Rulemaking on Anti-Money Laundering and Countering the Financing of Terrorism Programs
Comments

to the

Financial Crimes Enforcement Network (FinCEN)
United States Department of the Treasury

Regarding

Docket Number FINCEN–2024–0013
89 FR 55428 (July 3, 2024).

by the
National Consumer Law Center
on behalf of its low-income clients

Filed on September 3, 2024

Table of Contents

September 3, 2024

Financial Crimes Enforcement Network (FinCEN)
United States Department of the Treasury
Policy Division,
P.O. Box 39
Vienna, VA 22183

Re: Docket Number FINCEN–2024–0013

The National Consumer Law Center ("NCLC"),[1] on behalf of our low-income clients, is pleased to respond to the Financial Crimes Enforcement Network's (FinCEN) Proposed Notice of Rulemaking on Anti-Money Laundering and Countering the Financing of Terrorism Programs.[2]

We support FinCEN's efforts to strengthen and modernize the anti-money laundering and countering the financing of terrorism (AML/CFT) program requirements for financial institutions, but we urge FinCEN to do more. We especially support the inclusion of fraud in the priorities issued by FinCEN on June 20, 2021,[3] and its incorporation into the proposed rule.

FinCEN must, however, take additional steps to emphasize the importance of fraud prevention and fraud detection in combating money laundering and financing of terrorism within the U.S. banking and payments system. Specifically, FinCEN must place stricter requirements on non-bank entities that engage in payment and banking services. FinCEN should also update the SAR to catch information about accounts that receive fraudulent funds, and FinCEN should take additional measures to promote information sharing about payment fraud.

We also believe more clarity and guidance need to be included in the proposed rule as well as in any implementing guidance and examination manuals to ensure that financial institutions do not define risk too broadly. Financial institutions should not consider credit risk as a factor in developing and implementing an AML/CFT program, and without clarity, blunt-fisted, opaque identification requirements exclude vulnerable consumers from the U.S. banking system and allow for discrimination. More specificity and clarity are also necessary so that overly aggressive BSA/AML programs targeting fraud do not lead to bank account closures and freezes.

[1] Since 1969, the nonprofit National Consumer Law Center® (NCLC®) has used its expertise in consumer law and energy policy to work for consumer justice and economic security for low-income and other disadvantaged people in the United States. NCLC's expertise includes policy analysis and advocacy; consumer law and energy publications; litigation; expert witness services, and training and advice for advocates. NCLC works with nonprofit and legal services organizations, private attorneys, policymakers, and federal and state government and courts across the nation to stop exploitative practices, help financially stressed families build and retain wealth, and advance economic fairness. NCLC publishes a series of consumer law treatises, including *Consumer Banking and Payments Law* (7th ed. 2024), updated at library.nclc.org.

[2] The Notice of Proposed Rulemaking is available at https://www.federalregister.gov/d/2024-14414/page-55428 and published at 89 FR 55428 (Jul. 3, 2024).

[3] AML/CFT Priorities (Jun. 30, 2021), available at https://www.fincen.gov/news/newsreleases/fincen-issues-first-national-amlcftpriorities-and-accompanying-statements.

Additionally, FinCEN should protect specific vulnerable populations such as immigrants, domestic violence survivors, and justice-impacted individuals who experience financial exclusion often exacerbated by overly broad BSA/AML programs.

Finally, FinCEN should be extremely cautious and vigilant about the use of AI in AML/CFT programs and BSA compliance.

I. The BSA regime plays an important role in combatting fraud, and FinCEN should take additional steps to address payment fraud.

A. FinCEN must place stricter requirements on non-bank entities that engage in payment and banking services.

The proposed rule focuses on modernizing and strengthening the AML/CFT programs at financial institutions, but it does not address the specific requirements for complying with other parts of the Bank Secrecy Act (BSA). While we support the proposed rule, FinCEN must take additional steps to emphasize the importance of fraud prevention and fraud detection in combating money laundering and financing of terrorism within the U.S. banking and payments system. Specifically, FinCEN should expand the Customer Identification Program (CIP) and customer due diligence (CDD) requirements for entities other than banks that engage in payment and banking services, such as person-to person (P2P) payment apps, payment processors, fintech companies offering banking as a service or offering bank-like services, and crypto-related entities including crypto exchange platforms.

Person-to-person (P2P) payment apps have become increasingly popular among consumers. Seventy-six percent of households use Venmo or Cash App.[4] In addition to P2P payment services, consumers are also increasingly adopting other forms of technology to make payments.[5] These newer payment apps and technologies are accepted by more retailers, demonstrate a rapid growth trajectory, are situated within platforms with other financial services, and are being structured to work with crypto.

These platforms have become fertile ground for fraudsters and organized crime, posing risks to consumers and law enforcement. According to the FTC,[6] "payment app or service" is the third largest category of payment method specified by fraud victims in terms of number of reports (after credit cards and debit cards) for all of 2023, and the second largest category of payment method specified by fraud victims in terms of number of reports (after credit cards) for the first

[4] Anderson, Monica, "*Payment Apps like Venmo and Cash App Bring Convenience – and Security Concerns – to Some Users*," Pew Research Center (blog), (Sept. 8, 2022), available at https://www.pewresearch.org/short-reads/2022/09/08/payment-apps-like-venmo-and-cash-app-bring-convenience-and-security-concerns-to-some-users/.
[5] Chen, Jane, Mahajan, Deepa, Nadeau, Marie-Claude and Varadarajan, Roshan, "*Consumer Digital Payments: Already Mainstream, Increasingly Embedded, Still Evolving*," Digital Payments Consumer Survey, (Oct. 20, 2023), available at https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/consumer-digital-payments-already-mainstream-increasingly-embedded-still-evolving.
[6] Reports of fraud to the FTC do not always specify the payment method utilized to perpetuate the fraud; however, the FTC does collect and report data on payment method when available.

two quarters of 2024.[7] The Consumer Financial Protection Bureau (CFPB) has also seen high growth in complaints about fraud in P2P apps and digital wallets.[8] The existing P2P payment systems of large technology companies and financial institutions simply are not safe for consumers to use.[9]

P2P fraud has a particularly harsh impact on low-income families and communities of color. These communities, already struggling and often pushed out of the traditional banking system, can least afford to lose money to scams and errors. Because many minorities are also unbanked or underbanked,[10] they are the target audience for use of many of the P2P apps.[11] For example, a September 2022 Pew Research Center survey shows that 59% of Cash App users are Black and 37% are Hispanic.[12] Cash App has been subject to reports of widespread fraud,[13] failing to protect the very vulnerable populations it targets.

Cryptocurrency is another large category where reports of fraud are rife. "Cryptocurrency" "is the second largest category of payment method reported by fraud victims to the FTC in terms of number of dollars lost (after bank transfer or payment) for all of 2023 and the first two quarters of 2024.[14] Crypto platforms are not just prone to fraud by third parties; several crypto firms that

[7] FTC fraud reports by payment method, available at https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods. For 2023, only 474,328 (18%) of 2,606,042 fraud reports received by the FTC specified the payment method. For the first two quarters of 2024, only 222,540 (21%) of 1,085,474 fraud reports received by the FTC specified the payment method.

[8] U.S. PIRG Educ. Fund, *Virtual Wallets, Real Complaints*, at 2, (June 2021), available at https://uspirg.org/sites/pirg/files/reports/VirtualWallets/Virtualwallets_USP_V3.pdf.

[9] *See* Comments of 65 Consumer, Civil Rights, Faith, Legal Services and Community Groups to CFPB on Big Tech Payment Platforms at 4-5, Docket No. CFPB-2021-0017 (Dec. 21, 2021), available at https://bit.ly/CFPB-BTPS-comment ("CFPB Big Tech Payment Platform Comments"); Comments of 43 consumer, small business, civil rights, community and legal service groups to Federal Reserve Board Re: Collection of Checks and Other Items by Federal Reserve Banks and Funds Transfers Through Fedwire, Docket No. R-1750; RIN 7100-AG16 (Sept. 9, 2021), available at https://bit.ly/FedNowCoalitionComments (FedNow Comments).

[10] 11.3 percent of Black and 9.3 percent of Latino households are unbanked compared to only 2.1% of white households. *See* FDIC, *2021 FDIC National Survey of Unbanked and Underbanked Households*, at 2, available at https://www.fdic.gov/analysis/household-survey/2021report.pdf (last updated Jul. 24, 2023).

[11] As discussed more in Sections III.A.B. and D., the implementation of overly broad BSA/AML compliance programs at financial institutions also serve to push these underbanked and unbanked populations to unsafe products and platforms that offer bank-like services.

[12] Anderson, Monica, "*Payment apps like Venmo and Cash App bring convenience – and security concerns – to some users*," Pew Research Center (Sept. 8, 2022), available at https://www.pewresearch.org/short-reads/2022/09/08/payment-apps-like-venmo-and-cash-app-bring-convenience-and-security-concerns-to-some-users/.

[13] Hindenburg Research, "*Block: How Inflated User Metrics and 'Frictionless' Fraud Facilitation Enabled Insiders To Cash Out Over $1 Billion*," (Mar. 23, 2023), available at https://hindenburgresearch.com/block/. ("Former employees estimated that 40%-75% of accounts they reviewed were fake, involved in fraud, or were additional accounts tied to a single individual").

[14] FTC fraud reports by payment method, available at https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods. For 2023, roughly $ 1.4 billion was reported as lost due to fraud by cryptocurrency and $678.8 million in the first two quarters of 2024.

suffered losses or became insolvent during the 2022 crash in the crypto markets engaged in practices many believe were unfair, abusive, or deceptive.[15]

Perhaps just as troubling is the intent of many crypto companies to expand crypto-assets into the U.S. banking and payments system. Several large, well-capitalized crypto firms have made it clear that their business model is focused on making crypto and blockchain-based ledgers a mainstream payment method for American consumers. For example, at least one major payment provider has created a stablecoin expressly intended to facilitate consumers' purchase of household goods and services,[16] while another crypto "native" firm has created a platform where retail merchants are provided crypto wallets that can receive direct crypto payments from customers, without the need to convert crypto assets into fiat currency to settle the transaction.[17] Reports claim that the platform processes payments for thousands of merchants, for 'on-chain' payments worth billions of dollars.[18]

Even if FinCEN does not act to expand the Customer Identification Program (CIP) and customer due diligence (CDD) requirements for entities other than banks that engage in payment and banking services, or impose other more rigorous requirements for these non-bank entities, guidance and supervision/examination manuals should clarify that these types of entities are "intermediaries" as the term is defined in the proposed rule,[19] and any financial institution that conducts business with these entities should consider that activity a risk.

B. FinCEN should update the SAR to capture information about accounts that receive fraudulent funds.

FinCEN can help in the fight against payment fraud by updating the suspicious activity report (SAR) to encompass information about the accounts used to receive ill-gotten funds. The current SAR form only accommodates accounts related to the reporting institution.[20] In fraud cases where the destination account of the perpetrator is known, reporting institutions relegate the destination account to the narrative. This makes identification and aggregation of fraudulent activity more difficult for law enforcement.

When a consumer's financial institution files a SAR following an incident of payment fraud, if the payment was sent through a system that identifies the recipient (such as a wire transfer, ACH, or P2P system), the SAR should identify the recipient institution and account. Allowing accounts

---

[15] Federal Trade Commission, *"FTC Reaches Settlement with Crypto Company Voyager Digital; Charges Former Executive with Falsely Claiming Consumers' Deposits Were Insured by FDIC,"* (Oct. 12, 2023), available at https://www.ftc.gov/news-events/news/press-releases/2023/10/ftc-reaches-settlement-crypto-company-voyager-digital-charges-former-executive-falsely-claiming.

[16] PayPal, *"Designed for Payments. 1 USD: 1 PYUSD on PayPal,"* (accessed Jan. 5, 2024), available at https://www.paypal.com/us/webapps/mpp/digital-wallet/manage-money/crypto/pyusd.

[17] Coinbase, *"A New Standard in Global Crypto Payments: Coinbase Commerce,"* (accessed Jan. 5, 2024), available at https://www.coinbase.com/commerce.

[18] Akolkar, Bhushan, "*New Payments Protocol for Coinbase Commerce to Facilitate Instant Crypto Settlements*," *CoinGape* (blog), (Nov. 17, 2023), available at https://coingape.com/new-payments-protocol-for-coinbase-commerce-to-facilitate-instant-crypto-settlements/.

[19] *See* 89 FR 55428 (Jul. 3, 2024) at 55438-9.

[20] FinCEN SAR XML Electronic Filing Requirements: XML Schema 2.0, p. 108. (allowing only 33 – Subject and 41 Financial Institution Where Account Is Held as the only values).

not domiciled at the reporting institution to be reported and designated appropriately would assist FinCEN and law enforcement in identifying, aggregating, and prioritizing fraud investigations to better protect consumers.

Since fraud schemes affect many victims at various reporting institutions, fraud often results in a hub-and-spoke relationship with one account receiving funds from many different, unrelated accounts. This typology is recognized in the FFIEC Exam Manual[21] and should be supported at FinCEN by enhancing the SAR reporting process to include the fraud perpetrator's account at the receiving institution.

We urge FinCEN to enhance the SAR process to capture the identity of the account and institution that received the fraudulent funds.

C. FinCEN should take additional measures to promote information sharing about payment fraud.

To prevent and detect payment fraud, it is important to aggregate fraud reports from various sources to detect patterns. In the United States, regulatory oversight and supervision of actors in the payments space depends on several factors including the size, type, and nature of a financial institution,[22] as well as the extent to which the activities[23] undertaken by an institution are covered by existing law. As a result, no centralized federal agency receives or collects all data about payment fraud.[24] Additionally, defrauded consumers may report fraud to the Federal Trade Commission, the FBI's internet crimes division, and/or the Consumer Financial Protection Bureau, among other local law enforcement agencies, leading to differing and incomplete snapshots of payment fraud. Although these agencies may share fraud data with each other or the general public, there is no mandate to do so. [25]

Furthermore, financial institutions, payment processors, and payment operators are not required to report the incidents of payment fraud experienced by their customers/consumers to any federal agency. The institutions are required to file a Suspicious Activity Report (SAR) for large transactions in certain circumstances if they suspect their customer is engaged in fraudulent activity, but they are not required to report smaller fraudulent transactions or instances where

[21] Federal Financial Institutions Examination Council, *Bank Secrecy Act/Anti-Money Laundering Examination Manual*, F-2 (2014).
[22] Depending on the size and activity, a financial institution engaging in payment activity could be subject to supervision by the Office of the Comptroller of the Currency, the Federal Reserve Board, the Federal Deposit Insurance Corporation, the National Credit Union Administration, and/or the Consumer Financial Protection Bureau. Otherwise, the institution could be subject to state regulatory supervision under a state bank charter or money transmitter license. Some payment actors may not be subject to any supervision, though they are still required to comply with all laws.
[23] Though not covered by these comments, institutions engaged in payments through cryptocurrency and/or stablecoin face the possibility of oversight by the prudential regulators as well as Commodities Futures Trading Commission, the Securities and Exchange Commission, and/or the Consumer Financial Protection Bureau.
[24] Of any type, including fraud through P2P apps, bank-to-bank transfers, or check fraud.
[25] Though certain fraudulent activity is required to be reported to FinCEN, and the Federal Reserve Board will collect fraud data through FedNow. However, FinCEN does not publicly share the data it collects, and it is unclear how the Federal Reserve Board will utilize and disseminate the data it will collect for FedNow.

their clients have been victimized by fraud.[26] Even with SARs mandatory reporting, the information collected by FinCEN relies heavily on the discretion of a financial institution, and reporting depends on whether the fraud or potential fraud is discovered/flagged by the reporting institution and whether the transaction is large enough to warrant reporting.[27]

Players in the payment industry have recognized the need for fraud information sharing, and some payment operators do collect data about fraud. The Federal Reserve Board collects reports of fraud on FedNow as specified under Regulation J, Subpart C and keeps a "Negative List" of suspicious accounts that is shared with its participants.[28] The Clearing House also collects fraud reports for RTP® (its real time payments platform), and Early Warning Systems (EWS), the owner of Zelle, collects reports of fraud occurring on Zelle, though it is unclear if this information is shared widely among users.[29] Initiatives such as SardineX[30] and Beacon[31] were also launched in response to increased fraud in digital payments and real-time payment systems. However, the information shared is not available to the public and may be industry or payment specific. For example, if a bad actor is flagged in one payment system (i.e. Zelle), that does not mean a financial institution will have that bad actor flagged when allowing a fraudulent wire transfer to be released.[32]

---

[26] "Dollar Amount Thresholds- Banks are required to file a SAR in the following circumstances: insider abuse involving any amount; transactions aggregating $5,000 or more where a suspect can be identified; transactions aggregating $25,000 or more regardless of potential suspects; and transactions aggregating $5,000 or more that involve potential money laundering or violations of the BSA. It is recognized, however, that with respect to instances of possible terrorism, identity theft, and computer intrusions, the dollar thresholds for filing may not always be met. Financial institutions are encouraged to file nonetheless in appropriate situations involving these matters, based on the potential harm that such crimes can produce. Even when the dollar thresholds of the regulations are not met, financial institutions have the discretion to file a SAR and are protected by the safe harbor provided for in the statute." From FDIC *"Connecting the Dots… The Important of Timely and Effective Suspicious Activity Reports"* Supervisory Insights (updated Jul. 10, 2023), available at https://www.fdic.gov/regulations/examinations/supervisory/insights/siwin07/siwinter2007-article03.html#:~:text=Dollar%20Amount%20Thresholds%20%E2%80%93%20Banks%20are,and%20transactions%20aggregating%20%245%2C000%20or.

[27] *See* Mansfield, Cathy, "*It Takes a Thief…. and a Bank: Protecting Consumers From Fraud and Scams on P2P Payment Platforms,"* 57 U. Mich. J.L. Reform (2024).

[28] *See* Operating Circular 8: Funds Transfers through the FedNow Service (Sept. 21, 2022), available at https://www.frbservices.org/binaries/content/assets/crsocms/resources/rules-regulations/operating-circular-8.pdf.

[29] *See Faster Payments Fraud Trends and Mitigation Opportunities*, Faster Payments Council, Fraud Work Group Bulletin.01 at 5 (Jan. 2024), available at https://fasterpaymentscouncil.org/userfiles/2080/files/FPC%20Fraud%20Bulletin_01_01-24-2024_Final.pdf.

[30] *Join sardineX*, Sardine, available at https://go.sardine.ai/sardinex. SardineX is intended as a real-time fraud detection network made up of a consortium of financial institutions and fintech organizations, including banks, card networks, payment processors, and fintechs, which will include a shared database where participants can access fraud data on entities transacting across the network.

[31] Meier, Alain "*Introducing Beacon, the Anti-Fraud Network*," Plaid (Jun. 22, 2023), available at https://plaid.com/blog/introducing-plaid-beacon/. Beacon, launched by Plaid, is intended as an anti-fraud network enabling financial institutions and fintech companies to share critical fraud intelligence via API across Plaid. Members contribute by reporting instances of fraud and can use the network to detect if a specific identify has already been associated with fraud.

[32] Any private database of suspected fraud actors could be considered a "consumer reporting agency" (CRA) under the Fair Credit Reporting Act (FCRA). Early Warning Services already acknowledges it is a CRA. *See* CFPB, List of Consumer Reporting Companies, 2023, at 28 (2023), available at https://files.consumerfinance.gov/f/documents/cfpb_consumer-reporting-companies-list_2023.pdf. As such, these databases would be subject to the file disclosure, accuracy, and dispute resolution rights under the FCRA.

The fragmentation described above prevents a clear and cohesive picture of the payment fraud landscape, actors, and trends, and poses a barrier to forming effective strategies to combat fraud.

As a result, we urge FinCEN to promote greater sharing of fraud information among financial institutions and with regulators, beyond SARs. FinCEN along with Treasury should facilitate a public-private partnership including the relevant Federal and State financial regulators, consumer protection agencies, law enforcement, financial institutions, trade associations, consumer and privacy advocates, and other stakeholders.[33]

II. FinCEN must provide additional clarity and specificity to ensure that financial institutions do not define risk too broadly.

A. Financial institutions should not consider credit risk as a factor in developing an AML/CFT program.

FinCEN is seeking a "risk-based" approach to modernizing the AML regime to ensure "that financial institutions direct more attention and resources toward higher-risk customers and activities, consistent with the risk profile of the financial institution, rather than toward lower-risk customers and activities."[34] But it is unclear how financial institutions would and should identify what customers are considered higher risk and whether that risk analysis would be based solely on factors that may reveal that a person or entity is engaging in potentially illicit activities or whether credit risk would also factor into its risk analysis.[35]

It is a widely held belief that participation in the U.S. financial system often begins with access to a bank account. However, financial institutions have broad discretion in setting risk tolerances for whom they choose to allow as customers. This broad discretion often translates into policies that negatively impact the very consumers who are seeking entrance into the financial system.

As such, we recommend that the statement of purpose defining the goals of an effective, risk-based, and reasonably designed AML/CFT program[36] include the following language:

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

[33] As proposed in the Financial Services and General Government Appropriations Bill, 2024. (S. 2309), Title I. Department of the Treasury, "Financial Fraud" at 10, available at https://www.appropriations.senate.gov/imo/media/doc/fy24_fsgg_report.pdf.
[34] 31 U.S.C. 5318(h)(2)(B). *See also* Question 19 of the proposed rule, 89 FR 55428 (July 3, 2024) at 55447.
[35] See Question 23 of proposed rule, 89 FR 55428 (July 3, 2024) at 55448.
[36] *See* Question 1 of the proposed rule, 89 FR 55428 (July 3, 2024) at 55446-7.

system ***without creating unnecessary barriers for American consumers, especially those from underserved communities, to gain access to the U.S. financial services marketplace***."

As discussed in further detail below, consumers are often unsure why they are denied credit or access to a bank account and whether the denial is related to a financial institution's risk of violating the BSA or because of a risk of financial loss related to underwriting or monetary loss.

Although FinCEN states that the proposed rule is "consistent with the BSA's requirement for the Secretary to consider the extension of financial services to the underbanked and facilitating financial transactions while preventing criminal persons from abusing formal or informal financial services networks,"[37] we believe more clarity and guidance needs to be included in the proposed rule as well as in any implementing guidance and examination manuals to explain that credit risk is not the type of risk a financial institution should consider in developing and implementing its AML/CFT program and to comply with the BSA.

B. Blunt-fisted, opaque identification requirements exclude vulnerable consumers from the U.S. banking system and allow for discrimination.

1. Introduction

Financial institutions do not generally publicize which forms of identification they will accept from consumers when reviewing an application for a demand deposit account. This uncertainty means underserved consumers have no sense of whether they will be successful in opening an account.

Additionally, consumers are not often told why the financial institution denied a request to open a demand deposit account.[38] This generates an impression among consumers that they are not allowed to engage in our banking system because of some intrinsic quality around their situation when it could ultimately be caused by the use of discretion among individual branch employees, a consumer report such as ChexSystems, or a regional or national bank policy. Regardless of the reason, being denied access to financial services can be embarrassing, especially when the denial occurs in person. One negative interaction with our financial system can influence the way a consumer will interact with the system for years to come. The industry's opacity is unjustified given the stakes.

The excuse most often cited by financial institutions for this lack of transparency— and their unwillingness to accept certain alternative forms of ID for underserved consumers— is that they must comply with the BSA. Among other requirements imposed by the BSA, financial institutions must implement a Customer Identification Program (CIP) to verify the identity of an applicant.

[37] 89 FR 55428 (July 3, 2024) at 55432, referencing FN 39.

[38] Because a demand deposit account does not meet the definition of credit under the Equal Credit Opportunity Act, no adverse notice is required to be provided to the applicant/consumer. However, if a financial institution relied on a consumer report from ChexSystems, for example, it should provide the consumer with an adverse action notice under the Fair Credit Reporting Act.

However, federal regulations implementing the BSA permit banks to use a wide range of identification methods to open accounts for their customers and to implement their CIP. At its core, the CIP must explain the bank's procedures for opening an account, including stating what identifying information will be obtained from each customer and how the bank will verify their customers' identities through both documentary and non-documentary methods.[39]

A financial institution has broad discretion in what policies it adopts in its CIP. The only requirements BSA regulations impose are that a financial institution must obtain, at a minimum, the following information from a customer prior to opening an account:

> (1) Name;
> (2) Date of birth, for an individual;
> (3) Address; and
> (4) an Identification number, which must be a taxpayer identification number for "U.S. persons" or one or more of several options for non-U.S. persons, including an Individual Tax Identification Number issued by the IRS, a passport number and country of issuance, an alien identification card number, or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard.[40]

In addition, financial institutions must employ "risk-based procedures" for verifying the identity of each customer to the extent "reasonable and practicable," and within a reasonable time after the account is opened.[41] These procedures must enable the financial institution to form a reasonable belief that it knows the true identity of each customer, and the procedures must be "based on the bank's assessment of the relevant risks, including those presented by the various types of accounts maintained by the bank, the various methods of opening accounts provided by the bank, the various types of identifying information available, and the bank's size, location, and customer base."[42]

It is the requirement to utilize "risk-based" procedures consistent with the bank's level of risk tolerance that gives banks broad discretion in choosing who they bank. The "risk-based" procedures are often utilized as a shield for obfuscating account-opening policies. Without transparency into these policies, banks may ultimately engage in discriminatory practices, utilizing overly simplistic policies that exclude immigrants, domestic violence survivors, justice-involved people, and unhoused individuals who may lack access to various forms of government-issued identification.[43]

More clarity is needed in the guidance FinCEN and federal regulators provide to financial institutions. For example, local advocates in New York City, along with the New York Bankers Association, wrote to the federal financial regulators in 2015, asking if the then-emerging municipal ID for the City of New York would meet the minimum standards for verifying identity

[39] 31 C.F.R. § 1020.220(a)(2)(ii).
[40] 31 C.F.R. § 1020.220(a)(2)(i)(A)(1)-(4).
[41] 31 C.F.R. § 1020.220(a)(2).
[42] 31 C.F.R. § 1020.220(a)(2).
[43] Discussed in greater detail below in Section III.

at account opening.[44] The regulators' response did clarify that accepting the city's ID would not contradict the minimum standards in the regulations. But the regulators left the ultimate decision of whether to accept the municipal ID up to individual banks, writing that each institution "may determine that more information than the ID Card is necessary"[45] to satisfy their duties under this regulatory regime. Since 2015, other cities have implemented their own municipal ID programs, yet banks still have no uniform practice of publicly disclosing which municipal ID programs meet the requirements for their internal protocols, leaving consumers in the dark.

2. Recommendations

In general, FinCEN should consider implementing more detailed guidelines on how banks should exercise their discretion to ensure that they meet the obligations of the Bank Secrecy Act while also not excluding consumers from our banking system. These guidelines should emphasize the importance of transparency in account opening requirements, particularly for underserved consumers who may experience barriers to obtaining traditional forms of ID; provide guidance for local governments on developing municipal ID programs; and explicitly name forms of ID that may be used as primary and secondary ID for individuals unlikely to have access to state-issued ID. Similarly, regulators should specify that there is likely a corresponding risk of unfair, deceptive, or abusive practices associated with discriminating against consumers based on race or national origin and that a denial of a bank account that relies, at least in part, on information obtained within a consumer report triggers adverse action notice requirements under the Fair Credit Reporting Act.[46]

We also recommend that FinCEN, in collaboration with other federal agencies, take specific actions to ensure the financial inclusion of underserved consumers in our consumer financial markets without compromising the purpose of the BSA. To this end, FinCEN should work with and encourage relevant agencies to ensure that overly broad and discriminatory bank policies do not bar access to bank accounts and affordable credit by:

- Reviewing bank customer identification protocols, investigating the reasons behind denials at the deposit account opening stage, and making their findings public whenever possible. Specifically, FinCEN and other agencies should:
    - Ensure that financial institutions can justify that the policies implemented to comply with a risk-based and reasonably designed AML/CFT program are reasonably tailored, evidence-based, and implemented in a manner that is likely to actually reduce risk.
    - Determine whether and how background check reports, other screening or monitoring reports, and algorithms are used to (1) assess and manage credit risk, (2) assess and manage risk of fraud, (3) decide whether to give a prospective customer an account, and (4) determine whether to close an existing customer's account.

[44] Corkery, Michael and Silver-Greenberg, Jessica, "*Banks Reject New York City IDs, Leaving 'Unbanked' on Sidelines, NY Times*," (Dec. 23, 2015), available at https://www.nytimes.com/2015/12/24/business/dealbook/banks-reject-new-york-city-ids-leaving-unbanked-on-sidelines.html?login=smartlock&auth=login-smartlock.
[45] *Id.*
[46] 15 U.S.C. § 1681m(a).

- Clarifying the distinction between unauthorized immigrants living in the United States and non-U.S. persons living abroad in the FFIEC BSA AML/CFT examination manual and warning regulated entities that BSA AML/CFT compliance is not a justification for unlawful discrimination.
- Promulgating guidance clarifying the extent to which municipal IDs and prison IDs may meet the minimum identification requirements set out under the implementing regulations under the BSA and provide guidelines or standards for local governments and correctional facilities to follow when developing their ID programs.
- Encouraging and supporting correctional facilities in helping people obtain official photo identification prior to leaving incarceration.
- Clarifying and encouraging banks and lenders to permit applicants to provide non-traditional addresses, such as addresses of temporary group residences, homeless shelters, domestic violence shelters, and correctional facilities.
- Clarifying that financial institutions may not maintain blanket policies and practices that bar people with any kind of criminal record from having an account. There must be reliable evidence that the specific policy or practice actually assists in preventing fraud and complying with other legal obligations.

C. Overly aggressive BSA/AML programs targeting fraud lead to bank account closures and freezes.

1. Introduction

Recently, many consumers have raised concerns about bank account closures and/or freezes that seem to occur without any sudden change of behavior by the consumer. Consumers report frustration and uncertainty tied to account closures and freezes— primarily the lack of information as to why the closure or freeze occurred and the inability to access funds in a timely manner.

The number of consumers who have complained about checking and savings account closures to the CFPB more than tripled since 2017,[47] and in 2022 the CFPB ordered Wells Fargo to pay $160 million to over one million people for improperly freezing or closing bank accounts from 2011 to 2016 when it "believed that a fraudulent deposit had been made into a consumer deposit account based largely on an automated fraud detection system."[48]

There have been other stories featured by reporters detailing the devastating impact sudden account closures and freezes can have on consumers, especially when they are deprived of access

[47] Consumer Fin. Prot. Bureau, Consumer Complaint Database, *Trends Data for Complaints Received Due to Checking or Savings Account Closure*, (last visited Aug. 27, 2024), available at https://www.consumerfinance.gov/data-research/consumer-complaints/search/?chartType=line&dateInterval=Month&dateRange=All&date_received_max=2024-01-27&date_received_min=2011-12-01&has_narrative=true&issue=Closing%20an%20account%E2%80%A2Company%20closed%20your%20account&lens=Product&product=Checking%20or%20savings%20account&searchField=all&subLens=sub_product&tab=Trends.

[48] *In re. Wells Fargo Bank, N.A.*, CFPB No. 2022-CFPB-0011 (Dec. 20, 2022) (consent order), available at https://files.consumerfinance.gov/f/documents/cfpb_wells-fargo-na-2022_consent-order_2022-12.pdf.

to their funds, are not provided any information about the reason for the institution's actions and are not provided an opportunity to address any perceived risk.

Following are a few examples from a New York Times article detailing the responses consumers received after discovering their accounts were either frozen or closed and their attempts to communicate with their financial institutions about it:[49]

- Naafeh Dhillon, 28 from Brooklyn, NY, learned his account had been closed after his debit card and credit card were declined. He was later told by a Chase representative that the "bank's global security and investigation team had ultimately made the decision. Would the representative transfer him to that department? Nope… Since he wasn't given a specific reason for the closure, he couldn't disprove whatever raised suspicions in the first place."
- Todd Zolecki, 47 of Media, PA, did not have his account closed, but his bank did lock him out of access to his account. "They said your account has been suspended for further review," Why? "We can't tell you that. The only thing we can tell you is it can take up to 60 days for this review."

One of the reasons for the increase in account closures and freezes has to do with the increased adoption of tools utilized by financial institutions to combat payment fraud and detect suspicious activity, including adoption of artificial intelligence (AI) and machine learning technologies. Fraud vigilance is critical, and new technologies can play an important role. However, these tools may harm innocent consumers if not utilized properly and if institutions do not have clear procedures and timelines in place to restore access to funds that are improperly frozen.

Financial institutions have an obligation under the BSA and accompanying anti-money laundering (AML) regulations to ensure that they maintain and follow internal ongoing customer due diligence (CDD) policies. The CDD policies must allow the institution to understand "the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and [c]onducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information."[50]

Because of the CDD obligation and the ongoing problem of payment fraud, sometimes the appropriate response by an institution that suspects its customer is engaging in fraudulent or other illicit activity is to freeze a transaction or close an account that is being used to receive fraudulent funds before the funds are gone and more consumers can be defrauded. But sometimes banks get it wrong, especially when automated tools are used.

According to the Bank Policy Institute, "a sample of the largest banks reviewed approximately 16 million alerts, filed over 640,000 SARs, and received feedback from law enforcement on a median of 4% of those SARs. Ultimately, this means that 90-95% of the individuals that banks

[49] Barnard, Tara Siegel and Lieber, Ron, "*Banks Are Closing Customer Accounts, With Little Explanation*," N.Y. Times (Apr. 8, 2023), available at https://www.nytimes.com/2023/04/08/your-money/bank-account-suspicious-activity.html?unlocked_article_code=1.QU0.szRm.kfoZRQdD7-O6&smid=url-share.
[50] 31 C.F.R. § 1020.210(a)(2)(v);(b)(2)(v).

report on were likely innocent."[51] As these numbers demonstrate, even activity that leads to the filing of a SAR may ultimately not warrant an account freeze or closure. And if a financial institution is utilizing the review of SARs as part of its risk assessment process,[52] then a financial institution needs to consider which of the many SARs it may have filed truly posed a risk to the financial institution and which SARs were more precautionary but not ultimately tied to true risk.

The impact of sudden account closures in response to potential fraud on innocent consumers cannot be overstated. Often, the most vulnerable people have been denied access to their money, rendering them unable to eat or pay rent. Some impact on innocent individuals may be impossible to avoid, as banks may need to act quickly on imperfect information. But that is why it is imperative to have procedures in place to enable people to dispute account freezes and closures and get their money back as soon as possible.

For example, after Chime embarked on a marketing campaign to convince people to open Chime accounts to receive their stimulus payments, its inadequate identity verification led to a wave of fraud. Chime then froze numerous accounts. But instead of enabling people to quickly prove their identities, some people were left without their money for months on end.[53]

Similarly, Bank of America froze 350,000 unemployment debit cards in California after extensive fraud reports. But the freezes caught many legitimately unemployed workers, and the bank failed to respond in a timely fashion to their complaints.[54] Months later, after a lawsuit was filed, a judge prohibited the bank from freezing accounts for California unemployment benefits based solely on an automated fraud filter and required it to do a better job of responding when jobless people say their benefits were stolen.[55] The CFPB also brought enforcement actions against Bank of America[56] and U.S. Bank[57] for similar conduct in indiscriminately freezing accounts and leaving them frozen for long periods of time. This conduct harmed the most vulnerable consumers – those who had lost their jobs and were relying on unemployment benefits.

---

[51] Bank Policy Institute, "*The Truth About Suspicious Activity Reports*," (Sept. 22, 2020), available at https://bpi.com/the-truth-about-suspicious-activity-reports/ (citing, Bank Pol'y Inst., Getting to Effectiveness—Report on U.S. Financial Institution Resources Devoted to BSA/AML & Sanctions Compliance, (Oct. 29, 2018), available at https://bpi.com/wp-content/uploads/2018/10/BPI_AML_Sanctions_Study_vF.pdf).

[52] *See* Question 12 of the proposed rule, 89 FR 55428 (July 3, 2024) at 55447.

[53] Kessler, Carson, "*A Banking App Has Been Suddenly Closing Accounts, Sometimes Not Returning Customers' Money*," ProPublica (Jul. 6, 2021), available at https://www.propublica.org/article/chime.

[54] "*Bank Of America Freezes EDD Accounts Of Nearly 350,000 Unemployed Californians For Suspected Fraud*," KCAL News, (Oct. 29, 2020), available at https://www.cbsnews.com/losangeles/news/bank-of-americafreezes-edd-accounts-of-nearly-350000-unemployed-californians-for-suspected-fraud/.

[55] McGreevy, Patrick, "*Bank of America must provide more proof of fraud before freezing EDD accounts, court orders*," Los Angeles Times (Jun. 1, 2021), available at https://www.latimes.com/california/story/2021-06-01/bankof-america-ordered-to-unfreeze-unemployment-benefit-cards-in-california.

[56] CFPB, "*Federal Regulators Fine Bank of America $225 Million Over Botched Disbursement of State Unemployment Benefits at Height of Pandemic*," (Press Release) (July 14, 2022), available at https://www.consumerfinance.gov/about-us/newsroom/federal-regulators-fine-bank-of-america-225-million-overbotched-disbursement-of-state-unemployment-benefits-at-height-of-pandemic/.

[57] Consumer Fin. Prot. Bureau, "*CFPB Orders U.S. Bank to Pay $21 Million for Illegal Conduct During COVID-19 Pandemic*," (Press Release) (Dec. 19, 2023), available at https://www.consumerfinance.gov/about-us/newsroom/cfpb-orders-us-bankto-pay-21-million-for-illegal-conduct-during-covid-19-pandemic/#:~:text=The%20CFPB%20and%20OCC%20together,411%2DCFPB%20(2372).

Sudden account closures are also common among several communities that we feature in these comments. For instance, immigrants without immigration status and immigrants from specific countries, such as Iran, have reported having their bank accounts closed suddenly after being asked to provide proof of legal residency in the country.[58]

If people cannot access the money they need based on red flags triggered by automated fraud tracking systems, then they need a timely solution, not another obstacle. Yet that is what occurs; consumers face obstacles upon obstacles. When a consumer complains about an account closure or freeze, the complaint is often not followed by a reasonable investigation by the financial institution that includes a discussion with the consumer or that provides any clear timeline to unfreeze their money. Additionally, when the consumers facing these issues have other vulnerabilities discussed later in these comments—such as immigration status or involvement with our justice system—it can have an effect on the ways that entire families and communities interact with our system.

2. Recommendations

As discussed in the previous section, crude BSA/AML compliance policies can shut consumers out of our banking system. FinCEN and bank regulators should investigate the reasons that deposit accounts are closed or frozen and develop a strategy to minimize the number of account closures for innocent consumers.

FinCEN and bank regulators should also provide guidance to financial institutions about what information they may and should provide to accountholders regarding freezes and account closures while still complying with the BSA and the proposed AML/CFT program requirements. For example, they could clarify in an FAQ that, while financial institutions are not allowed to disclose that a SAR was filed, they are allowed to disclose that an account was frozen or closed due to suspicious activity and/or describe the specific activities that raised concerns, allowing the consumer to respond.

FinCEN should also clarify that if a SAR does not lead to criminal prosecution or involvement by law enforcement for suspected money laundering/financing of terrorism activity, then a financial institution should not automatically take derisking measures and close the account based solely on the filing of a SAR but should instead take a measured, case-by-case, risk-based approach.[59]

Finally, FinCEN, along with the CFPB and bank regulators, should provide guidance to financial institutions about the importance of having clear procedures to enable consumers to quickly

[58] *See, e.g.*, Nia v. Bank of America, N.A., 603 F.Supp.3d 894, (S.D. Cal. May 18, 2022) (Denying motion to dismiss); Chouhoud, Youseff, "*Banking While Muslim*," Inst. for Soc. Pol'y and Understanding, 4 (Mar. 14, 2023), available at https://www.ispu.org/banking-while-muslim/ (last visited Aug. 27, 2024) (finding that one third of Muslims reporting challenges with the banking system had their accounts closed or suspended); Wile, Rob, "*He's Been Studying in the U.S. Legally for 7 Years. Bank of America Froze His Account Anyway*," Miami Herald, (Aug. 31, 2018), available at https://www.miamiherald.com/news/business/article217095125.html.

[59] Answering Question 12 of the proposed rule, 89 FR 55428 (July 3, 2024) at 55447, on how a financial institution should use BSA reporting to identify and assess risk.

regain access to their funds when they are frozen due to concerns of suspicious activity, provide guidance as to the timeliness of returning an accountholder's funds after account closure, and specify that failing to have clear procedures and provide timely return of any funds may constitute an Unfair or Abusive business practice.

III. FinCEN should protect specific vulnerable populations that experience financial exclusion often exacerbated by overly broad BSA/AML programs.

The following sections highlight factors that render specific vulnerable groups of consumers susceptible to exclusion from our financial system and limitations that may result in barriers to participating in our mainstream system.[60]

A. Barriers experienced by immigrants

The United States has more immigrants than any other country in the world, with roughly fourteen percent of the U.S. population having been born in another country, totaling 47 million people.[61] The foreign-born experience in the United States varies widely depending on the circumstances that led to their migration— whether they have permanent, temporary, or no status to remain in the country and whether they are proficient in English. Despite their diversity, immigrants from all walks of life often face similar obstacles to fully participating in our financial system.

1. Immigration status as a barrier to banking services

Of the foreign-born population in the U.S., 10.5 million people are considered "unauthorized," which the Department of Homeland Security defines as "all foreign-born non-citizens who are not legal residents."[62] Not all of these individuals are subject to a heightened risk of immediate removal— many have been awarded temporary protection from removal through programs such as Deferred Action for Childhood Arrivals (DACA), Temporary Protected Status (TPS), or pending asylum cases.[63] Individuals who are unauthorized without asylum cases pending or any temporary relief from removal are often among our society's most vulnerable. In addition to

[60] The following sections answer Question 29 of the proposed rule, 89 FR 55428 (July 3, 2024) at 55448. For a more in-depth discussion of the financial barriers encountered by the communities highlighted in these comments and additional recommendations, *see* NCLC's Comments to Treasury's Request for Information on Financial Inclusion available at https://www.nclc.org/resources/comments-on-treasury-departments-request-for-information-on-financial-inclusion/.

[61] Krogstad, Jens Manuel and Passel, Jeffrey, "*What we know about unauthorized immigrants living in the U.S.*," Pew Research Ctr. (Nov. 16, 2023), available at https://www.pewresearch.org/short-reads/2023/11/16/what-we-know-about-unauthorized-immigrants-living-in-the-us/.

[62] *Id. See also* Baker, Bryan, "*Estimates of the Unauthorized Immigrant Population Residing in the United States: January 2015–January 2018*," Dep't. of Homeland Sec., (Jan. 2021), available at https://www.dhs.gov/sites/default/files/publications/immigration-statistics/Pop_Estimate/UnauthImmigrant/unauthorized_immigrant_population_estimates_2015_-_2018.pdf.

[63] *Id.*

facing a near-constant fear of removal, these individuals often experience exploitation and wage theft from their employers[64] and are more likely to live in poverty.[65]

First, immigrants experience barriers in obtaining banking services because of a lack of an identification number. When an individual first moves to the United States, they are unlikely to already have a U.S. government-issued identification number, such as a social security number or an individual tax identification number (ITIN), which is a prerequisite to opening a bank or credit account in the United States.[66] Given current backlogs in our immigration system, it can take weeks for an immigrant or asylum seeker eligible for a SSN to get their social security cards from the Social Security Administration. However, it can take even longer for consumers ineligible for an SSN to receive an ITIN from the Internal Revenue Service, which requires that a W-7 form for a new ITIN be submitted along with a completed U.S. federal income tax return.[67] The IRS also has strict identification requirements to qualify for an ITIN, and requires that applicants either mail their original identification documents (or certified copies of documents from the issuing agency) along with their application or apply for an ITIN in person using an IRS-authorized Certifying Acceptance Agent (CAA).[68] These delays often result in new arrivals and immigrants without status lacking one of the most fundamental prerequisites to opening bank accounts and building credit in our country.

Second, immigrants without status experience barriers to opening bank accounts and building credit, even if they can obtain an ITIN from the IRS, because the system attributes higher risks to noncitizens. In the banking context, immigrants without status are often treated as "non-U.S. persons," which the federal financial regulators list as a "risk factor" associated with money laundering and terrorism financing in the Federal Financial Institutions Examination Council (FFIEC) BSA/AML examination manual.[69] This manual also specifically instructs institutions to consider the forms of identification and the account holder's home country as "risk factors" when determining the risk profile for a "nonresident alien" account.[70] However, this manual does not provide any guidance on the relative risk profiles of nonresidents currently residing in the

---

[64] Felsen, Michael and Smith, Patricia M., "*Wage Theft is a Real National Emergency*," National Employment Law Project, available at https://www.nelp.org/commentary/wage-theft-real-national-emergency/ (last visited Feb 14, 2024).

[65] See, e.g., "*Double Disadvantage: A Profile of Undocumented Women in the United States*," Gender Equity Policy Institute 7, (Jun. 2023), available at https://thegepi.org/wp-content/uploads/2023/06/GEPI-Double-Disadvantage.pdf; Batalova, Jeanne and Fix, Michael, "*Understanding Poverty Declines Among Immigrants and Their Children in The United States*," Migration Policy Institute, (May 2023), available at https://www.migrationpolicy.org/sites/default/files/publications/mpi-poverty-declines-immigrants-2023_final.pdf; ("Immigrants represented 14 percent of the U.S. population in 2021, but they were 24 percent of those experiencing poverty that year"); Migration Policy Institute, "*A Profile of Low-Income Immigrants in the United States*," (Nov. 2022), available at https://www.migrationpolicy.org/sites/default/files/publications/mpi_low-income-immigrants-factsheet_final.pdf.

[66] 31 C.F.R. § 1020.220(a)(2)(i)(A)(1)-(4).

[67] Internal Revenue Service, *How do I apply for an ITIN?*, available at https://www.irs.gov/individuals/how-do-i-apply-for-an-itin (last visited Aug. 27, 2024).

[68] *Id.*

[69] Fed. Fin. Inst. Examination Council, BSA/AML Examination Manual, Risks Associated with Money Laundering and Terrorist Financing, Nonresident Aliens and Foreign Individuals, available at https://bsaaml.ffiec.gov/docs/manual/09_RisksAssociatedWithMoneyLaunderingAndTerroristFinancing/19.pdf (last visited Feb. 14, 2024).

[70] *Id.* at 2.

U.S. without status and with no intent to leave, making no distinction between these individuals and those persons not residing within the U.S. This policy rewards overly aggressive bank policies that exclude immigrants without status, without addressing any corresponding compliance risks associated with discrimination, and may be partly to blame for some of the unnecessary account closures and freezes described above.

Finally, immigrants without status experience barriers to opening a bank account because of problems associated with obtaining a government-issued photo ID. Only sixteen states allow undocumented persons to obtain driver's licenses.[71] These limitations have led to some municipalities offering their own IDs, yet, as discussed above, many financial institutions will only accept municipal IDs as a secondary form of identification in opening a deposit account.[72]

2. Recommendations to address the impacts of overly broad BSA/AML programs on immigrants

FinCEN, in collaboration with other federal agencies, should take action to ensure the financial inclusion of immigrants. FinCEN should work with the relevant agencies to ensure that overly broad and discriminatory bank policies do not bar access to bank accounts and affordable credit by:

- Reviewing bank customer identification protocols, investigating the reasons behind denials at the deposit account opening stage, and making their findings public whenever possible.
- Promulgating guidance clarifying the extent to which municipal IDs may meet the minimum identification requirements set out under the implementing regulations under the BSA and provide guidelines or standards for local governments to follow when developing their municipal ID programs.
- Clarifying the distinction between unauthorized immigrants living in the United States and non-U.S. persons living abroad in the FFIEC BSA/AML examination manual and warn regulated entities that BSA AML/CFT compliance is not a justification for unlawful discrimination.

B. Barriers experienced by survivors of domestic violence

1. Economic abuse and the financial impact of domestic violence

Survivors of domestic violence experience unique barriers to participating in our financial system. Safety comes at a cost. Abusers intentionally isolate survivors, reducing their social network of friends, family, and social systems and access to resources. As a result, a survivor must often choose between returning to an abusive partner for money or incurring debt to access safety. A study on the economic well-being of survivors revealed that 74% of survivors reported

[71] "*United We Dream, Can I Get a Driver's License if I Am Undocumented?*", available at https://unitedwedream.org/how-to-obtain-a-drivers-license-if-youre-undocumented/ (last visited Aug. 27, 2024).
[72] Corkery, Michael and Silver-Greenberg, Jessica, "*Banks Reject New York City IDs, Leaving 'Unbanked' on Sidelines, N.Y. Times*," (Dec. 23, 2015), available at https://www.nytimes.com/2015/12/24/business/dealbook/banks-reject-new-york-city-ids-leaving-unbanked-on-sidelines.html?login=smartlock&auth=login-smartlock.

having to use a credit card to pay for things their family needed because they did not have enough money.[73] The same economic well-being study found that 74% of survivors had to borrow money from a payday lender or car title lender to pay for things their family needed.

In addition to experiencing various types of physical, psychological, and emotional abuse and the financial cost of leaving an abusive relationship, survivors of domestic violence are negatively impacted by the economic abuse they experience. Economic abuse can include acts that deprive a survivor of access to their own financial assets and accounts; acts that prevent a survivor from being able to meet existing financial obligations (like paying bills or going to work or school); and acts that cause a survivor to incur debt. Economic abuse is a tactic often employed by abusers to prevent survivors from leaving an abusive relationship. In fact, 99% of survivors of domestic violence experience economic abuse, and financial concerns are the most cited reasons why a survivor cannot leave an abusive relationship.[74]

Economic abuse has lifelong, lasting effects on survivors. The gravity of its impacts has received federal recognition warranting codification of the term economic abuse in the Violence Against Women Act Reauthorization of 2022. Economic abuse, in the context of domestic violence, dating violence, and abuse in later life, means behavior that is coercive, deceptive, or unreasonably controls or restrains a person's ability to acquire, use, or maintain economic resources to which they are entitled, including using coercion, fraud, or manipulation to:

- Restrict a person's access to money, assets, credit, or financial information;
- Unfairly use a person's personal economic resources, including money, assets, and credit, for one's own advantage; or
- Exert undue influence over a person's financial and economic behavior or decisions, including forcing default on joint or other financial obligations, exploiting powers of attorney, guardianship, or conservatorship, or failing or neglecting to act in the best interests of a person to whom one has a fiduciary duty.[75]

This pervasive and sweeping form of abuse and dominance presents itself in many ways, including preventing a survivor from accessing bank accounts and financial resources, spending down previously held assets, and employment sabotage, all of which create economic dependence on the abusive partner.

Economic abuse occurs in an environment of coercive control, which is a dense net of behaviors a person puts into place to control another. Coercive control can include isolating the survivor from friends and family, establishing rules for the survivor's behavior, and limiting the survivor's access to transportation, education, and employment. These behaviors do not stand alone – they exist within an environment of intimidation, a history of past violence, and the threat of future violence or other harm if the survivor does not comply. Economic abuse is not limited to a discrete incident; rather, economic abuse consists of a series of acts that compound

[73] Center for Survivor Agency and Justice, "*Domestic Violence and Economic Well-being Study*," available at https://csaj.org/resource/domestic-violence-and-economic-well-being-study/ (last visited Feb. 16, 2024).
[74] National Coalition Against Domestic Violence, "*Quick Guide: Economic and Financial Abuse*," (Apr. 12, 2017), available at https://ncadv.org/blog/posts/quick-guide-economic-and-financial-abuse.
[75] 34 U.S.C.A. § 12291(a)(13).

and result in an "economic ripple effect" that creates economic barriers to safety across a survivor's lifetime.[76]

When a survivor has been subjected to economic abuse, it is far more likely that they will have damaged credit, reduced income, and a potentially negative rental history. As a result, survivors of economic abuse are highly likely to experience credit, housing, and employment denials or obtain less favorable credit, housing, and employment options.

2. Barriers faced by survivors at account opening

The intimate nature of domestic violence means that abusive partners often have access to a survivor's personal identifying information (PII), such as a Social Security number, date of birth, employer, income data, and address history, all of which allow an abuser to obtain credit and open accounts without the survivor's knowledge or consent. The National Domestic Violence Hotline, a non-profit serving the needs of domestic violence victims, shared that 22% of female callers reported that their partners created debt in their name via a fraudulent transaction.

When an abusive partner opens an account in the survivor's name, the abuser can create a fraudulent credit profile with an address, phone number, email, employment history, or income data that do not actually belong to the survivor. Furthermore, the abuser can set up PINs, passwords, security questions, and responses to the fraudulent account that ensure complete and sole control and access to the account. Though a survivor may have various legal remedies available in this context, they often cannot access the fraudulent account as they are unable to provide correct security information.

Without access to the account, a survivor is unable to stop the abusive partner from continuing to accrue debt in their name and is unable to close the account completely. One advocate recalls the hours she spent on the phone with a survivor trying to dispute a fraudulent credit card account with Citibank. The survivor did not know the password to the account her abuser created to access the account online, and she did not know the PIN her abuser created, all of which prevented her from being able to speak to a representative on the phone. The survivor could not take any action on the account quickly but instead had to send a dispute letter to the billing error address, which she could not have done without the help of a lawyer. This same survivor only learned of the Citibank account, as well as various other fraudulent credit accounts totaling $60,000, when in the middle of a divorce proceeding. It took the survivor over three years, and the help of a lawyer, to finally remove all the information on her credit report linked to her abusive spouse and the fraudulent accounts.

Even though the survivors are the victims of fraud, financial institutions may often hold the survivor as complicit in the fraud and refuse to continue to extend credit or bank the survivor. As a result, a survivor is unfairly categorized as a risk to the financial institution.

[76] Sara J. Shoener & Erika A. Sussman, "*Economic Ripple Effect of IPV: Building Partnerships for Systemic Change,"* Domestic Violence Report, available at https://csaj.org/wp-content/uploads/2021/10/Economic-Ripple-Effect-of-IPV-Building-Partnerships-for-Systemic-Change.pdf.

Furthermore, survivors of domestic violence often encounter additional difficulties with opening a new account – whether it is a credit account or a bank account. Survivors may not have sufficient documentation to prove identity or residential address. A survivor may have fled from their previous residence in a rush, without the various forms of identification required to open their own bank accounts. On some occasions, abusive partners may also retain the survivor's identification as a method to continue to exert control over the survivor. Some survivors separating from an abusive partner may need to live in transitional housing, such as a domestic violence shelter, and thus lack a permanent address. By failing to address these barriers, our banking and credit systems make it that much harder for domestic violence survivors to separate from the abuser.

3. Recommendations to address the impacts of overly broad BSA/AML programs on survivors

In addition to the many recommendations previously mentioned, we suggest specific actions to enable domestic violence survivors to fully participate in our financial system.

FinCEN should encourage financial institutions to develop policies to assist survivors of domestic violence at account opening. For example, FinCEN, alongside financial regulators, could:

- Issue guidance clarifying that financial institutions may accept non-traditional forms of identification.
- Issue guidance clarifying and encouraging banks and lenders to permit applicants to provide non-traditional addresses, such as addresses of temporary group residences, domestic violence shelters, and homeless shelters.[77]

C. Barriers experienced by justice-involved individuals

1. The financial impact of involvement with the justice system

Justice-involved people are often locked out of the mainstream consumer financial marketplace for various interconnected reasons. Being locked out of the mainstream can, in turn, prolong justice involvement – for example, if a person recently released from prison cannot get credit to buy or lease a car, they may not be able to meet their release requirements – with ripple effects on families and communities.[78]

The population of justice-involved people in the United States is vast. As of March 2023, nearly 2 million people were incarcerated in this country, including over one million in state prisons,

[77] Institutions could consider providing a six-month grace period in obtaining address verification if a domestic violence survivor has provided a letter from a domestic violence shelter or transitional living center confirming that the survivor has resided there or adopting a policy accepting the address of the shelter.

[78] *See, e.g.*, Consumer Fin. Prot. Bureau, Justice-Involved Individuals and the Consumer Financial Marketplace 35–36 (Jan. 2022), available at https://files.consumerfinance.gov/f/documents/cfpb_jic_report_2022-01.pdf [hereinafter CFPB, Justice-Involved Individuals Report] (explaining how lack of access to affordable credit can perpetuate justice involvement and prevent people from participating in the consumer financial marketplace).

over 500,000 in local jails, and over 200,000 in federal prisons and jails.[79] One in three adults—about 77 million people—has a criminal record.[80] Nearly half of children in the United States have at least one parent with a record.[81]

Black, Latino, and Native people are massively overrepresented in the criminal legal system. For instance, Black Americans are twice as likely to be arrested as white Americans,[82] and are more likely to be stopped by the police, detained, charged with more serious crimes, and sentenced more harshly than white American.[83] As the U.S. Department of Housing and Urban Development has stated, these racial and ethnic disparities are "well established and persistent"; they "cannot be simply attributed to certain groups committing more crimes and are better explained by biases" in the criminal legal system."[84]

People with disabilities and members of the LGBTQ+ community are also disproportionately represented in the criminal legal system. According to the U.S. Commission on Civil Rights, "[i]ncarcerated people are twice as likely to have an intellectual disability, four to six times more likely to have a cognitive disability, twice as likely to have a mobility disorder, three to four times more likely to be blind or have a vision impairment, and two to three times more likely to

[79] Sawyer, Wendy and Wagner, Peter, Prison Pol'y Initiative, "*Mass Incarceration: The Whole Pie 2023*," (2023) available at https://www.prisonpolicy.org/reports/pie2023.html (the remaining fraction are held in juvenile correctional facilities, immigration detention facilities, Indian country jails, military prisons, civil commitment centers, state psychiatric hospitals, and prisons in the U.S. territories).

[80] CFPB, Justice-Involved Individuals Report, at 4 (citing National Conference of State Legislatures, Criminal Records and Reentry (May 5, 2020), available at ncsl.org/research/civiland-criminal-justice/criminal-records-and-reentry.aspx).

[81] Avery, Beth, Nat'l Employment Law Proj., "*Fact Sheet: Research Supports Fair Chance Policies,"* (Jan. 16, 2024), available at https://www.nelp.org/publication/research-supports-fair-chance-policies/ [hereinafter NELP, Fact Sheet].

[82] Waddell, Kaveh, "*How Tenant Screening Reports Make It Hard for People to Bounce Back from Tough Times*," Consumer Reports (Mar. 11, 2021), available at https://www.consumerreports.org/electronics/algorithmic-bias/tenant-screening-reports-make-it-hard-to-bounce-back-from-tough-times-a2331058426/; Avery, Beth, et al., Nat'l Employment Law Proj. "*Fair Chance Licensing Reform: Opening Pathways for People with Records to Join Licensed Professions*," 18, (2018), available at https://www.nelp.org/publication/fair-chance-licensing-reform-opening-pathways-for-people-with-records-to-join-licensed-professions/.

[83] Hinton, Elizabeth, et al., Vera Inst. of Just., "*An Unjust Burden: The Disparate Treatment of Black Americans in the Criminal Justice System,"* 1, 7–10 (2018), available at https://www.vera.org/downloads/publications/for-the-record-unjust-burden-racial-disparities.pdf.

[84] Memorandum from Principal Deputy Assistant Sec'y for Fair Hous. and Equal Opportunity, U.S. Dep't of Housing and Urban Dev., to Office of Fair Hous. & Equal Opportunity, Fair Hous. Assistance Program Agencies, Fair Hous. Initiatives Program Grantees, at 3 (June 10, 2022), available at https://www.hud.gov/sites/dfiles/FHEO/documents/Implementation%20of%20OGC%20Guidance%20on%20Application%20of%20FHA%20Standards%20to%20the%20Use%20of%20Criminal%20Records%20-%20June%2010%202022.pdf; *see also* U.S. Equal Emp. Opportunity Comm'n, Enforcement Guidance on the Consideration of Arrest and Conviction Records in Employment Decisions under Title VII of the Civil Rights Act; NELP, Fact Sheet.

have a hearing impairment than the general population."[85] The incarceration rate of LGBTQ+ individuals is more than three times that of the U.S. adult population.[86]

Poverty is both a predictor and result of justice involvement.[87] The median income among people *entering* prison is 41 percent less than the national average,[88] and people have virtually no ability to earn meaningful wages while they are incarcerated.[89] People *leaving* incarceration are even worse off financially, including because they often lose out on careers-long earning potential while they are incarcerated.[90] People with any kind of criminal record also often struggle to find gainful employment and housing because of bias and policies against justice-involved individuals and issues stemming from inaccurate or misleading background checks.[91] Barriers to housing and employment often result in high rates of homelessness among the formerly incarcerated.[92]

Justice-involved individuals also frequently accrue court debt in the form of fines, fees, and restitution that are imposed in the criminal legal system, often without any assessment of their ability to pay.[93] Because justice-involved people and their families are disproportionately poor,

[85] U.S. Comm'n on Civ. Rts., Collateral Consequences: The Crossroads of Punishment, Redemption, and the Effects on Communities 21 (2019), available at https://www.usccr.gov/files/pubs/2019/06-13-Collateral-Consequences.pdf.
[86] *Id.* at 21; *see also id.* at 22 ("Although 4.1 percent of American adults identify as LGBT, 9.3 percent of male prisoners and 42.1 percent of female prisoners identified as LGBT or reported having same-sex encounters before incarceration. . . . Twenty-one percent of transgender women and 10 percent of transgender men report that they have spent time in jail or prison.").
[87] *See, e.g.*, Hayes, Tara O'Neill and Barnhorst, Margaret, Am. Action Forum, "*Incarceration and Poverty in the United States*," available at https://www.americanactionforum.org/research/incarceration-and-poverty-in-the-united-states/#ixzz8RjexiLfH ("While it is difficult to ascertain whether poverty makes someone more likely to commit a crime, data show it does make a person more susceptible to being arrested and more likely to be charged with a harsher crime and to receive a longer sentence. Adults in poverty are three times more likely to be arrested than those who aren't, and people earning less than 150 percent of the federal poverty level are 15 times more likely to be charged with a felony—which, by definition, carries a longer sentence—than people earning above that threshold."); Day, Eli, "*The Race Gap in US Prisons Is Glaring, and Poverty is Making It Worse*," Mother Jones (Feb. 2, 2018); NELP, Fact Sheet (discussing how the carceral system worsens poverty).
[88] Kopf, Daniel and Rabuy, Bernadette, Prison Pol'y Initiative, "*Prisons of Poverty: Uncovering the Pre-Incarceration Incomes of the Imprisoned*," (2015), available at https://www.prisonpolicy.org/reports/income.html ("We found that, in 2014 dollars, incarcerated people had a median annual income of $19,185 prior to their incarceration, which is 41% less than nonincarcerated people of similar ages.").
[89] Sawyer, Wendy, "*How Much Do Incarcerated People Earn in Each State?*," Prison Pol'y Initiative (Apr. 10, 2017), available at https://www.prisonpolicy.org/blog/2017/04/10/wages/. (showing average hourly wages of 14¢ to 63¢ for typical prison jobs).
[90] *See, e.g.*, Craigie, Terry-Ann, et al., Brennan Ctr. for Just., "*Conviction, Imprisonment, and Lost Earnings: How Involvement with the Criminal Justice System Deepens Inequality*," 6 (2020), available at https://www.brennancenter.org/our-work/research-reports/conviction-imprisonment-and-lost-earnings-how-involvement-criminal?ref=honeysucklemag.com (finding that "[o]n average, formerly imprisoned people earn nearly half a million dollars less over their careers than they might have otherwise," that "[t]hese losses are borne disproportionately by people already living in poverty," and that "they help perpetuate it").
[91] NELP, Fact Sheet.
[92] Couloute, Lucius, Prison Pol'y Initiative, "*Nowhere to Go: Homelessness among formerly incarcerated people*," (2018), available at https://www.prisonpolicy.org/reports/housing.html.
[93] CFPB, Justice Involved Individuals Report, at 37–38.

many are not able to afford repayment and their debts become past due,[94] perpetuating cycles of extraction and poverty and prolonging justice involvement.

2. Limited access to banking and credit products

Upon leaving custody, justice-involved people struggle to access checking and savings accounts due to various account opening requirements.[95] First, banks typically require photo identification to open a bank account, as discussed above. A person may have had their driver's license suspended because of outstanding criminal justice debt that they cannot afford to pay[96] or had their ID expire or get lost while incarcerated, meaning they cannot satisfy this requirement.

Second, people must demonstrate proof of address both to renew a license and to open a bank account.[97] Justice-involved people may struggle to meet this requirement if they are currently incarcerated, living in a halfway house or other temporary group residence, or are unhoused.

Third, banks may deny justice-involved people accounts based on credit checks.[98] For example, banks generally request reports on potential customers from companies such as Early Warning Systems and ChexSystems that include information on accounts closed by banks because of unpaid fees or suspected fraud.[99] People leaving incarceration may face these issues, including because managing accounts while in prison or jail can be very difficult. People also report having been victims of identity theft or "identity sharing" gone wrong while incarcerated.[100]

Fourth, some accounts come with conditions to maintain an account – opening deposits, minimum balances, or monthly fees. Justice-involved individuals, including those who recently left incarceration, likely have limited financial resources as described above, and will struggle to meet these requirements.[101]

Justice-involved people also struggle to access mainstream consumer credit. Justice-involved people are more likely than people without justice involvement to have "poor" or "very poor" credit scores.[102] Even when justice-involved people do manage to obtain credit, such as in the form of a credit card, that may not be the end of the story. Some lenders conduct background

---

[94] *Id.* at 39; *see also* Report from the President's Council of Economic Advisors on Fines, Fees, and Bail (2015), available at https://obamawhitehouse.archives.gov/sites/default/files/page/files/1215_cea_fine_fee_bail_issue_brief.pdf.
[95] *Id.* at 27, 29.
[96] Currently, half of all U.S. states still suspend, revoke or refuse to renew driver's licenses for unpaid traffic, toll, misdemeanor and felony fines and fees. Fines & Fees Justice Center, "*Free to Drive: National Campaign to End Debt-Based License Restrictions*," available at https://finesandfeesjusticecenter.org/campaigns/national-drivers-license-suspension-campaign-free-to-drive/ (last visited Aug. 27, 2024).
[97] *Id.* at 29.
[98] *Id.*
[99] *Id.*
[100] Harper, Annie, et al., "Let Me Be Bill-free": Consumer Debt in the Shadow of Incarceration, 63 *Sociological Perspectives* 992 (2020); CFPB, Justice-Involved Individuals Report, at 26.
[101] CFPB, Justice-Involved Individuals Report, at 29.
[102] Watson, Spencer, First Step Alliance, "*Economic Wellbeing of U.S. Adults with Experiences with Incarceration and Unpaid Legal Costs*," available at https://www.firststepalliance.org/post/first-step-alliance-report-economic-health-of-justice-involved-individuals (last visited Aug. 27, 2024).

checks on applicants and on existing customers.[103] These background checks may result in a decrease in the availability of or an increase in the cost of consumer credit for people with criminal records.[104] They may also result in the closure of existing customers' credit cards—without explanation from the lender or information about the entity that conducted the background check or what the background check includes.[105] As the CFPB has flagged, given the racial disparities in arrests and convictions, such practices may raise fair lending concerns.[106] These practices may also violate the adverse action notice requirements of the FCRA and ECOA, as well as the FCRA provision providing that a consumer reporting agency may not prohibit a user of a report from disclosing the content of the report to the consumer if an adverse action has been taken.[107]

3. Recommendations to address the impacts of overly broad BSA/AML programs on justice-involved individuals

FinCEN, in collaboration with other federal agencies and state correctional institutions, should take action to ensure that justice-involved individuals are not hurt by overly broad BSA AML/CFT programs by:

- Ensuring that overly broad, discriminatory criminal records policies do not bar access to bank accounts and affordable credit. To do so, FinCEN should collaborate with the CFPB and other relevant agencies:
  - To investigate both bank account and credit account closures based on criminal records and make their findings public whenever possible.
    - The agencies should determine whether and how background check reports, other screening or monitoring reports, and algorithms are used to (1) assess and manage credit risk, (2) assess and manage the risk of fraud,

[103] *Id.*; *see also* Lieber, Ron and Siegel Bernard, Tara, "*Why Banks Are Suddenly Closing Down Customer Accounts*," NY Times (Nov. 5, 2023), available at https://www.nytimes.com/2023/11/05/business/banks-accounts-close-suddenly.html.
[104] CFPB, Justice-involved Individuals, at 35.
[105] *Id.* (one formerly incarcerated person submitted a complaint to the CFPB explaining that an issuer closed their credit card upon learning of their criminal history). Sometimes the account closure is the result of an *erroneous* background check, where someone else's criminal record is attributed to the card holder. *See, e.g.*, Complaint, *Carr v. Regulatory Datacorp, Inc.*, No. 2:22-cv-02139 (E.D. Pa. Oct. 14, 2022).
[106] CFPB, Justice-involved Individuals, at 35. *See also* Third Amended Complaint for Declaratory Relief and Damages; Public Injunctive Relief, Martinez v. Citibank, N.A., No. 23AHCV00759 (Cal. Super. July 3, 2024) (alleging Citibank has a policy and practice of denying credit to individuals with criminal convictions regardless of circumstances, which has a disparate impact on racial and ethnic minorities; alleging violations of the Equal Credit Opportunity Act and California law on the basis that).
[107] *See e.g.*, Third Amended Complaint for Declaratory Relief and Damages; Public Injunctive Relief, Martinez v. Citibank, N.A. 6–7, No. 23AHCV00759 (Cal. Super. July 3, 2024) (Citibank failed to provide plaintiff with adverse action notice and refused to disclose its use of Refinitiv or the World-Check databases to obtain information about plaintiff used in connection with cancellation of credit cards); Memorandum of Law in Support of Plaintiff's Motion for Class Certification Carr v. Regulatory Datacorp, Inc. 4,–5, 26, No. 2:22-cv—2139-MRP (E.D. Pa. Apr. 18, 2024), ECF No. 72-1 (based on the report defendants supplied, Capital One took adverse action against plaintiff by closing his account, but pursuant to the contract between defendants and Capital One, Capital One was prohibited from providing any information to Plaintiff about the report, including its contents or its existence, in violation of 15 U.S.C. § 1681e(c)).

(3) decide whether to give a prospective client an account, and (4) determine whether to close an existing client's account.

- Issue guidance clarifying that financial institutions may not maintain blanket policies and practices that bar people with any kind of criminal record from having an account. There must be reliable evidence that the specific policy or practice actually assists in preventing fraud and complying with other legal obligations.

- ∉ Collaborating with relevant partner agencies to issue guidance clarifying that financial institutions may accept non-traditional forms of identification, such as prison IDs.
- ∉ Encouraging and supporting correctional facilities in helping people obtain official picture identification before leaving incarceration.
- ∉ Issuing guidance clarifying and encouraging banks and lenders to permit applicants to provide non-traditional addresses, such as addresses of temporary group residences, homeless shelters, and correctional facilities.[108]

IV. FinCEN should be extremely cautious and vigilant about the use of AI in AML/CFT programs and BSA compliance.

In its proposed rule, FinCEN seeks feedback regarding the use of innovative approaches and the use of emerging technologies, such as machine learning or artificial intelligence.[109] FinCEN also states that although "one of the AML Act's purposes is to 'encourage technological innovation and the adoption of new technology by financial institutions to more effectively counter money laundering and the financing of terrorism',"[110] it "recognizes that automated transaction monitoring systems have the potential to generate a significant number of alerts that are not necessarily indicative of suspicious activity."[111]

We agree that it is of great importance for all parties who engage in payments (financial institutions, payment processors, card networks, money service businesses, and fintech companies) to utilize tools to combat payment fraud, including AI and machine learning technologies. However, without proper supervision and consumer protections in place, these tools may harm innocent consumers.[112]

Furthermore, concerns about the use of AI and machine learning tools arise regarding the lack of transparency and explainability of the more complicated models, the unrestrained surveillance and collection of consumer data, and the potential for bias and discrimination. The speed and

---

[108] As discussed at Treasury's Re-Entry Financial Resilience Discussion: Addressing Barriers in Financial Services for Justice-Impacted Communities on January 12, 2024, some credit unions, such as Stepping Stones Federal Credit Union already serve incarcerated people. Brock Fritz, 'Everything we do is to better the community,' Credit Union National Association (Jan. 10, 2024), available at https://news.cuna.org/articles/123443-everything-we-do-is-to-better-the-community.

[109] *See* Questions 27 and 40 of the proposed rule, 89 FR 55428 (July 3, 2024) at 55448 and 55449, respectively.

[110] 89 FR 55428 (July 3, 2024) at 55434, referencing FN 60.

[111] 89 FR 55428 (July 3, 2024) at 55434, referencing FN 61.

[112] For a more in depth discussion of our concerns regarding the use of AI, *see* NCLC's Comments in response to the U.S. Department of Treasury's (Treasury) Request for Information on Uses, Opportunities, and Risks of Artificial intelligence in the Financial Services Sector, available at https://www.nclc.org/wp-content/uploads/2024/08/Treasury-RFI-on-AI-August-2024.pdf. Section III of the comments specifically focuses on the use of AI and automated tools to open and monitor bank accounts for fraud risks.

power of this technology, and its wide-scale adoption with little regulatory oversight, puts consumers at systemic risk of harm. AI and machine learning systems used for BSA compliance and risk assessment have the capacity to make decisions about who obtains credit, housing, banking, insurance, and financial services. These are high-risk systems that should receive the highest level of regulatory scrutiny.

FinCEN and Treasury, along with other federal agencies and regulators, should develop a regulatory framework that requires robust evaluation of AI and machine learning systems used by financial institutions at every stage of development and deployment to determine whether AI systems are safe and effective. The framework should pursue a rights-based approach that protects consumers from harm and preserves their rights. This framework should look at the potential harm to consumers rather than seeking only to mitigate the risk the AI or machine learning technology poses to financial institutions. This approach is consistent with the White House's blueprint for the AI Bill of Rights and is the basis for a robust regulatory scheme that protects consumers.[113] An approach that prioritizes the risks to financial institutions can result in an unacceptable infringement of civil rights, constitutional rights, privacy rights, and statutory consumer protections.

V. Conclusion

We recognize that developing a rule for anti-money laundering and countering the financing of terrorism programs is an arduous undertaking that requires some flexibility. We also recognize that a strong rule will help prevent and address fraud that impacts millions of consumers. However, more clarity and guidance are needed to ensure that these efforts do not harm consumers' access to financial services—especially consumers belonging to certain vulnerable populations— or give financial institutions the ability to use compliance with the BSA as a shield or an excuse for denying access to these consumers. As a result, we urge FinCEN to keep underserved populations top of mind when developing guidance, policies, and examination requirements.

In summary, FinCEN should address fraud by:

- Expanding the Customer Identification Program (CIP) and customer due diligence (CDD) requirements for entities other than banks that engage in payment and banking services, such as person-to person (P2P) payment apps, payment processors, fintech companies offering banking as a service or offering bank-like services, and crypto-related entities including crypto exchange platforms.
- Enhancing the SAR process to capture the identity of the account and institution that receives fraudulent funds.
- Promoting greater sharing of fraud information among financial institutions and with regulators, beyond SARs.
    - FinCEN along with Treasury should facilitate a public-private partnership including the relevant Federal and State financial regulators, consumer protection agencies, law enforcement, financial institutions, trade associations, consumer and privacy advocates, and other stakeholders.

[113] White House, Blueprint for an AI Bill of Rights, available at https://www.whitehouse.gov/ostp/ai-bill-of-rights/.

In addition, FinCEN should provide greater clarity and specificity to ensure that financial institutions do not define risk too broadly by:

- Ensuring that financial institutions do not consider credit risk as a factor in developing an AML/CFT program.
- Reviewing bank customer identification protocols, investigating the reasons behind denials at the deposit account opening stage, and making their findings public whenever possible. Specifically, FinCEN and other relevant regulatory agencies should:
    - Ensure that financial institutions can justify that the policies implemented to comply with a risk-based and reasonably designed AML/CFT program are reasonably tailored, evidence-based, and implemented in a manner that is likely to actually reduce risk.
    - Determine whether and how background check reports, other screening or monitoring reports, and algorithms are used to (1) assess and manage credit risk, (2) assess and manage risk of fraud, (3) decide whether to give a prospective customer an account, and (4) determine whether to close an existing customer's account.
- Clarifying the distinction between unauthorized immigrants living in the United States and non-U.S. persons living abroad in the FFIEC BSA AML/CFT examination manual and warning regulated entities that BSA AML/CFT compliance is not a justification for unlawful discrimination.
- Promulgating guidance clarifying the extent to which municipal IDs and prison IDs may meet the minimum identification requirements set out by the BSA regulations and provide guidelines or standards for local governments and correctional facilities to follow when developing their ID programs.
- Encouraging and supporting correctional facilities in helping people obtain official photo identification prior to leaving incarceration.
- Clarifying and encouraging banks and lenders to permit applicants to provide non-traditional addresses, such as addresses of temporary group residences, homeless shelters, domestic violence shelters, and correctional facilities.
- Clarifying that financial institutions may not maintain blanket policies and practices that bar people with any kind of criminal record from having an account. There must be reliable evidence that the specific policy or practice actually assists in preventing fraud and complying with other legal obligations.
- Ensuring that overly aggressive BSA/AML programs targeting fraud do not lead to bank account closures and freezes. Specifically, FinCEN, along with the CFPB and bank regulators, should:
    - investigate the reasons that deposit accounts are closed or frozen and develop a strategy to minimize the number of account closures for innocent consumers;
    - provide guidance to financial institutions about what information they may and should provide to accountholders regarding freezes and account closures while still complying with the BSA and the proposed AML/CFT program requirements.
    - clarify that if a SAR does not lead to criminal prosecution or involvement by law enforcement for suspected money laundering/financing of terrorism activity, then a financial institution should not automatically take derisking measures and close the account based solely on the filing of a SAR but should instead take a measured, case-by-case, risk-based approach.

- provide guidance to financial institutions about the importance of having clear procedures to enable consumers to quickly regain access to their funds when they are frozen due to concerns of suspicious activity; the timeliness of returning an accountholder's funds after account closure; and specify that failing to have clear procedures and timely return of any funds may constitute an Unfair or Abusive business practice.

FinCEN should also protect specific vulnerable populations that experience financial exclusion often exacerbated by overly broad BSA/AML programs. FinCEN, in collaboration with other federal agencies, should:

- Take action to ensure the financial inclusion of immigrants by:
  - Reviewing bank customer identification protocols, investigating the reasons behind denials at the deposit account opening stage, and making their findings public whenever possible.
  - Promulgating guidance clarifying the extent to which municipal IDs may meet the minimum identification requirements set out under the BSA regulations, and provide guidelines or standards for local governments to follow when developing their municipal ID programs.
  - Clarifying the distinction between unauthorized immigrants living in the United States and non-U.S. persons living abroad in the FFIEC BSA/AML examination manual and warn regulated entities that BSA AML/CFT compliance is not a justification for unlawful discrimination.
- Take action to assist survivors of domestic violence at account opening by issuing guidance:
  - Clarifying that financial institutions may accept non-traditional forms of identification.
  - Clarifying and encouraging banks and lenders to permit applicants to provide non-traditional addresses, such as addresses of temporary group residences, domestic violence shelters, and homeless shelters.
- Take action to ensure that justice-involved individuals are not hurt by overly broad BSA AML/CFT programs by:
  - Investigating both bank account and credit account closures based on criminal records and making the findings public whenever possible.
  - Issuing guidance clarifying that financial institutions may not maintain blanket policies and practices that bar people with any kind of criminal record from having an account.
  - Issuing guidance clarifying that financial institutions may accept non-traditional forms of identification, such as prison IDs.
  - Encouraging and supporting correctional facilities in helping people obtain official photo identification before leaving incarceration.
  - Issuing guidance clarifying and encouraging banks and lenders to permit applicants to provide non-traditional addresses, such as addresses of temporary group residences, homeless shelters, and correctional facilities.

Finally, FinCEN should be extremely cautious and vigilant about the use of AI in AML/CFT programs and BSA compliance. FinCEN and Treasury, along with other federal agencies and regulators, should:

- Develop a regulatory framework that requires robust evaluation of AI and machine learning systems used by financial institutions at every stage of development and deployment to determine whether AI systems are safe and effective. The framework should look at the potential harm to consumers rather than seeking only to mitigate the risk the AI or machine learning technology poses to financial institutions.

We appreciate FinCEN's willingness to undertake this effort and are happy to answer questions. If you have any questions, please contact Carla Sanchez-Adams at csanchezadams@nclc.org.

Respectfully submitted,

National Consumer Law Center, on behalf of its low-income clients