Davis Polk

FinCEN releases final rule on access to beneficial ownership information

December 28, 2023 | Client Update | 14-minute read

FinCEN released its long-awaited final rule governing access to the national database of beneficial ownership information. The final rule addresses some of the most significant concerns that commenters raised with the proposed rule, including its limitations on the use of information in the database for anti-money laundering compliance purposes.

On December 22, 2023, the Financial Crimes Enforcement Network (FinCEN) published a final rule that establishes the standards for financial institutions and government entities to access beneficial ownership information (BOI) reported to FinCEN (the Access Rule). The Access Rule is the second of three rulemakings implementing the Corporate Transparency Act (CTA), a statute designed to increase transparency in the ownership of corporate entities. The Access Rule follows the Beneficial Ownership Information Reporting Requirements Rule (the BOI Reporting Rule), which will become effective on January 1, 2024, and requires non-exempt corporations, limited liability companies and other similar entities (collectively, reporting companies) to report identifying information about themselves, their beneficial owners, and the company applicants who form or register them.[1] BOI reported to FinCEN will be housed in a national database that FinCEN expects to go live on January 1, 2024 (the BO IT System). The Access Rule prescribes the circumstances under which BOI may be disclosed to authorized recipients through the BO IT System, the purposes for which BOI may be used, and the standards for safeguarding BOI. The third and final CTA rulemaking will make conforming amendments to the beneficial ownership requirements of FinCEN's existing Customer Due Diligence (CDD) Rule.[2]

In response to public comment, FinCEN made a number of significant revisions to the Access Rule relative to the notice of proposed rulemaking released in December 2022 (the Proposed Rule).[3] Many commenters – including industry groups and members of Congress – were critical of the Proposed Rule for imposing what they viewed as unnecessary and unreasonable restrictions on financial institutions' use of BOI for anti-money laundering and countering the financing of terrorism (AML/CFT) compliance purposes. The Access Rule addresses some of the key concerns raised by commenters by, among other things, broadening the purposes for which BOI may be used and permitting BOI to be shared with non-U.S. employees, agents, and contractors in most jurisdictions. Although FinCEN acknowledged that other questions remain regarding the implementation of the CTA (and its implications for the compliance expectations for financial institutions), the agency committed to addressing further questions through its impending CDD Rule rulemaking, as well as further guidance specific to the Access Rule.

Importantly, FinCEN is taking a phased approach to providing access to the BO IT System, beginning with a pilot program in 2024 that will extend access to a handful of key federal agency users. Financial institutions and their regulators will be the last category of users that will have access to the BO IT System, beginning with entities that are subject to the CDD Rule. Accordingly, financial institutions are not likely to have access to the BO IT System any time soon. Additionally, financial institutions will not be required to use the BO IT System or report discrepancies to FinCEN, and thus until the CDD Rule is amended, their current compliance obligations under the CDD Rule and Bank Secrecy Act (BSA) remain unchanged.

We provide below a summary of the key terms of the Access Rule and notable changes relative to the Proposed Rule. The Access Rule will become effective on February 20, 2024.

Access to BOI under the final rule

Who can access BOI

The CTA and Access Rule authorize FinCEN to disclose BOI stored in the BO IT System to five categories of recipients for specific purposes:

- **Financial institutions**, with the consent of the relevant customer, to facilitate compliance with CDD requirements under applicable law, and **federal functional regulators and other appropriate regulatory agencies** acting in a supervisory capacity to assess financial institutions' compliance with applicable CDD requirements;[4]
- **Federal agencies** engaged in national security, intelligence, and/or law enforcement activities if the requested BOI is for use in furtherance of such activities;
- **State, local, and tribal law enforcement agencies** if "a court of competent jurisdiction" has authorized the law enforcement agency to seek the information in a criminal or civil investigation;
- **Foreign requesters** (e.g., foreign law enforcement agencies, judges, or competent authorities) provided that their requests follow specific processes and meet certain criteria; and
- **Treasury personnel** including any Treasury officer or employee (1) whose official duties require BOI inspection or disclosure, or (2) for tax administration.

The Access Rule imposes specific conditions on each category of recipients' access to the BO IT System, including requirements to obtain various forms of authorization (e.g., court authorization for state law enforcement authorities) and limitations on their scope of access to the BO IT System. These restrictions are intended to reflect the CTA's policy of treating BOI as inherently sensitive information. The Access Rule's core standards for government entities' access to BOI are largely consistent with the Proposed Rule (other than certain clarifications and modifications, including standards for foreign requestors' access to BOI and court authorization requirements for law enforcement). However, FinCEN made several notable revisions with respect to financial institutions' use of BOI.

For purposes of financial institutions' access to BOI, the Proposed Rule interpreted the CTA's reference to "customer due diligence requirements under applicable law" as a narrow reference to the CDD Rule. This narrow reading had two effects: first, the Proposed Rule would have only permitted financial institutions to use BOI for CDD Rule compliance purposes, rather than the broader compliance purposes for which financial institutions typically use customer information, such as suspicious activity monitoring and reporting and sanctions screening. Second, the Proposed Rule would have only permitted the subset of financial institutions that are subject to the CDD Rule (i.e., banks, broker-dealers, futures commission merchants, introducing brokers in commodities, and mutual funds) to access the BO IT System, whereas other financial institutions subject to the BSA – such as money service businesses (MSBs) (including cryptocurrency companies) – would not have access. Many commenters objected to this narrow interpretation of "customer due diligence requirements," arguing that, among other things, the restrictions exceeded those that apply to the use of customer information under the CDD Rule and materially undermine the value of the BO IT System for AML/CFT compliance purposes.

In response to these comments, FinCEN broadened the definition of "customer due diligence requirements under applicable law" and will authorize financial institutions to use BOI to satisfy any AML/CFT obligations under the BSA, as well as other legal requirements designed to safeguard U.S. national security (e.g., sanctions laws and regulations), provided that such compliance reasonably requires a financial institution to identify and verify beneficial ownership.[5] Accordingly, a financial institution will be permitted to use BOI to satisfy its broader BSA compliance obligations, including its AML program, customer identification, SAR filing, and enhanced due diligence requirements, as well as compliance with U.S. sanctions (e.g., through sanctions screening).[6] Financial institutions are prohibited from using BOI for any unrelated purpose, however, such as business development or assessing whether to extend credit to a legal entity.

FinCEN's broader reading of "customer due diligence requirements" also gives the agency the discretion to extend BOI access to financial institutions that are not subject to the CDD Rule, such as MSBs. FinCEN stated, however, that in the immediate term it intends to limit access exclusively to entities subject to the CDD Rule. FinCEN believes that this phased approach is necessary to ensure that BOI remains subject to adequate safeguards, as covered financial institutions under the 2016 CDD Rule are subject to strict data security requirements under the Gramm-Leach-Bliley Act, whereas other financial institutions are subject to "more fragmented security standards" that will require "additional time to evaluate and determine the extent to which standards and oversight mechanisms are required." FinCEN noted, however, that it will continue to evaluate the possibility of expanding access to other categories of financial institutions, as well as other relevant industry sectors.

In response to a common question from stakeholders, FinCEN also clarified in the Access Rule that banks are not required to use the BO IT System and may continue to use their existing processes to comply with the CDD Rule, and the BSA more broadly. FinCEN, together with federal and state banking regulators, also released a statement to the same effect, which reiterated that the Access Rule "does not create a new regulatory requirement for banks to access BOI from the BO IT System or a supervisory expectation that they do so."[7] However, to the extent that financial institutions use BOI from the BO IT System, they must comply with the Access Rule.

Standards and timing for access

FinCEN stated that it intends to take a phased approach to providing access to the BO IT System. Starting in 2024, FinCEN will administer a pilot program that will initially extend access to the BO IT System to a handful of key federal agency users, followed by a second stage extending access to certain federal law enforcement and national security agencies that have existing memoranda of understanding with FinCEN, and a third phase that extends access to other federal and state agencies and partners. Finally, covered financial institutions and their regulators will be the last category of users that will have access to the BO IT System. FinCEN stated that the agency expects "that the timing of their access will roughly coincide with the upcoming revision of FinCEN's 2016 CDD Rule."

Government entities and financial institutions will also receive varying degrees of access to the BO IT System. Whereas certain government entities (e.g., Treasury personnel and federal law enforcement and intelligence agencies) will have the ability to run multiple direct searches through the BO IT System, financial institutions will have more limited access. In particular, financial institutions would be required to submit specific identifying information for a reporting company "and receive in return an electronic transcript with that entity's BOI."[8] FinCEN anticipates that the results would be available immediately and search requests would not be subject to manual review by FinCEN. The agency further stated that it intends to establish a dedicated contact center to respond to inquiries regarding BOI reporting requirements and technical issues with the BO IT System. The Access Rule does not specify the parameters or technical standards for access to the BO IT System; however, FinCEN stated that it expects that financial institutions will use Application Programming Interfaces (APIs) to access BOI and that the BO IT System will accommodate the use of APIs for this purpose.

Security, confidentiality, disclosure, and violations/penalties

Re-disclosure of BOI

Notably, FinCEN responded to comments from industry stakeholders by loosening and clarifying the restrictions on re-disclosure of BOI to officers, employees, contractors, and agents. Under the CTA, authorized recipients may re-disclose BOI to specific parties, including to officers, employees, contractors, and agents for the particular purpose for which the BOI was requested. In the Proposed Rule, FinCEN interpreted the CTA's re-disclosure provisions narrowly and only permitted financial institutions to re-disclose information with officers, agents, contractors, and employees "in the United States." Many commenters voiced concerns with those restrictions, noting that a flat prohibition on sending BOI abroad would impose unnecessary burdens on financial institutions, many of which operate global compliance programs that distribute responsibilities across regions. FinCEN acknowledged these comments in the Access Rule and revised the regulatory language to allow financial institutions to send BOI to most jurisdictions outside of the United States, other than China, Russia, any jurisdiction designated as a state sponsor of terrorism, and any jurisdiction that is subject to comprehensive sanctions.

FinCEN also clarified that financial institutions will be permitted to share BOI with beneficial ownership data service providers, "RegTech" firms, due diligence vendors, and other third-party service providers, provided that "they and their employees are 'agents' or 'contractors' of a financial institution" and "are performing a function on behalf of the financial institution that requires direct access to it." A financial institution's "contractors" and "agents" also include individuals and entities performing work for the financial institution by contract, such as outside counsel, auditors, and providers of data analysis software tools.[9] Financial institutions would remain liable for any failure by contractors or agents to comply with the Access Rule, however, and agents and contractors would only be permitted to use BOI for purposes permitted under the CTA and Access Rule (meaning that BOI may not be integrated into downstream services offered by a service provider).

Data security and consent

The Access Rule requires financial institutions and government entities to implement controls and policies to safeguard BOI and ensure that it is only used for permissible purposes. For financial institutions, the security requirements under the Access Rule broadly align with those of the Proposed Rule. Financial institutions must, among other things, establish security and information handling procedures that align with the standards required under section 501 of the Gramm-Leach Bliley Act and its implementing regulations[10] and implement procedures for employee training. FinCEN expects that federal functional regulators will assess compliance with the Access Rule during the course of safety and soundness examinations and that SROs will similarly assess compliance during their BSA examinations.

Under the CTA, financial institutions are also required to obtain customer consent prior to accessing BOI. The Access Rule does not prescribe any particular means through which financial institutions must obtain a customer's consent, and FinCEN noted that the Rule affords financial institutions "substantial discretion" to obtain consent through any lawful method.[11]

Violations and penalties

The CTA and Access Rule provide for civil and criminal penalties for violations of the rule, which FinCEN implemented without change. Violations of the CTA may result in a civil penalty of $500 per day for each violation that continues or has not been remedied. Criminal penalties may result in a fine of no more than $250,000 or imprisonment for not more than 5 years (or both). In addition, FinCEN will have discretion to suspend or revoke access to the BO IT System if a financial institution fails to comply with the Access Rule. FinCEN stated that decisions to suspend or revoke access will be made on a case-by-case basis, based on all facts and circumstances.

Looking ahead

FinCEN acknowledged that many open questions remain regarding the implementation of the CTA and its implications for financial institutions' compliance obligations. For example, it is still unclear how financial institutions would be expected to address discrepancies between information contained in the BO IT System and information provided by a customer, or whether financial institutions would receive a safe harbor if they relied on information in the BO IT System. FinCEN generally deferred discussion of these issues for its forthcoming rulemaking amending the CDD Rule. FinCEN noted, however, that financial institutions would not be required to use the BO IT System or report discrepancies to FinCEN, and until the CDD Rule is amended, their current compliance obligations under the CDD Rule and BSA remain unchanged. FinCEN did not commit to any particular date for issuing a proposed rule amending the CDD Rule, and the timeline remains uncertain given the agency's many competing obligations and limited resources.

FinCEN's amendments to the Access Rule were received positively by many industry stakeholders and may meaningfully increase the utility of the BO IT System for financial institutions. Whether most financial institutions decide to rely on the BO IT System, rather than their current CDD processes and procedures, remains to be seen, however, and will likely depend on FinCEN's amendments to the CDD Rule. More broadly, it remains unclear if the CTA will ultimately reduce the compliance burdens for financial institutions in any material respect. Financial institutions and other stakeholders are advised to continue to monitor developments over the coming months.

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Paul Marquardt
+1 202 962 7156
paul.marquardt@davispolk.com

Will Schisa
+1 202 962 7129
will.schisa@davispolk.com

Daniel P. Stipano
+1 202 962 7012
dan.stipano@davispolk.com

Charles Marshall Wilson
+1 202 962 7130
charles.wilson@davispolk.com

[1] The BOI Reporting Rule is described in our October 2022 client update.

[2] 31 CFR § 1010.230

[3] The Proposed Rule is described in our December 2022 client update.

[4] Authorized agencies also include state bank supervisors and state credit union regulators. Certain qualifying self-regulatory organizations (SROs) such as FINRA are also permitted to receive BOI from financial institutions and federal functional regulators for the purpose of assessing a financial institution's compliance with CDD requirements.

[5] Specifically, the Access Rule defines "customer due diligence requirements under applicable law" to include "any legal requirement or prohibition designed to counter money laundering or the financing of terrorism, or to safeguard the national security of the United States, to comply with which it is reasonably necessary for a financial institution to obtain or verify beneficial ownership information of a legal entity customer."

[6] For example, a financial institution may use BOI to assess whether sanctions apply to an entity by virtue of the Office of Foreign Assets Control's "50-percent" rule.

[7] FinCEN, Board of Governors of the Federal Reserve System Federal Deposit Insurance Corporation National Credit Union Administration Office of the Comptroller of the Currency, and State Bank and Credit Union Regulators, Interagency Statement for Banks on the Issuance of the Beneficial Ownership Information Access Rule (December 21, 2023), https://www.fdic.gov/news/financial-institution-letters/2023/fil23067a.pdf.

[8] Financial institutions will have access to the information included in each reporting company's BOI report, including identifying information about its beneficial owners (e.g., name, date of birth, residential or business address, and either a unique identifying number from an acceptable identification document such as a passport or the individual's FinCEN identifier). However, financial institutions will not have access to images of the identifying documents (e.g., passports or government IDs). In addition, FinCEN does not anticipate providing bulk data exports to authorized users.

[9] FinCEN acknowledged that financial institutions may also be required to share BOI with other entities that do not qualify as employees, contractors, or agents (e.g., affiliated financial institutions or other financial institutions involved in syndicated loan agreements) but deferred any further discussion of the issue for future guidance.

[10] *See* 15 U.S.C. 6801(b) and 6805. Section 501 of the Gramm-Leach-Bliley Act requires each Federal functional regulator to establish appropriate standards for the financial institutions subject to its jurisdiction relating to administrative, technical, and physical safeguards to (1) ensure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of such records; and (3) protect against unauthorized access to or use of such records or information which could result in substantial harm or

inconvenience to any customer. The Federal functional regulators have implemented these requirements in different ways. For example, the OCC, FRB, FDIC, and NCUA have issued the standards in the form of interagency guidelines, while the CFTC and SEC have incorporated the Gramm-Leach-Bliley standards into their regulations, respectively 17 CFR § 160 and 17 CFR § 248.30(a).

[11] FinCEN noted that the Access Rule "only requires the financial institution to obtain a reporting company's consent at a time prior to an initial request for the reporting company's BOI from FinCEN, and it may rely on that consent to retrieve the same reporting company's BOI on subsequent occasions, including to open additional accounts for that reporting company, unless the consent is revoked."