Surveillance Impact Report
FinCEN Query
San Diego City Attorney's Office

DESCRIPTION:

FinCEN Query is a database tool that provides authorized users (Federal, State, and local law enforcement, investigators, and regulatory users) access to financial transaction data primarily gathered by financial institutions to support law enforcement and regulatory agencies.

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 criminality by collecting and analyzing financial data from banks and businesses to provide 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.

FinCEN Query is to be used by the Affirmative Civil Enforcement (ACE) Unit of the San Diego City Attorney's Office (SDCAO) in cases where the City of San Diego is involved in investigating fraud, consumer protection complaints, and violations of the California Unfair Competition Law (UCL).

LOCATION:

FinCEN Query is to be accessed by SDCAO authorized ACE Unit employees via SDCAO computers, both in the SDCAO work site and remotely, with mandatory security protocols in place, such as the City's Virtual Private Network and Multi-Factor Authentication. The work sites of the SDCAO are in secure, access-controlled buildings. FinCEN Query is a web-based application that must be accessed via login authentication.

IMPACT:

The SDCAO's FinCEN Query Surveillance Use Policy safeguards civil liberties and civil rights. FinCEN Query uses are not based on discriminatory or viewpoint-based factors. The SDCAO's use of surveillance technology is intended to support and benefit the City of San Diego while minimizing and mitigating potential impacts on community members' civil rights and civil liberties. It is used only in performing legal services for the City. The information provided by FinCEN Query is sourced from financial institutions to protect against money laundering, fraud, and other illegal activity.

Surveillance Impact Report
FinCEN Query
San Diego City Attorney's Office

MITIGATION:

The collection, use, retention, or dissemination of data shall not be used to violate the Constitutional rights of any person or be used in any manner that would discriminate against any person based upon their ethnicity, race, gender, national origin, religion, sexual orientation, or gender identity. FinCEN Query is administered by the United States Treasury Department and serves to document financial transactions under the Bank Secrecy Act of 1970; it provides efficient and time-saving access to review these restricted records. FinCEN Query does not utilize visual or audio recording capabilities or use facial recognition.

DATA TYPES AND SOURCES:

FinCEN Query provides authorized users with information gathered from financial institutions including banks, credit unions, casinos, broker-dealers, and money services businesses, as well as corporate filings. Data types include:

- **Currency Transaction Reports (CTRs):** Records of cash transactions exceeding $10,000 conducted by financial institutions.

- **Suspicious Activity Reports (SARs):** Disclosures filed by financial institutions regarding known or suspected criminal activities, such as fraud, money laundering, or identity theft.

- **Reports of Foreign Bank and Financial Accounts (FBAR):** Filings used to report a financial interest in or signature authority over foreign financial accounts.

- **Currency and Monetary Instrument Report (CMIR):** A regulatory document used to report the physical movement or mailing of more than $10,000 in cash or monetary instruments into or out of the United States.

- **Designated/Specialized Forms:** Reports tracking specific high-risk operations like commercial casino transactions or monetary instrument sales.

DATA SECURITY:

SDCAO Computers require user login authentication and are situated in secure buildings with access control. When working remotely, authorized users are required to login via the City's Virtual Private Network using a work computer and multi-factor authentication. Only authorized employees of the SDCAO working in ACE Unit assignments shall access the data.

Surveillance Impact Report
FinCEN Query
San Diego City Attorney's Office

FISCAL COST:

FinCEN Query access is provided at no cost.

THIRD PARTY DEPENDENCE:

The SDCAO does not store data in FinCEN Query. FinCEN Query data are managed by FinCEN. FinCEN retains a user's search history for audit purposes. All data stored within the platform is restricted and only accessible to authorized persons. Information can be accessed by the SDCAO ACE Unit user and saved in secure network drives managed by the SDCAO. No data will be stored on City hardware or network drives unless downloaded from the web application for use in a qualifying investigation.

ALTERNATIVES:

Currently, there is no direct or legal alternative to FinCEN Query for accessing government-mandated financial reporting datasets like Suspicious Activity Reports (SARs), Currency Transaction Reports (CTRs), and other financial activity reports to which FinCEN provides access.

TRACK RECORD

The SDCAO has not previously implemented usage of FinCEN Query, however, the database search tool is commonly utilized in investigations by law enforcement, including San Diego Police Department (SDPD).

In June 2026, the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) recognized several cases during its Law Enforcement Awards Program for effectively using financial reporting data through FinCEN to support criminal prosecutions and safeguard the U.S. financial system:

Fraud: The Federal Housing Finance Agency-Office of Inspector General (OIG), the U.S. Department of Housing and Urban Development-OIG, and the Internal Revenue Service–Criminal Investigation (IRS-CI) investigated two real estate companies that conspired to purchase real estate at fraudulently depressed short sale prices, costing mortgage loan holders millions of dollars in losses. The five defendants and their co-conspirators corrupted a process meant to assist homeowners facing foreclosure. A federal jury returned a guilty verdict against the primary defendant for conspiracy to commit wire fraud and bank fraud, and related wire fraud counts.

Cybercrime: The Federal Bureau of Investigation (FBI) led an investigation into an international, financially motivated sextortion and money laundering scheme involving cyberstalking, interstate threats, extortion, money laundering, and wire fraud. The six subjects and additional co-conspirators attempted to extort approximately $6.9 million from thousands of potential victims and successfully extorted approximately $1.9 million from those victims, using digital wallet accounts.

Corruption: The U.S. Postal Inspection Service **(**USPIS) investigated a subject who was conspiring to commit mail and bank fraud and aggravated identity theft. The conspiracy victimized more than 900 individuals, stealing more than 700 checks, totaling a face value of more than $5 million. Following a guilty plea, the subject was sentenced to 114 months in federal prison.
(https://www.fincen.gov/news/news-releases/fincen-announces-recipients-its-11th-law-enforcement-awards-program)

PUBLIC ENGAGEMENT AND COMMENTS:

On September 23, 2026, at 12:00 p.m., there was a publicly held meeting in all nine council districts in the City of San Diego. The following surveillance technologies were presented by the SDCAO:

1. Aggregate Public Records Search Systems
2. Automated Regional Justice Information Systems
3. Products Received from Law Enforcement
4. SDLaw
5. FinCEN Query

The SDCAO video recorded this meeting so that it could be presented to a larger group. The benefit of the video was the capability of translating the presentation into over 100 languages such as Spanish, and other languages frequently used by the communities within San Diego, to maximize penetration of the materials to affected groups. The link to the video (TRUST Community Meeting - City Attorney's Office) is at:
https://www.youtube.com/watch?v=QOkigc7fNdw

There were eight attendees in San Diego City Council District 3. There were no attendees in any of the other districts.

There were six public comments and no questions out of the eight attendees. There were no comments submitted to the online public comment form.

Surveillance Impact Report
FinCEN Query
San Diego City Attorney's Office

Comment #1:

The speaker strongly opposed San Diego's continued use and funding of surveillance technologies such as ARJIS and ALPRs [Automated License Plate Recognition systems]. The speaker argued that these tools enable unrestricted data harvesting, violate civil rights, and were designed to circumvent protections rather than enhance safety. The speaker emphasized that surveillance and AI systems are inherently dangerous, cannot be responsibly regulated, and disproportionately harm vulnerable communities, especially in the context of ICE actions. The speaker concluded by urging elected officials to address these concerns and reaffirmed that the community will continue holding leaders accountable.

Comment #2:

The speaker expressed concern that technological progress should serve the public, not powerful interests. The speaker highlighted a report showing thousands of ALPR search entries labeled only as "other," which the speaker argued enables misuse despite supposed safeguards. The speaker stated that ambiguous search categories and limited auditing allow systems like ARJIS to be abused by malicious actors. The speaker stressed that subjective assurances of ethical data practices are insufficient and called for an end to the city's use of these surveillance technologies.

Comment #3:

The speaker spoke about how surveillance technology contributes to systems of displacement. He criticized the meeting's timing and short notice as a form of manufactured consent that limits public participation. The speaker also warned against relying on arrest data, noting that many arrests are biased or unconstitutional and should not inform surveillance systems. The speaker raised concerns about offsite access to these tools through VPNs and underscored that both the technologies and the processes surrounding them are deeply problematic.

Comment #4:

The speaker argued that San Diego must rethink its approach to surveillance technology. Speaker described a pattern in which society embraces new technologies without understanding their long-term consequences, using smartphones as an example. The speaker noted that individuals can control their personal devices, but government surveillance systems offer no comparable control to the public. Speaker urged leaders to follow a "do no harm" principle when implementing advanced technologies and stressed the need for transparency under the Trust Ordinance. Speaker stated that while harms from ALPRs are already known, the community still lacks critical information about ARJIS and its use.

Comment #5:

Speaker expressed frustration that the city has not followed the processes outlined in the Trust Ordinance, despite its unanimous approval. Speaker said the annual report, which passed the Privacy Advisory Board, still has not been presented to the City Council, calling this a failure of accountability. Speaker noted that required use policies and reviews for existing technologies have not occurred and criticized the city for discussing even more powerful surveillance tools without adhering to proper procedures. Speaker voiced deep concern about the impact on communities already facing risks from ICE actions and stated that the city is not taking the issue seriously.

Comment #6:

Speaker raised concerns that new surveillance technologies consistently bypass the Privacy Advisory Board, undermining their role in ensuring transparency and accountability. They warned that powerful entities, including large corporations and investors, may gain access to sensitive data, which could be exploited in harmful ways. Drawing comparisons to surveillance systems in other countries, the speaker cautioned that data could be weaponized to restrict essential services or freedoms. They argued that the government's partnerships with wealthy corporations contradict claims of avoiding such alliances and urged the city to scrutinize where data is being sent and how it might be used.

At an evening meeting on September 24, 2026, at 5:30 p.m., the SDCAO re-broadcast the recorded video from September 23, 2026. The link to the video (TRUST Evening Community Meeting City Attorney's Office) is at: https://www.youtube.com/watch?v=M2uG7aHxfw0

For the evening meeting, there were two attendees in San Diego City Council District 3 and four attendees virtually.

There were two public comments and no questions out of the attendees. There were no comments or questions submitted to the online public comment form.

Comment #1:

The speaker expressed deep appreciation for meeting host and the City Attorney's Office for their presentation on surveillance technology. The speaker described feeling overwhelmed by the information but grateful for gaining a new awareness of privacy and surveillance. The speaker now recognizes that monitoring is constant once they leave their home and commit to being more alert while staying open to emerging technology. The speaker close by reaffirming their long-time support for the PAB [Privacy Advisory Board], expressing love for its work, and sharing excitement about attending an upcoming meeting.

Comment #2:

The speaker thanked the group for hosting the public forum and praised the presenter for balancing civil data collection topics with law enforcement considerations such as "SARS" reporting and coordination with county sheriffs. The speaker raised concerns about data retention, referencing a state bill that would require judicial warrants for accessing personal data. The speaker questioned whether the standard of expunging data after 30 days is genuinely practiced and encouraged deeper discussion on both warrant requirements and long-term data retention in future PAB [Privacy Advisory Board] meetings.