Surveillance Use Policy
FinCEN
San Diego City Attorney's Office

PURPOSE

The Financial Crimes Enforcement Network (FinCEN) is a bureau of the U.S. Department of the Treasury whose mission is to safeguard the financial system from illicit activity. FinCEN aids in investigating fraud, unlawful business practices, and other criminal activity by collecting and analyzing financial data from banks and businesses, providing actionable leads to investigative agencies.

FinCEN hosts a secure website query tool (FinCEN Query) for authorized users to access and analyze FinCEN data. It is intended to meet the mission needs of FinCEN's analysts as well as law enforcement and regulatory users.

USE

FinCEN Query is to be used by the Affirmative Civil Enforcement (ACE) Unit in the Civil Litigation Division of the San Diego City Attorney's Office (SDCAO) to investigate fraud, consumer protection complaints, and violations of the California Unfair Competition Law (UCL). Use of the system is based on a "right to know, need to know" basis, meaning that the employee accessing the system is both authorized to use it based on their specific work duties and are using it only for a specific case or task assigned to them. The use of FinCEN Query is an essential component of case investigation that both enhances and advances the investigative process; it is used by sworn and non-sworn law enforcement, and regulatory employees throughout San Diego County.

City of San Diego Administrative Regulations associated with Use include:

- A.R. 90.62 Information and Communications Technology Acceptable Use
- A.R. 90.63 Information Security
- A.R. 90.64 Protection of Sensitive Information & Data
- A.R. 90.68 Procurement of Technology Solutions
- A.R. 90.75 Data Governance

Users can make inquiries on a variety of identifiers, such as name, date of birth, social security number, and identification number. The system provides a list of query results in logical groupings that can be sorted and searched for the information needed. The search results are a possible match to the query and should be confirmed with the record source, as necessary.

Information generated through FinCEN Query searches includes reports and documentation that banking institutions, money service businesses, and businesses submit in accordance with the Bank Secrecy Act (BSA). Common documentation includes Suspicious Activity Reports (SARs) and Currency Transaction Reports (CTRs).

The SAR is a report filed by bank personnel if certain circumstances appear uncommon or suspicious. The information, in and of itself, is not proof of a crime or other violation of law, but an indicator that some banking or transactional activity is atypical and possibly an indicator of fraud, money laundering, or other illicit activity.

The CTR is a reporting of a cash withdrawal or deposit above a threshold amount exceeding $10,000. The CTR also is not evidence of a crime, but merely a report documenting large cash transactions. In instances where cash transactions are broken up over a series of days that may total or exceed the $10,000 threshold amount, the activity may prompt bank personnel to file a SAR for suspected "structuring" transactions that may signal attempts to evade the $10,000 CTR reporting requirement.

DATA COLLECTION

The SDCAO does not collect the data that is accessed through FinCEN Query. The data is collected from financial institutions and the SDCAO accesses that data as needed to protect consumers from unlawful practices and to enforce state and local labor laws to hold employers accountable.

DATA ACCESS

Only authorized SDCAO ACE Unit Investigators may access FinCEN Query on a "right to know, need to know" basis. All queries must be conducted for a legitimate work purpose. When a user conducts a query using FinCEN Query, when prompted they must indicate the purpose category and/or the specific purpose for the search by using a specific case number.

DATA PROTECTION

Users are required to log in to FinCEN Query using their work computer in a secure, access-controlled facility. Work computers require an individual user login for access. When working remotely, users are required to log in via the City's Virtual Private Network (VPN) using a work computer and multi-factor authentication.

City of San Diego Administrative Regulations associated with Use include:

- A.R. 90.95 Telework Program

City of San Diego Policies associated with Data Protection include:

- Information Technology Policy - Information Security Standards and Guidelines
- Information Technology Policy - Data Loss Prevention System Guidelines and Standards

DATA RETENTION

When the SDCAO determines that FinCEN information no longer has a legitimate case need, the information is destroyed in a manner preventing the identity of the subject from being reasonably ascertained, e.g., shredding printouts, deleting electronic records, and clearing from computer "Trash" folders.

The SDCAO will follow its Records Retention Guidelines with regards to FinCEN data as established by law and policy.

Government Code associated with ARJIS Data Retention include:

- Government Code 34090 – Records Retention Period

City of San Diego Administrative Regulation associated with SDLAW Data Retention include:

- A.R. 85.10 – Records Management, Retention and Disposition

PUBLIC ACCESS

The public has no access to the FinCEN Query applications or its secure network, or to information in its database.

THIRD PARTY DATA SHARING

There is no third-party data sharing with the following exception. The SDCAO may provide relevant information obtained from FinCEN query to outside counsel contracted with the SDCAO to handle select cases and using a secure, approved file-sharing method.

TRAINING

FinCEN Query provides online training in the use of its applications on its secure web portal for all authorized users. It will also provide in-person training by request. Users must have completed FinCEN training prior to use. In addition, users must have completed all required City of San Diego training related to Information Technology before receiving access.

AUDITING AND OVERSIGHT

FinCEN Query captures users' query transactions and audit reports can be provided to the SDCAO Agency CLETS Coordinator or their designee for review. Users who leave the SDCAO or transfer to an assignment not requiring FinCEN Query use have their access removed. When conducting an audit, court case numbers and names entered by the user for queries will aid in confirming the user's "right to know, need to know." The SDCAO will conduct periodic random checks of system access and request audits for proper authorized use.

MAINTENANCE

FinCEN is responsible for uploading and maintaining the information into the application database; it is also responsible for maintaining the application. FinCEN Query has a Help Desk system that can be accessed via telephone or email.