requests.

Failure to comply with the requirements of 31 CFR 1010.540, however, results in loss of this safe harbor protection. A bank is not required to file a SAR solely as a result of receiving a request to share information under Section 314(b). The bank's policies and procedures on filing SARs should be in accordance with suspicious activity reporting regulations. Section 314(b) does not authorize a bank to share a SAR, nor does it permit a bank to disclose the existence of a SAR. However, a bank may share the underlying transactions and customer information that formed the basis of a SAR. A bank may use information obtained under Section 314(b) to determine whether to file a SAR, and financial institutions sharing information pursuant to Section 314(b) may work together to file joint SARs pursuant to suspicious activity reporting requirements.

Examiner Assessment of Compliance with Special Information Sharing Procedures to Deter Money Laundering and Terrorist Activity

Examiners should assess the adequacy of the bank's policies, procedures, and processes related to the bank's compliance with the BSA regulatory requirements for special information sharing procedures to deter ML and terrorist activity (Section 314 information requests). Examiners may review information, such as independent testing or audit reports, to aid in their assessment of the bank's compliance with information sharing requirements. Refer to the Assessing the BSA/AML Compliance Program - BSA/AML Internal Controls section of this Manual for more information.

SPECIAL INFORMATION SHARING PROCEDURES TO DETER MONEY LAUNDERING AND TERRORIST ACTIVITY EXAMINATION AND TESTING PROCEDURES

Objective: *Assess the bank's compliance with the Bank Secrecy Act (BSA) regulatory requirements for special information sharing procedures to deter money laundering (ML) and terrorist activity (Section 314 information requests).*

Information Sharing Between Government Agencies and Financial Institutions (Section 314(a) of the USA PATRIOT Act)

1. Review the bank's policies, procedures, and processes to comply with regulations regarding information sharing between government agencies and financial institutions. Determine whether the bank's policies, procedures, and processes:

   - Designate points of contact (POCs) for receiving and reviewing information requests.
   - Establish a process for responding to Financial Crimes Enforcement Network (FinCEN's) requests in the manner and in the time frame specified that includes searching the bank's records for:
     - any current account maintained for a named suspect;
     - any account maintained for a named suspect during the preceding 12 months; and
     - any transaction conducted by or on behalf of a named suspect, or any transmittal of funds conducted in which a named suspect was either the transmitter or the recipient, during the preceding six months that is required under law or regulation to be recorded by the financial institution or is recorded and maintained electronically by the institution.
   - Protect the security and confidentiality of the Section 314(a) subject list.

2. Verify that the bank has designated POCs and is receiving Section 314(a) information requests from FinCEN. If the bank is not receiving Section 314(a) information requests or needs to make changes to POC information, the bank should use information provided on FinCEN's website to update POC information in accordance with instructions provided by its primary regulator.

3. If the bank uses a third-party vendor to perform or facilitate searches, determine whether an agreement or procedures are in place to ensure confidentiality. Verify that the bank is not providing direct access to the Secure Information Sharing System (SISS) to a third-party vendor.

4. On the basis of a risk assessment, prior examination reports, and a review of the bank's audit findings, select a sample of Section 314(a) information requests. Review the bank's documentation to evidence compliance with each sampled information request. For example, this documentation may include:

   - Copies of Section 314(a) information requests and documentation that verifies the bank searched appropriate records for each information request received.

- Activity reports from the SISS showing a log of the bank's download and response history, including any positive response dates, or a log that records the tracking numbers, date of review, records and time frames reviewed, reviewing party, and review results.
- Records and supporting documentation of the positive matches reported to verify that a response was provided to FinCEN within the required time frame.
- Confirmation that the bank uses Section 314(a) information requests only in the manner and for the purposes allowed and keeps information secure and confidential. This requirement may be verified through discussions with management.

5. On the basis of the examination and testing procedures completed, form a conclusion about the adequacy of policies, procedures, and processes the bank has developed to meet Bank Secrecy Act (BSA) regulatory requirements associated with Section 314(a) information requests.

Voluntary Information Sharing Among Financial Institutions (Section 314(b) of the USA PATRIOT Act)

1. Determine whether the bank has opted to participate in voluntary information sharing. If the bank participates in voluntary information sharing, verify that the bank has filed a notification form with FinCEN and that the effective date for voluntary information sharing is within the previous 12 months.

2. Review the bank's policies, procedures, and processes for complying with voluntary information sharing requirements. Determine whether the bank's policies, procedures, and processes:

   - Designate at least one POC for receiving and providing information, including identification of such person to FinCEN.
   - Establish a process for initiating and responding to requests, including ensuring that other parties with whom the bank intends to share information (including affiliates) have filed the proper notice.
   - Protect the security and the confidentiality of information received.

3. On the basis of a risk assessment, prior examination reports, and a review of the bank's audit findings, select a sample of voluntary information sharing requests initiated and received. Review the bank's documentation to evidence compliance with voluntary information sharing requirements. For example, this may include documentation that the bank:

   - Verifies that the requesting or receiving financial institution (or association of financial institutions) has filed the proper notice with FinCEN. FFIEC BSA/AML Examination Manual 9 August 2023 Special Information Sharing Procedures to Deter Money Laundering and Terrorist Activity Examination and Testing Procedures
   - Uses information related to voluntary information sharing requests only in the manner and for the purposes allowed and keeps information secure and confidential. This requirement may be verified through discussions with management.

4. On the basis of the examination and testing procedures completed, form a conclusion about the adequacy of policies, procedures, and processes the bank has developed to meet BSA regulatory requirements associated with Section 314(b) information sharing.

DUE DILIGENCE PROGRAMS FOR PRIVATE BANKING ACCOUNTS

Objective: *Assess the bank's compliance with the Bank Secrecy Act (BSA) regulatory requirements for due diligence programs for private banking accounts established, maintained, administered, or managed in the United States for non-U.S. persons.*

Regulatory Requirements for Due Diligence Programs for Private Banking Accounts

This section outlines the regulatory requirements for banks in 31 CFR Chapter X regarding due diligence programs for private banking accounts. Specifically, it covers:

- 31 CFR 1010.605 (Definitions)
- 31 CFR 1010.620

Generally, private banking services (sometimes referred to as wealth management services) consist of personalized services to higher net worth clients. A central point of contact, such as a relationship manager, usually acts as a liaison between the customer and the bank and facilitates the customer's use of the bank's financial services and products. Refer to Appendix N of this Manual for an example of a typical private banking structure and an illustration of the central role of the relationship manager. Banks typically base private banking thresholds and associated fees on the amount of assets under management and on the use of specific products or services. Products and services offered in a private banking relationship may include, but are not limited to:

- Cash management, such as checking accounts, overdraft privileges, cash sweeps, and billpaying services.
- Funds transfers.
- Asset management, such as trust, investment advisory, investment management, custodial, and brokerage services.
- Facilitation of the establishment of shell companies and offshore entities, such as private investment companies, international business corporations, and trusts.
- Lending services, such as mortgage loans, credit cards, personal loans, and letters of credit.
- Financial planning services, including tax and estate planning.
- Other services as requested, such as mail services.

Private banking relationships present varying levels of money laundering (ML), terrorist financing (TF), and other illicit financial activity risks, depending upon the facts and circumstances specific to individual client relationships. Banks may establish, maintain, administer, or manage private banking relationships for both domestic and international customers. However, banks are required to take specific anti-money laundering (AML) measures with respect to private banking accounts established, maintained, administered, or managed in the United States for non-U.S. persons. These measures involve establishing a due diligence program that includes policies, procedures, and controls that are reasonably designed to detect and report any known or suspected ML or suspicious activity conducted through or involving such accounts. Additionally, for private banking accounts in which a senior foreign political figure (SFPF) is a nominal or beneficial owner, the bank's due diligence program must include enhanced scrutiny of the accounts that is reasonably designed to detect and report transactions that may involve the proceeds of foreign corruption.

Some banks may have wealth management and/or private banking accounts that do not meet the definition of "private banking accounts" for purposes of 31 CFR 1010.620. These accounts are

often held by individuals with a high net worth and may also include high-dollar accounts or large transactions. Although these accounts are not covered by 31 CFR 1010.620, they are subject to other applicable Bank Secrecy Act (BSA)/AML regulatory requirements, such as customer due diligence and suspicious activity reporting.

Definitions

For purposes of these requirements, certain terms are defined as follows:

A **"private banking account"** means an account (or any combination of accounts) maintained at a bank that:

- Requires a minimum aggregate deposit of funds or other assets of not less than $1 million;
- Is established on behalf of, or for the benefit of, one or more non-U.S. persons who are direct or beneficial owners of the account; and
- Is assigned to, or is administered or managed by, in whole or in part, an officer, employee, or agent of a bank acting as a liaison between the bank and the direct or beneficial owner of the account.

A **"beneficial owner"** means an individual who has a level of control over, or entitlement to, the funds or assets in an account that, as a practical matter, enables the individual, directly or indirectly, to control, manage or direct the account. The ability to fund an account or the entitlement to the funds of an account alone, however, without any corresponding authority to control, manage, or direct the account (such as in the case of a minor child beneficiary), does not cause the individual to be a beneficial owner.

A **"non-U.S. person"** means a natural person who is neither a U.S. citizen nor is accorded the privilege of residing permanently in the United States pursuant to Title 8 of the United States Code.

A **"senior foreign political figure"** means:

- A current or former:
- Senior official in the executive, legislative, administrative, military, or judicial branches of a foreign government (whether elected or not);
- Senior official of a major foreign political party; or
- Senior executive of a foreign government-owned commercial enterprise.
    - A corporation, business, or other entity that has been formed by, or for the benefit of, any such individual.
    - An immediate family member of any such individual.
    - A person who is widely and publicly known (or is actually known by the relevant bank) to be a close associate of such individual.

A **"senior official or executive"** means an individual with substantial authority over policy, operations, or the use of government-owned resources.

An **"immediate family member"** means spouses, parents, siblings, children, and a spouse's parents and siblings.

Due Diligence Programs for Private Banking Accounts

Banks must maintain a due diligence program that includes policies, procedures, and controls that are reasonably designed to detect and report any known or suspected ML or suspicious activity conducted through or involving any private banking account that is established, maintained, administered, or managed in the United States on behalf of or for the benefit of a non-U.S. person. The due diligence program must be designed to ensure that, at a minimum, the bank takes reasonable steps to:

- Ascertain the identity of all nominal and beneficial owners of a private banking account;
- Ascertain whether any nominal or beneficial owner of a private banking account is an SFPF;
- Ascertain the source(s) of funds deposited into a private banking account and the purpose and expected use of the account; and
- Review the activity of the account to ensure that it is consistent with the information obtained about the client's source of funds, and with the stated purpose and expected use of the account, as needed to guard against ML, and to report, in accordance with applicable laws and regulations, any known or suspected ML or suspicious activity conducted to, from, or through a private banking account.

The purpose and expected account activity can establish a baseline for account activity that enables a bank to better detect potentially suspicious activity and to assess situations where additional verification of information may be necessary. Banks should monitor deposits and transactions as necessary to ensure that activity is consistent with information the bank has received about the client's source of funds and with the stated purpose and expected use of the account. Such monitoring facilitates the identification of accounts that warrant additional scrutiny.

Identifying Senior Foreign Political Figures

As noted above, a bank's due diligence program for private banking accounts must be designed to ensure that the bank takes reasonable steps to ascertain whether any nominal or beneficial owner of a private banking account is an SFPF as defined in the regulation. Procedures for meeting this requirement may include seeking information directly from the customer, obtaining information regarding employment and other sources of income of the customer, or reviewing public sources of information regarding the customer.

Special Requirements for Senior Foreign Political Figures

For private banking accounts in which an SFPF is a nominal or beneficial owner, the bank's due diligence program must include enhanced scrutiny of the account that is reasonably designed to detect and report transactions that may involve the proceeds of foreign corruption. Enhanced scrutiny may include consulting publicly available information regarding the home country of the customer, contacting branches of the U.S. bank operating in the home country of the customer to obtain additional information about the customer and the political environment, and reviewing with greater scrutiny the customer's employment history and sources of income.

For the purposes of this requirement, the term "proceeds of foreign corruption" means any asset or property that is acquired by, through, or on behalf of an SFPF through misappropriation,

theft, or embezzlement of public funds, the unlawful conversion of property of a foreign government, or through acts of bribery or extortion, and includes any other property into which any such assets have been transformed or converted. In cases where a bank files a suspicious activity report (SAR) concerning a transaction that may involve the proceeds of foreign corruption, FinCEN has requested that the term "foreign corruption" be included in the narrative portion of the SAR.

Special Procedures When Due Diligence Cannot Be Performed

A bank's due diligence program for private banking accounts must include procedures to be followed in circumstances where appropriate due diligence cannot be performed, including when the bank should:

- Refuse to open the account.
- Suspend transaction activity.
- File a SAR.
- Close the account.

Examiner Assessment of Compliance with Due Diligence Program Requirements for Private Banking Accounts

Examiners should assess the adequacy of the bank's policies, procedures, and controls related to the bank's compliance with the BSA regulatory requirements for due diligence programs for private banking accounts. Specifically, examiners should determine whether these controls are designed to detect and report any known or suspected ML or suspicious activity conducted through or involving such accounts, as well as comply with due diligence requirements. Examiners may review information, such as independent testing or audit reports, to aid in their assessment of the bank's compliance with due diligence requirements for private banking accounts.

Examiners should determine whether the bank's internal controls for private banking accounts are designed to ensure ongoing compliance with the requirements and are commensurate with the bank's size or complexity and organizational structure. Refer to the Assessing the BSA/AML Compliance Program - BSA/AML Internal Controls section in this Manual for more information. Refer to the Risks Associated with Money Laundering and Terrorist Financing section in this Manual for additional information and procedures regarding ML/TF and other illicit financial activity risks for certain types of private banking activities.

Risk-Based Due Diligence Policies, Procedures, and Controls

A bank's due diligence program must incorporate the minimum requirements noted above and should also be risk-based. Not all private banking clients automatically represent a uniformly higher risk of ML/TF and other illicit financial activities. The potential risk to a bank depends on the facts and circumstances specific to each private banking relationship. The nature and extent of due diligence should be commensurate with the risks presented by the private banking relationship. For example, more due diligence may be appropriate for new clients and clients who operate in, or whose funds are transmitted from or through, jurisdictions with weak AML controls. Due diligence should also be commensurate with the size of an account and the complexity of the

private banking relationship. For example, more due diligence may be appropriate for accounts with relatively more deposits and assets.

Risk-based due diligence policies, procedures, and controls for private banking accounts will vary by bank depending upon a bank's risk profile and may include consideration of the following information about the private banking customer:

- The source of the client's wealth and estimated net worth.
- The nature of the client's profession or business.
- The products and services involved in the relationship.
- The nature and duration of the client's relationship with the bank (including the bank's affiliates).
- The type of client, such as individual, trust, international business corporation, shell company, or private investment company, and, if applicable, the entity's structure, such as privately held or publicly traded stock ownership.
- The geographic locations and AML controls where the private banking customer resides and conducts business.

DUE DILIGENCE PROGRAMS FOR PRIVATE BANKING

ACCOUNTS EXAMINATION AND TESTING PROCEDURES

Objective: *Assess the bank's compliance with the Bank Secrecy Act (BSA) regulatory requirements for due diligence programs for private banking accounts established, maintained, administered, or managed in the United States for non-U.S. persons.*

1. Determine whether the bank offers accounts that meet the regulatory definition of a private banking account:

   - Requires a minimum aggregate deposit of funds or other assets of not less than $1 million;
   - Is established on behalf of, or for the benefit of, one or more non-U.S. persons who are direct or beneficial owners of the account; and
   - Is assigned to, or is administered or managed by, in whole or in part, an officer, employee, or agent of a bank acting as a liaison between the bank and the direct or beneficial owner of the account.

2. Review the bank's due diligence policies, procedures, and controls related to private banking accounts. Determine whether the bank's policies, procedures, and controls:

   - Are reasonably designed to detect and report any known or suspected money laundering (ML) or suspicious activity conducted through or involving any private banking account that is established, maintained, administered, or managed in the United States.
   - Require the bank to take reasonable steps to:
     - Ascertain the identity of all nominal and beneficial owners of a private banking account.
     - Ascertain whether the nominal or beneficial owner of any private banking account is a senior foreign political figure (SFPF).
     - Ascertain the source(s) of funds deposited into a private banking account and the purpose and expected use of the account.

- Review the activity of the account to ensure that it is consistent with the information obtained about the client's source of funds, and with the stated purpose and expected use of the account, as needed to guard against ML, and to report, in accordance with applicable laws and regulations, any known or suspected ML or suspicious activity conducted to, from, or through a private banking account.
- Require the bank to perform enhanced scrutiny for private banking accounts in which an SFPF is a nominal or beneficial owner. Enhanced scrutiny of the account must be reasonably designed to detect and report transactions that may involve the proceeds of foreign corruption.
- Include special procedures to be followed when appropriate due diligence cannot be performed, including when the bank should:
  - Refuse to open the account.
  - Suspend transaction activity.
  - File a suspicious activity report.
  - Close the account.

3. On the basis of a risk assessment, prior examination reports, and a review of the bank's audit findings, select a sample of private banking accounts. The sample should include, if applicable, private banking accounts with nominal or beneficial owners that are SFPFs and/or any private banking accounts that were closed. From the sample selected, determine whether the bank:

   - Ascertained the identity of all nominal and beneficial owners of a private banking account.
   - Ascertained whether the nominal or beneficial owner of any private banking account is an SFPF.
   - Ascertained the source(s) of funds deposited into a private banking account and the purpose and expected use of the account.
   - Completed reviews of activity to ensure it is consistent with the information obtained about the client's source of funds, with the stated purpose and expected use of the account, and with any other information obtained in accordance with the bank's policy.
   - Performed enhanced scrutiny of private banking accounts in which SFPFs are nominal or beneficial owners.
   - Followed special procedures for any private banking accounts where appropriate due diligence was not able to be performed.

4. On the basis of examination and testing procedures completed, form a conclusion about the adequacy of policies, procedures, and controls the bank has developed to meet Bank Secrecy Act (BSA) regulatory requirements for due diligence programs for private banking accounts.

FinCEN: Payroll Tax Evasion and Workers' Compensation Fraud in the Construction Sector (August 15, 2023)

Link

https://www.fincen.gov/sites/default/files/shared/FinCEN_Notice_Payroll_Tax_Evasion_and_Workers_Comp_508%20FINAL.pdf

Text

The Financial Crimes Enforcement Network (FinCEN) is issuing this Notice to call financial institutions' attention to what law enforcement has identified as a concerning increase in state and federal payroll tax evasion and workers' compensation insurance fraud in the U.S. residential and commercial real estate construction industries.

Every year across the United States, state and federal tax authorities lose hundreds of millions of dollars to these schemes, which are perpetrated by illicit actors primarily through banks and check cashers. As described in this Notice, many payroll tax evasion and workers' compensation fraud schemes involve networks of individuals and the use of shell companies and fraudulent documents. These schemes further affect the local and national construction job markets, and put legitimate construction contractors and their employees at a competitive disadvantage. This Notice aligns with the anti-money laundering/countering the financing of terrorism (AML/CFT) National Priorities, and provides financial institutions with an overview of the underlying schemes, red flag indicators, and specific SAR filing instructions.

Description of Payroll Tax Evasion and Workers' Compensation Fraud Schemes

Payroll tax evasion and workers' compensation fraud schemes are perpetrated through the use of shell companies and fraudulent documents. The basic structure of the scheme is as follows:

1. Individuals involved in the scheme will set up a shell company whose sole purpose is to allow certain construction contractors to avoid paying workers' compensation premiums as well as state and federal payroll taxes.

2. The shell company achieves this by engaging in two kinds of fraud:

   - First, once established, the shell company operators take out a minimal workers' compensation policy and rents or sells the policy to construction contractors that employ a much larger number of workers than the policy is designed to cover, thereby committing insurance fraud.
   - Second, the shell company operators facilitate tax fraud because the contractors use the shell company to pay their workers "off the books," and without paying the required state and federal government payroll taxes.

Each step in these schemes is described further below.

Insurance Fraud

Step 1: As described in Figure 1 below, the scheme begins when individuals, usually part of an existing fraud network, recruit others into that network.

Step 2: The new recruits establish a shell company purporting to be a legitimate subcontracting construction company and whose existence enables construction contractors with whom it partners to underbid law-abiding construction firms and evade paying the requisite payroll taxes and workers' compensation premiums. The shell company may also engage in other illicit transactions such as money laundering.

Step 3: Next, the shell company operators, or other facilitators within the network, obtain a minimal workers' compensation policy for a small number of purported employees, typically through a local insurance agent. The insurance policy enables the shell company to apply for and receive official business registration status, which can be verified through the appropriate state authority's website.

Step 4: The shell company then "rents" or sells access to its minimal workers' compensation policy, along with its business license and any tax documents, to construction contractors (who may be complicit in the scheme), most of whom employ a larger number of workers than what the insurance policy is designed to cover. The result is that a workers' compensation policy that was meant to cover just a handful of workers is used fraudulently to cover potentially hundreds of workers. This enables the construction contractors that have rented or purchased access to the workers' compensation policy to avoid paying most of their workers' compensation insurance premiums

Figure 1 – *Establishment of a Shell Construction Company*

Omitted

Evasion of Worker Payroll Taxes

The second component of the scheme is when the construction contractors write checks payable to the shell company to facilitate "off the books" payroll and evade state and federal payroll taxes (Figure 2 below).

Step 1: Construction contractors write checks payable to the shell company which creates the façade that the shell company is performing construction projects.

Step 2: After the shell company operators receive the contractors' checks from either a work crew boss or other representative, the shell company operators will take the checks to a check casher or deposit them into the shell company's bank accounts and make bulk cash withdrawals from the company's bank accounts.

Step 3: The shell company operator will then return the cash to the construction contractor, but not before deducting a fee (typically four to ten percent) from the contractor for renting the workers' compensation insurance policy and conducting the payroll-related cash transactions. The shell company operator may also choose to issue individual checks drawn on the shell company's account and made out directly to each worker working for the construction contractor.

Step 4: The construction contractors will then use the cash or checks to pay the workers without withholding appropriate payroll-related taxes or paying any workers' compensation premiums.

Figure 2 – *Payroll Tax Evasion Transactional Steps*

Omitted

Construction Company Operator Sentenced to Federal Prison for Role in Payroll Tax Evasion Scheme

A Portland, Oregon, area construction company operator was sentenced to federal prison for his role in a multiyear scheme to evade the payment of payroll and income taxes on the wages of construction workers. The individual, Melesio Gomez-Rivera, was sentenced to 30 months in federal prison and three years of supervised release. He was also ordered to pay $29.9 million in restitution to the Internal Revenue Service (IRS). According to court documents, he owned and operated a residential construction company called Novatos Construction. From January 2014 until December 2017, Gomez-Rivera and several other construction company owners conspired with each other and David A. Katz, the operator of Check Cash Pacific, Inc., a check cashing business with locations in the Portland area and Vancouver, Washington, to defraud the United States by facilitating under-the-table cash wage payments to construction workers. Their actions, individually and collectively, impeded and obstructed the IRS's ability to compute, assess, and collect payroll and income taxes due on the cash wages. To carry out the scheme, Gomez-Rivera and the other company owners cashed or had other individuals cash millions of dollars in payroll checks at various locations of Katz's check cashing business, used the cash to pay construction workers under-the-table, and filed false business and payroll tax returns. In total, the group cashed approximately $192 million in payroll checks, causing a combined employment and individual income tax loss of $68 million. On December 2, 2021, a federal grand jury in Portland returned a five-count indictment charging Gomez-Rivera, Katz and four other individuals with conspiring with one another to defraud the United States. Katz was additionally charged with four counts of filing false Currency Transaction Reports (CTRs) with FinCEN. On March 1, 2023, Gomez-Rivera became the first of the six co-conspirators to plead guilty. All others are awaiting trial, presently scheduled to begin on December 5, 2023.

Select Red Flag Indicators of Construction-Related Payroll Tax Evasion and Workers' Compensation Fraud

FinCEN, in coordination with the Internal Revenue Service-Criminal Investigation (IRS-CI) and Homeland Security Investigations (HSI), has identified a range of red flags to assist financial institutions in detecting, preventing, and reporting suspicious transactions associated with shell companies perpetrating payroll tax evasion and workers' compensation fraud in the construction industry. No single red flag is determinative of suspicious activity, and 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 is indicative of payroll tax evasion and workers' compensation fraud or is otherwise suspicious.

1. The customer is a new (i.e., less than two years old) small construction company specializing in one type of construction trade (e.g., framing, drywall, stucco, masonry, painting, etc.) with minimal to no online presence and has indicators of being a shell company for illicit activity.
2. The person or company opening the account has no known prior involvement with, or in, the construction industry, and the individual opening the account provides a non-U.S. passport as a form of identification.

3. Beneficial owners of the shell company have no known prior involvement with, or in, the construction company and may have prior convictions involving fraud.
4. The company's recently acquired workers' compensation insurance policy, which may be verifiable through an official state website, was issued within the last year and covers only a small number of employees. However, a high volume of transactions is observed in the company's bank accounts, which is not commensurate with a construction company of that size.
5. A customer receives weekly deposits in their account that exceed normal account activity from several construction contractors involved in multiple construction trades (e.g., framing, drywall, stucco, masonry, painting, etc.). The deposits may be conducted from locations in multiple cities or states.
6. A customer engages in behavior that suggests efforts to evade CTR filing requirements (e.g., the account holder or company representative alters or cancels a transaction when advised a CTR would be filed or engages in structuring with multiple check payments for under $10,000).
7. A representative of the construction company conducts large or unusual volumes of cash withdrawals or negotiation of checks for cash when accompanied by another involved person(s) or using an armored car service to deliver bulk cash.
8. Large volumes of checks for under $1,000 are drawn on the company's bank account and made payable to separate individuals (i.e., the workers), which are subsequently negotiated for cash by the payee.
9. The company's bank account has minimal to no tax- or payroll-related payments to the IRS, state and local tax authorities, or a third-party payroll company despite a large volume of deposits from clients.
10. The Internet Protocol (IP) address identified from the account holder's online banking activity also may be associated with the online banking activity for another customer involved in the same type of purported construction-related activity.
11. The account holder or company representative makes statements to bank tellers or check cashers that the purpose of the cash withdrawals, negotiation of checks for cash, or check cashing activity is for payroll and the volume, amount, and frequency of transactions are uncharacteristic for a construction company with a small number of employees.

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 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 payroll tax evasion and workers' compensation 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-2023-NTC1"** 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 select SAR Field 34(z) (FRAUD-Other) as the associated suspicious activity type and include the term **"Payroll tax evasion"** and/or **"workers compensation"** 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 any and 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 any and 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.

Law enforcement has found the following types of information, when included as a part of the SAR or when kept as supporting documentation that law enforcement can request, valuable to their investigations:

- Customer profile information for the shell company and owner.
- Spreadsheet of transactional details associated with the suspicious activity. • Examples of deposited or cashed items described in the SAR, including copies of the fronts and backs of checks.
- Examples of checks paid or cashed that were described in the SAR, including copies of the fronts and backs of checks.
- Bank or MSB surveillance footage of the subject(s) of the SAR withdrawing cash or negotiating checks that has been taken inside the branch or agent location (particularly if the customer does not have a driver's license as law enforcement may not have a picture of the person otherwise available), as well as outside before and after the transaction; this may capture footage of the meetings that frequently occur just outside the bank or MSB branch or agent location to disperse the cash to the contractor or crew bosses.
- Any statements made by the subject(s) regarding the basis for the transaction(s).

- IP address information associated with the subject's online banking sessions.

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 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 **"FIN2023-NTC1"** in the **"Comments"** section of the report.

Information Sharing

Information sharing among financial institutions is critical to identifying, reporting, and preventing payroll tax evasion and workers' compensation fraud. 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.

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.

If you have immediate information to share with law enforcement regarding this or any other payroll tax fraud, please contact the IRS-CI field office nearest you (or your state tax authority).

If you would like to report criminal activity relating to this or any other form of workers' compensation, insurance, labor exploitation or wire fraud, please contact HSI at 1-866-347-2423.

What You Need to Do:

Informational; please share with appropriate team members.

FinCEN: Alert on Investment Scam Commonly Known as "Pig Butchering" (September 8, 2023)

Link

https://www.fincen.gov/sites/default/files/shared/FinCEN_Alert_Pig_Butchering_FINAL_508c.pdf

Text

The Financial Crimes Enforcement Network (FinCEN) issued an alert to highlight a prominent virtual currency investment scam known as "pig butchering." Multiple U.S. law enforcement sources estimate victims in the United States have lost billions of dollars to these scams and other virtual currency investment frauds.

"Pig butchering" scams resemble the practice of fattening a hog before slaughter. Victims invest in supposedly legitimate virtual currency investment opportunities before they are conned out of their money. Scammers refer to victims as "pigs," and may leverage fictitious identities, the guise of potential relationships, and elaborate storylines to "fatten up" the victim into believing they are in trusted partnerships before they defraud the victims of their assets—the "butchering." These scams are largely perpetrated by criminal enterprises based in Southeast Asia who use victims of labor trafficking to conduct outreach to millions of unsuspecting individuals around the world.

FinCEN's alert explains the scam's methodology; provides behavioral, financial, and technical red flags to help financial institutions identify and report related suspicious activity; and reminds financial institutions of their reporting requirements under the Bank Secrecy Act.

FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as "Pig Butchering"

The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) is issuing this alert to U.S. financial institutions and the broader public to bring attention to a prominent virtual currency investment scam called "pig butchering." These scams are referred to as "pig butchering" as they resemble the practice of fattening a hog before slaughter. The victims in this situation are referred to as "pigs" by the scammers who leverage fictitious identities, the guise of potential relationships, and elaborate storylines to "fatten up" the victim into believing they are in trusted partnerships. The scammers then refer to "butchering" or "slaughtering" the victim after victim assets are stolen, causing the victims financial and emotional harm. In many cases, the "butchering" phase involves convincing victims to invest in virtual currency, or in some cases, over-the-counter foreign exchange schemes —all with the intent of defrauding them of their investment. Pig butchering scams are largely perpetrated by criminal organizations based in Southeast Asia who use victims of labor trafficking to conduct outreach to millions of unsuspecting individuals around the world. Multiple U.S. law enforcement sources estimate victims in the United States have lost billions of dollars to these scams and other virtual currency investment frauds.

This alert explains the pig butchering scam methodology, provides red flag indicators to assist with identifying and reporting related suspicious activity, and reminds financial institutions of their reporting requirements under the Bank Secrecy Act (BSA). Pig butchering scams are linked to fraud and certain types of cybercrime, which are two of FinCEN's Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) National Priorities.

The information contained in this alert is derived from FinCEN's analysis of BSA data, opensource reporting, and information from law enforcement partners.

Methodology of a Pig Butchering Scam

Initial Contact with Victim

A scammer typically makes initial contact with a potential victim through text messages, direct messages on social media, or other communication tools and platforms, usually under the guise of accidentally reaching a wrong number or trying to re-establish a connection with an old friend. The scammer, who may claim to be an investor or money manager, may also create a social media profile which showcases wealth and an enviable lifestyle. Once the scammer elicits a response from a victim, the scammer will communicate with them over time to establish trust and build a relationship.

The "Investment" Sales Pitch

Once trust or a relationship has been established, the scammer will introduce the victim to a supposedly lucrative investment opportunity in virtual currency and direct them to use virtual currency investment websites or applications designed to appear legitimate, but which are fraudulent and ultimately controlled or manipulated by the scammer. This includes the use of legitimate applications with third-party plugins that allow the scammer to manipulate or falsify information presented to the victim. A scammer may also request remote access to the victim's devices to register accounts with virtual currency service providers (i.e., virtual asset service providers, or VASPs) on the victim's behalf, or instruct their victims to take screenshots of their device so that the scammers can walk them through the process of purchasing virtual currency. According to the FBI, many victims also report being directed to make wire transfers to overseas accounts or purchase large amounts of prepaid cards to purchase virtual currency. The use of virtual currency and virtual currency kiosks is also an emerging method of payment. Once a victim acquires virtual currency, the scammer directs them to "invest" the funds through the investment websites or applications, although the funds are funneled to virtual currency addresses and accounts controlled by scammers and their co-conspirators.

Occasionally, a scammer will leverage high-pressure sales tactics such as telling their victim that they will lose out on the opportunity if they do not invest by a certain deadline. A scammer may also encourage the victim to bring their friends and family to invest into the scheme. In more recent iterations, the scammer will invite the victim to join online or mobile games, advertised as "play-to-earn" games offering financial incentives to players, but which in reality are fake gaming applications created by the scammer to steal virtual currency from players.

The Promise of Greater Returns

Once the victim invests with the scammer, the scammer will show the victim extraordinary returns on the investment that have been fabricated. The scammer may even allow the victim to withdraw a small amount of that investment to further build the victim's confidence before urging

the victim to invest more. Victims have been known to liquidate holdings in tax-advantaged accounts or take out home equity lines of credit (HELOC) and second mortgages on their homes in order to increase their investments.

The Point of No Return

When a victim's pace of investment slows or stops, the scammer will use even more aggressive tactics to extract any final payments. The scammer may present the victim with supposed losses on the investment and encourage them to make up the difference through additional deposits. If the victim attempts to withdraw their investment, the scammer may demand that the victim pay purported taxes or early withdrawal fees. Once the victim is unable or unwilling to pay more into the scam, the scammer will abruptly cease communication with the victim, taking the victim's entire investment with them.

Case Study: Court Authorizes the Seizure of Domains Used in Furtherance of a Cryptocurrency Pig Butchering Scheme

In November 2022, the U.S. Attorney's Office for the Eastern District of Virginia announced the seizure of seven domain names used in a pig butchering scam. According to court records, from at least May through August 2022, scammers induced five victims in the United States by using the seven seized domains, which were all spoofed domains of the Singapore International Monetary Exchange. The term "spoofed" refers to domain spoofing and involves a cyberattack in which fraudsters or hackers seek to persuade individuals that a web address or email belongs to a legitimate and generally trusted company, when in fact it links the user to a false site controlled by a cybercriminal. The scammers convinced the victims that they were investing in a legitimate cryptocurrency opportunity. After the victims transferred investments into the deposit addresses that the scammers provided through the seven seized domain names, the victims' funds were immediately transferred through numerous private wallets and swapping services in an effort to conceal the source of the funds. In total, the victims lost over $10 million.

Red Flag Indicators

FinCEN, in consultation with law enforcement, has identified the following indicators to help detect, prevent, and report potential suspicious activity related to pig butchering. As 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 behavior or transaction is suspicious or otherwise indicative of pig butchering. In line with their risk-based approach to compliance with the BSA, financial institutions are also encouraged to perform additional due diligence where appropriate.

Behavioral Red Flags

1. A customer with no history or background of using, exchanging, or otherwise interacting with virtual currency attempts to exchange a high amount of fiat currency from an existing or newly opened bank account for virtual currency or attempts to initiate high-value transfers to VASPs.

2. A customer mentions or expresses interest in an investment opportunity leveraging virtual currency with significant returns that they were told about from a new contact who reached out to them unsolicited online or through text message.
3. A customer mentions that they were instructed by an individual who recently contacted them to exchange fiat currency for virtual currency at a virtual currency kiosk and deposit the virtual currency at an address supplied by the individual.
4. A customer appears distressed or anxious to access funds to meet demands or the timeline of a virtual currency investment opportunity.

Financial Red Flags

5. A customer uncharacteristically liquidates savings accounts prior to maturation, such as a certificate of deposit, and then subsequently attempts to wire the liquidated fiat currency to a VASP or to exchange them for virtual currency.
6. A customer takes out a HELOC, home equity loan, or second mortgage and uses the proceeds to purchase virtual currency or wires the proceeds to a VASP for the purchase of virtual currency.
7. A customer receives what appears to be a deposit of virtual currency from a virtual currency address at or slightly above the amount that the customer previously transferred out of their virtual currency account. This deposit is then followed by outgoing transfers from the customer in substantially larger amounts.
8. Accounts with large balances that are inactive or have limited activity begin to show constant, uncharacteristic, sudden, abnormally frequent, or significant withdrawals of large amounts of money being transferred to a VASP or being exchanged for virtual currency.
9. A customer sends multiple electronic funds transfers (EFTs) or wire transfers to a VASP or sends part of their available balance from an account or wallet they maintain with a VASP and notes that the transaction is for "taxes," "fees," or "penalties."
10. A customer with a short history of conducting several small-value EFTs to a VASP abruptly stops sending EFTs and begins sending multiple high-value wire transfers to accounts of holding companies, limited liability corporations, and individuals with which the customer has no prior transaction history. This is indicative of a victim sending trial transactions to a scammer before committing to and sending larger amounts.

Technical Red Flags

11. System monitoring and logs show that a customer's account is accessed repeatedly by unique IP addresses, device IDs, or geographies inconsistent with prior access patterns. Additionally, logins to a customer's online account at a VASP come from a variety of different device IDs and names inconsistent with the customer's typical logins.
12. A customer mentions that they are transacting to invest in virtual currency using a service that has a website or application with poor spelling or grammatical structure, dubious customer testimonials, or a generally amateurish site design.
13. A customer mentions visiting a website or application that is purported to be associated with a legitimate VASP or business involved in investing in virtual currency. The website or application shows warning signs such as a web address or domain name that is misspelled in such a manner as to resemble that of another business, a recently

registered web address or domain name, no physical street address, international contact information, or contact methods that include only chat or email.

14. A customer mentions that they downloaded an application on their phone directly from a third-party website, rather than from a well-known third-party application store or an application store installed by the manufacturer of the device.
15. A customer receives a large amount of virtual currency such as ether at an exchange, subsequently converts the amount to a virtual currency with lower transaction fees such as TRX, and then abruptly sends it out of the exchange.

Pig Butchering Fraud Reporting

In addition to filing a SAR, financial institutions are encouraged to refer their customers who may be victims of pig butchering to the FBI's IC3: https://www.ic3.gov/, and may also refer their customers to the Securities and Exchange Commission's tips, complaints, and referrals (TCR) system to report investment fraud: https://www.sec.gov/tcr.

In the case of elder victims of pig butchering, financial institutions may also refer their customers to DOJ's National Elder Fraud Hotline at 833-FRAUD-11 or 833-372-8311.

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, including pig butchering. 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 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

When filing a SAR in connection with this alert, FinCEN requests that financial institutions include the key term **"FIN-2023-PIGBUTCHERING"** in SAR field 2 (Filing Institution Note to FinCEN) and the narrative to indicate a connection between the suspicious activity being reported and the activities highlighted in this alert. Financial Institutions should also select "Fraud-Other" under SAR field 34(z) with the description "Pig Butchering."

Financial institutions should include any and all available information relating to the account and locations involved in the reported activity, identifying information and descriptions of any legal entities or arrangements involved and associated beneficial owners, and any information about related persons or entities involved in the activity. Financial institutions also should provide any and 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.

Inclusion of Technical Cyber Indicators: When submitting a report pursuant to this alert, financial institutions should include any relevant technical cyber indicators related to cyber events and associated transactions within the available structured cyber event indicator fields on the SAR form or as part of the attachment field. Any data or information that helps identify the activity as suspicious can be included as an indicator. Examples include chat logs, phone numbers, and social media usernames used by the scammer; suspicious email addresses; type of virtual currency and digital assets involved; virtual currency and / or digital asset addresses and transaction hashes native to the blockchain(s) involved; apps used; and the URL, domain, and IP address of the service the victim was instructed to deposit into.

Other Relevant BSA Reporting Requirements

Financial institutions and other entities or persons may also have other relevant BSA reporting requirements to provide information in connection with the subject of this alert. 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 alert, FinCEN requests that the filer select ***Box 1b*** ("suspicious transaction") and include the key term **"FIN2023-PIGBUTCHERING"** in the **"Comments"** section of the report.

Information Sharing

Information sharing among financial institutions is critical to identifying, reporting, and preventing pig butchering and related 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.

For Further Information

Questions or comments regarding the contents of this alert should be sent to the FinCEN Regulatory Support Section at frc@fincen.gov.

What You Need to Do:

Informational; please share with appropriate team members.

FinCEN: Analysis of Trends and Patterns in Suspicious Activity Potentially Tied to Evasion of Russia-Related Export Controls (September 8, 2023)

Link

https://www.fincen.gov/sites/default/files/shared/FTA_Russian_Export_Controls_FINAL_508.pdf

Text

The Financial Crimes Enforcement Network (FinCEN) issued a Financial Trend Analysis (FTA) on patterns and trends contained in Bank Secrecy Act (BSA) reporting on suspected evasion of Russia-related export controls. The BSA reports analyzed for this FTA were filed in response to previous joint Alerts on this topic and indicate almost $1 billion in suspicious activity.

The Bureau of Industry and Security (BIS) leverages information from BSA reporting filed in response to the joint Alerts by providing leads to their export enforcement agents to help predicate new investigations and support preexisting investigations. BIS also uses the information gleaned from BSA reporting to identify parties in Russia and third countries acting contrary to U.S. national security and foreign policy interests, leading to their designation on the Entity List and imposition of license requirements for transactions subject to the Export Administration Regulations. Both of these efforts disrupt the ability of foreign parties to evade BIS export controls.

The FTA describes several trends found in this BSA reporting:

- Suspicious transactions conducted after Russia's invasion indicate that companies in intermediary countries appear to have purchased U.S.-origin goods on behalf of Russian end-users.
- Suspicious transactions link trade activity, likely involving sensitive items, between end users in Russia and other jurisdictions, particularly China, Hong Kong, and Turkey.
- The majority of companies within the dataset are linked to the electronics industry and are potentially associated with—or directly facilitating—Russian export control evasion.
- Companies in the industrial machinery industry are also potentially supplying Russia with equipment.

FinCEN anticipates that new trends in BSA data may emerge as more individuals and entities are publicly identified as being potentially connected to evasion of Russia-related export controls.

For formal guidance to financial institutions on reporting suspicious activity related to Russia-linked actors, please refer to FinCEN's resource page on advisories, at

https://www.fincen.gov/resources/advisoriesbulletinsfact-sheets.

What You Need to Do:

Informational; please share with appropriate team members.

FinCEN: Small Entity Compliance Guide for Beneficial Ownership (September 18, 2023)

Link

https://www.fincen.gov/sites/default/files/shared/BOI_Small_Compliance_Guide_FINAL_Sept_508C.pdf

Text

The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) published a Small Entity Compliance Guide to assist the small business community in complying with the beneficial ownership information (BOI) reporting rule. Starting in 2024, many entities created in or registered to do business in the United States will be required to report information about their beneficial owners—the individuals who ultimately own or control a company—to FinCEN. The Guide is intended to help businesses determine if they are required to report their beneficial ownership information to FinCEN.

The Guide is now available on FinCEN's beneficial ownership information reporting webpage.

Among other things, the Guide:

- Describes each of the BOI reporting rule's provisions in simple, easy-to-read language;
- Answers key questions; and
- Provides interactive checklists, infographics, and other tools to assist businesses in complying with the BOI reporting rule.

The requirements become effective on January 1, 2024, and companies will be able to begin reporting beneficial ownership information to FinCEN at that time. FinCEN will provide additional guidance on how to submit beneficial ownership information soon. Small businesses can continue to monitor FinCEN's website for more information or subscribe to FinCEN updates.

What You Need to Do:

Informational; please share with appropriate team members.

FinCEN: NPRM to extend the deadline for certain companies to file their beneficial ownership information reports (September 27, 2023)

Link

https://www.federalregister.gov/documents/2023/09/28/2023-21226/beneficial-ownership-information-reporting-deadline-extension-for-reporting-companies-created-or

Text

The Financial Crimes Enforcement Network (FinCEN) issued a Notice of Proposed Rulemaking (NPRM) to extend the deadline for certain reporting companies to file their initial beneficial ownership information (BOI) reports.

FinCEN is proposing to amend its final BOI Reporting Rule to provide 90 days for reporting companies created or registered in 2024 to file their initial reports, instead of 30 days. The proposed rule would not make any other changes to the final BOI Reporting Rule: reporting companies created or registered before January 1, 2024, would have until January 1, 2025, to file their initial BOI reports with FinCEN, and entities created or registered on or after January 1, 2025, would have 30 days to file their initial BOI reports.

FinCEN believes the proposed extension will have significant benefits. An extension will give reporting companies created or registered in 2024 additional time to understand their regulatory obligations under the Reporting Rule and obtain the required information. They will also have additional time to become familiar with FinCEN's guidance and educational materials located at www.fincen.gov/boi and resolve questions that may arise in the process of completing their initial BOI reports. After January 1, 2025, however, reporting companies should be familiar with BOI reporting requirements and be in a better position to file required BOI reports on a timely basis.

FinCEN strongly encourages all interested parties to submit comments on the NPRM. Written comments on the NPRM should be submitted by October 30, 2023.

What You Need to Do:

Informational; please share with appropriate team members.

FinCEN: Beneficial Ownership Information FAQs (September 29, 2023)

Link

https://www.fincen.gov/sites/default/files/shared/BOI_FAQs_Q&A_09.29.23._508C.pdf

Text

FinCEN has prepared Frequently Asked Questions (FAQs) in response to inquiries received relating to the Beneficial Ownership Information Reporting Rule.

These FAQs are explanatory only and do not supplement or modify any obligations imposed by statute or regulation. Please refer to the Beneficial Ownership Information Reporting Rule, available at www.fincen.gov/boi, for details on specific provisions. FinCEN expects to publish additional guidance in the future. Questions may be submitted on FinCEN's Contact web page.

What You Need to Do:

Informational; please share with appropriate team members.