KPMG

Regulatory Alert

Regulatory Insights

January 2024

FinCEN CTA: Beneficial Ownership Information Access

KPMG Insights:

- ***BOI Who?:*** *Only authorized recipients can request access to the BOI database under the CTA, with unique access pathways and purposes for each category.*
- ***Safeguarding Information:*** *Seeks to ensure authorized recipients protect BOI with security measures, confidentiality requirements, and standardized access protocols.*
- ***Penalties Strike:*** *Unauthorized use of BOI comes with risks ranging from civil and criminal penalties to suspension from the BOI system.*

Implementation of the CTA BOI requirements consists of three rulemakings: 1) BOI Reporting Rule (finalized September 2022 - see KPMG Regulatory Alert, here); 2) BOI Access Rule (finalized December 2023); and 3) revisions to the current customer due diligence (CDD) requirements for financial institutions (forthcoming).

BOI is considered to be sensitive information and will be held to the government's "high rating". Authorized recipients of BOI need standards and procedures for storing the information, with restrictions in place for authorized personnel access only and for authorized purposes only. Any authorized entity or individual that is transmitting, receiving, accessing and/or analyzing BOI data should have MOUs/agreements in place for all procedural and control requirements before obtaining BOI.

The Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) issues a final rule to implement the beneficial ownership information (BOI) access and related safeguards provisions of the Corporate Transparency Act (CTA). These regulations will govern authorized access to the BOI database (referred to as the beneficial ownership IT system – or BO IT system), which became operational on January 1, 2024. The final BOI Access Rule will become effective February 20, 2024, though access to the BO IT system will take a phased approach beginning with a pilot for certain federal agency users during 2024.

The final rule is adopted largely as proposed (see KPMG's Regulatory Alert, here), with a modification that permits financial institutions and regulatory agencies to access BOI from the FinCEN BOI database (the BO IT system) for a broader range of purposes than originally proposed, including to facilitate AML/CFT requirements, safeguard national security, and help ensure compliance with these requirements.

The final rule, outlined below, aims to limit BOI access: 1) to authorized recipients only, 2) for purposes permitted by the CTA, and 3) while maintaining security and confidentiality.

Beneficial Ownership Information Access & Safeguards

1) & 2) Authorized Recipients/Purpose

The CTA authorizes FinCEN to disclose BOI to six categories of recipients highlighted in the table below. The final rule outlines each category's unique access to

FinCEN's BO IT system, the purposes for which recipients can request BOI, and associated restrictions and requirements.

Recipients	Access	Purpose	Restrictions/Requirements
Federal government agencies **State, local, and tribal law enforcement agencies**	Direct	National security, intelligence, or law enforcement activities.	— Justifications for accessing BOI in system would need to be filed by federal agencies with FinCEN and subject to audit by FinCEN. — A "court of competent jurisdiction" would need to authorize state, local, and tribal law enforcement access to BOI in system.
Foreign law enforcement and central authorities (foreign requesters)	Indirect	National security, intelligence, or law enforcement activities.	Requests must come through an intermediary (federal agency) channel and be made either: — In compliance with international treaties, agreements, or conventions, or — By law enforcement, judicial, or prosecutorial authorities in a trusted foreign country. If approved, intermediary would retrieve BOI from system and securely transmit to foreign requester.
Financial Institutions (FIs)	Direct, but limited	Facilitate compliance with customer due diligence (CDD) obligations and any legal requirements or prohibitions (e.g., AML/CFT) or safeguarding national security.	Must have relevant reporting company's consent and FinCEN identifier to query BOI directly from system.
Federal Functional Regulators and Other Regulatory Agencies	Direct, but limited	Supervisory capacity for assessing FIs' compliance with CDD requirements.	— May access the same BOI as the FIs they supervise directly from system for compliance with CDD, AML, CFT, or national security-related requirements. — May directly access BOI for law enforcement activities.
Department of the Treasury	Direct	Any purpose tied to any Treasury officer or employee's official duties, including BOI inspection or disclosure, and tax administration; permitted to use BOI for tax administration, enforcement actions, intelligence and analytical purposes, sanctions designation investigations, identification of blocked property, audits, and oversight.	

3) Security and Confidentiality

The CTA imposes access-control protocols on "requesting agencies" and the final rule imposes BOI data security and confidentiality requirements that vary by recipient category, but generally require recipients to:

— Have standards and procedures for storing the information in a secure system to which only authorized personnel have access and only for authorized purposes.

— Enter into an agreement with FinCEN specifying these standards and procedures.

— Maintain for review or audit key information about specific BOI searches or requests.

— Provide certifications regarding compliance with the statute and implementing regulations, as applicable.

The final rule specifically requires FI recipients to:

— Develop and implement administrative, technical, and physical safeguards "reasonably designed" to

protect BOI as a precondition for receiving it (based on the safeguard requirements for FIs under Section 501 of the Gramm-Leach-Bliley Act (GLBA) – notably FIs not subject to regulations issued pursuant to Section 501 of the GLBA would be held to these same standards).

- Obtain and document a reporting company's consent before requesting that company's BOI (though FinCEN will not require proof at the time of request).
- Provide certification to FinCEN "in such form and manner as FinCEN shall prescribe" for each BOI request that the FI:
  - Is requesting the information to facilitate its compliance with CDD requirements under applicable law.
  - Obtained the reporting company's written consent to request its BOI.
  - Has fulfilled other requirements of the section, including those related to restrictions on personnel access to the information and safeguards to protect the security, confidentiality, and integrity of the information.

FinCEN states that FI compliance with these requirements will be assessed by their Federal Functional Regulators in the course of safety and soundness or GLBA examinations, or by financial Self-Regulatory Organizations (SROs) during Bank Secrecy Act (BSA) examinations.

Violations and Penalties

The final rule defines "unauthorized use" of BOI to include any unauthorized access of BOI, including any activity in which an employee, officer, director, contractor, or agent of an authorized recipient knowingly violates applicable security and confidentiality requirements in connection with accessing such information.

The CTA provides for both civil and criminal penalties. In addition, FinCEN may suspend or debar a requesting entity from access to BOI for failing to satisfy the requirements regarding obtaining BOI, using BOI, and securing BOI.

Implementation

The final rule becomes effective February 20, 2024. FinCEN is taking a multistage approach to providing access to the BO IT system from which authorized users may obtain BOI.

- First Stage: Pilot program for "a handful of key Federal agency users" starting in 2024.
- Second Stage: Extend access to Treasury offices and certain Federal agencies engaged in law enforcement and national security activities that already have Memoranda of Understanding (MOUs) for access to BSA information.
- Subsequent Stages: Extend access to additional Federal agencies engaged in law enforcement, national security, and intelligence activities, as well as state, local, and tribal law enforcement partners, intermediary federal agencies in connection with foreign government requests, and financial institutions and their supervisors.

FinCEN will publish for public comment the forms that state, local and Tribal law enforcement agencies and financial institutions will use to obtain BOI from FinCEN.

Note: On November 30, 2023, FinCEN published a separate final rule that extends the timeframe for reporting companies to submit their initial BOI reports to FinCEN. Under the final rule, reporting companies created or registered on or after January 1, 2024, and before January 1, 2025, will have 90 days to submit their initial BOI reports, while those formed on or after January 1, 2025, will continue to be required to submit their initial BOI reports within 30 days.

Interagency Statement

FinCEN, along with the Federal Reserve Board (FRB), the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC), the National Credit Union Administration (NCUA), and state bank and credit union regulators, also issue a related interagency statement to banks regarding the final rule.

The agencies state 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. The rule does not require changes to BSA/AML/CFT compliance programs designed to comply with the current CDD rule and other BSA requirements, such as the institution's customer identification program requirements and suspicious activity reporting procedures. However, access to and use of BOI obtained from the BO IT System must comply with the CTA and the final rule's requirements.

For more information, please contact John Caruso, or Michaela Soctomah.

Contact the author:

Amy Matsuo
Principal and National Leader
Regulatory Insights
amatsuo@kpmg.com

kpmg.com/socialme