FINANCIAL CRIMES ENFORCEMENT NETWORK

BSA SPOTLIGHT

Iranian Shadow Banking: Update on Trends in Bank Secrecy Act Data

November 23, 2026

A Financial Trend Analysis



This BSA Spotlight is a subset of FinCEN's Financial Trend Analysis series, which focuses on pattern and trend information identified in BSA data pursuant to Section 6206 of the Anti-Money Laundering Act of 2020 (AMLA). Section 6206 of the AMLA requires FinCEN to periodically publish threat pattern and trend information derived from BSA filings.[1] BSA Spotlights are designed to provide a visual representation of key data insights, illustrating trends and patterns found in BSA data in a concise format. The information contained in this report is relevant to the public, including a wide range of businesses, industries, and critical infrastructure sectors. The report also highlights the insights provided from BSA information filed by regulated financial institutions.

1. The AMLA was enacted as Division F, §§ 6001-6511, of the William M. (Mac) Thornberry National Defense Authorization.

Iranian Shadow Banking: Update on Trends in Bank Secrecy Act Data

Executive Summary: Based on reporting from U.S. financial institutions, FinCEN identified approximately $14.7 billion of financial activity (the "dataset") from January 2025 to August 2026 (the "review period") related to potential Iranian shadow banking activities. Based on FinCEN analysis of the dataset, potential Iranian shadow banking appears to have decreased by volume during the review period, which may be indicative of at least partial disruption of Iran's ability to operate shadow banking networks. The trends and methods associated with Iranian shadow banking remained relatively consistent through 2026, when compared to FinCEN's findings in its Financial Trend Analysis Iranian Shadow Banking: Trends in BSA Data (published October 2025), which reviewed transactions that occurred between 1 January and 31 December 2024. Potential Iranian shadow banking networks continue to be connected across continents—most prominently in the United Arab Emirates (UAE), Hong Kong, and Singapore—by a diverse array of businesses, including oil companies, shipping companies, investment companies, and technology procurement companies. These entities—many of which are likely front companies—transacted, on average, approximately $2.9 million per transaction during the review period, with a median of approximately $3.7 million per transaction, including with counterparties that may be witting or unwitting.

Key Updates and Findings

- Top transaction countries by company registration (total of originator and beneficiary transaction values) included the UAE (approximately $11.3 billion), Hong Kong (approximately $7.4 billion), and Singapore (approximately $4.9 billion). See figure 1 for more information.
- Top transaction countries by banking location (total of originator and beneficiary transaction values) included the UAE (approximately $9.6 billion), mainland China (approximately $6.2 billion), and Singapore (approximately $3.3 billion). See figure 2 for more information.
- Originators registered in Hong Kong (primarily banking in mainland China) sent the greatest amount of funds (approximately $5 billion or 34 percent), followed by originators registered in the UAE (approximately $3.8 billion or 26 percent) and Singapore (approximately $2.8 billion or 19 percent). See figure 3 for more information.
- Beneficiaries registered in the UAE received the greatest amount of funds (approximately $7.6 billion or 52 percent), followed by beneficiaries registered in Hong Kong (approximately $2.3 billion or 16 percent) and Singapore (approximately $2.2 billion or 15 percent). See figure 4 for more information.
- Hong Kong-registered companies banking at mainland China-based financial institutions originated 73 percent (approximately $3.7 billion) of the Hong Kong-originated transactions. An additional 15 percent of Hong Kong-registered companies sent funds using accounts at Hong Kong-based financial institutions (approximately $746 million).

- UAE-registered beneficiaries with accounts at Banque Misr UAE received approximately six percent of the total funds (approximately $941 million).[2]
- Companies registered in the Dubai Multi Commodities Centre (DMCC) Free Zone accounted for approximately 30 percent of UAE-related funds, and Limited Liability Companies in the UAE accounted for approximately 19 percent of UAE-related funds. Approximately 25 percent of funds were associated with seven other UAE-based free trade zones.[3]
- Funds flows from mainland China-based financial institutions to those in the UAE were the most common (approximately $2.6 billion), followed by Singapore to the UAE (approximately $981 million); unidentified jurisdictions to the UAE ($943 million); and the United Kingdom (UK) to the UAE (approximately $922 million).
- The potential exploitation of companies registered in the Marshall Islands and British Virgin Islands (BVI), usually at addresses linked to corporate registries, emerged as a potential area of concern.
- Financial institutions based in the UAE, mainland China, Hong Kong, and Singapore, as well as the UK and Switzerland, continue to be used by potential Iran-linked companies.
- Many potential Iran-linked companies had little to no web presence, had opaque ownership, were co-located with numerous other companies, or were recently incorporated.[4]
- Certain potential Iran-linked companies over a short timeframe sent or received multimillion dollar wire transfers that did not contain information about the source of funds, contained incomplete information about the source of funds, or did not match the customer's line of business.
- Potential Iran-linked companies frequently appeared in the same financial networks, demonstrating similar company characteristics and transacting in patterns similar to those referenced above with many of the same counterparties. The companies were involved in a diverse array of businesses, including shipping companies or oil companies.
- Potential Iran-linked companies did not appear to have everyday operational expenses such as salaries/wages or other miscellaneous/business expenses.

The information in this report is based on information obtained from FinCEN's analysis of BSA data and open sources, as well as insights from law enforcement and other partners.

2. On August 28, 2026, FinCEN issued a notice of proposed rulemaking (NPRM) identifying Banque Misr UAE as a financial institution operating outside of the United States of primary money laundering concern, and proposing a rule, pursuant to section 311 of the USA PATRIOT Act, prohibiting U.S. financial institutions from opening or maintaining a correspondent account for, or on behalf of, Banque Misr UAE.
3. Approximately 25 percent of funds were associated with UAE-registered entities where FinCEN could not determine the free trade zone location.
4. Connections to Iran were established using open source information, commercially acquired data, the Office of Foreign Assets Control's Specially Designated Nationals and Blocked Persons list, and other information available to FinCEN.

A Note on BSA Data

BSA reporting is merely tip and lead information, and the mere reporting of suspicious activity does not serve as proof of illegal activity. BSA reporting reflects suspicious activity that has been identified and reported by financial institutions and, therefore, should not be considered a complete representation of the scope of any particular type of suspicious activity. BSA reporting may include additional transactions and information beyond a specific transaction that may be reportable as suspicious and, accordingly, the total reportable suspicious activity amount in any report may be overly inclusive. For example, BSA reporting may reflect both completed and attempted transactions, both inbound and outbound transactions, transfers between accounts, and both legal and illicit activities associated with a particular subject. BSA reporting may also describe continuing suspicious activity or amend earlier reporting, or reports that cover expanded networks involved in potential illicit activity and therefore may reflect cumulative transactions from a single filer involving the same subject.

Scope and Methodology: FinCEN analyzed BSA information detailing transactions in the review period where financial institutions or FinCEN connected the financial activity to potential Iranian shadow banking activities from other BSA data, open source information, and other information available to FinCEN. This included select Suspicious Activity Reports (SARs) filed from February 2025 to August 2026, limited to transactions that occurred during the review period, as well as reporting from U.S. financial institutions related to correspondent transactions from specified foreign financial agencies. FinCEN further restricted the dataset to transactions valued at $500,000 and above, based on past analysis and research of Iranian shadow banking networks. FinCEN removed transactions where its analysis of BSA and other information could not corroborate links to Iran described by financial institutions. The final dataset totaled 4,983 transactions that occurred during the review period, totaling approximately $14.7 billion in activity.

Figure 1: Top Transaction Countries by Company Registration in Dataset, Total Originator and Beneficiary Transaction Values (USD), January 2025 – August 2026[5]

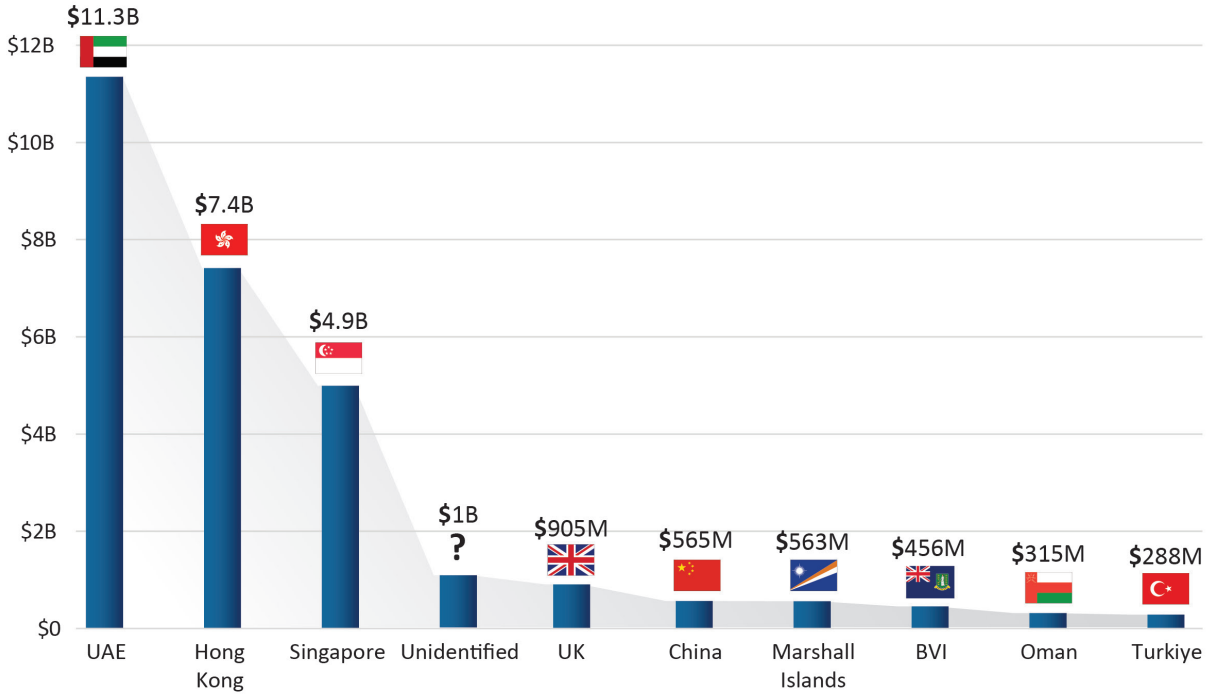
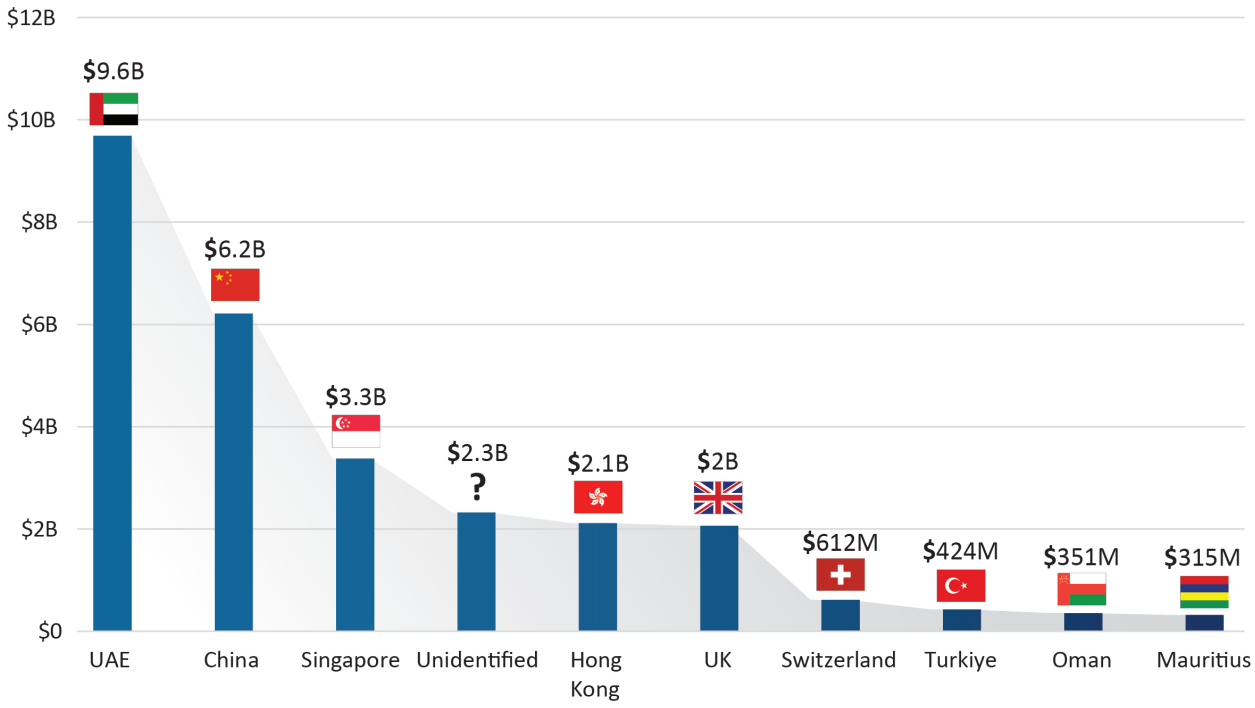


Figure 2: Top Transaction Countries by Banking Location in Dataset, Total Originator and Beneficiary Transaction Values (USD), January 2025 – August 2026



5. Jurisdictions may be unidentified due to incomplete or missing data provided to FinCEN. All charts include actual financial activity from January 2025 to August 2026.

Figure 3: Top Originator Registration Countries, by Transaction Value (USD), January 2025 – August 2026[6]

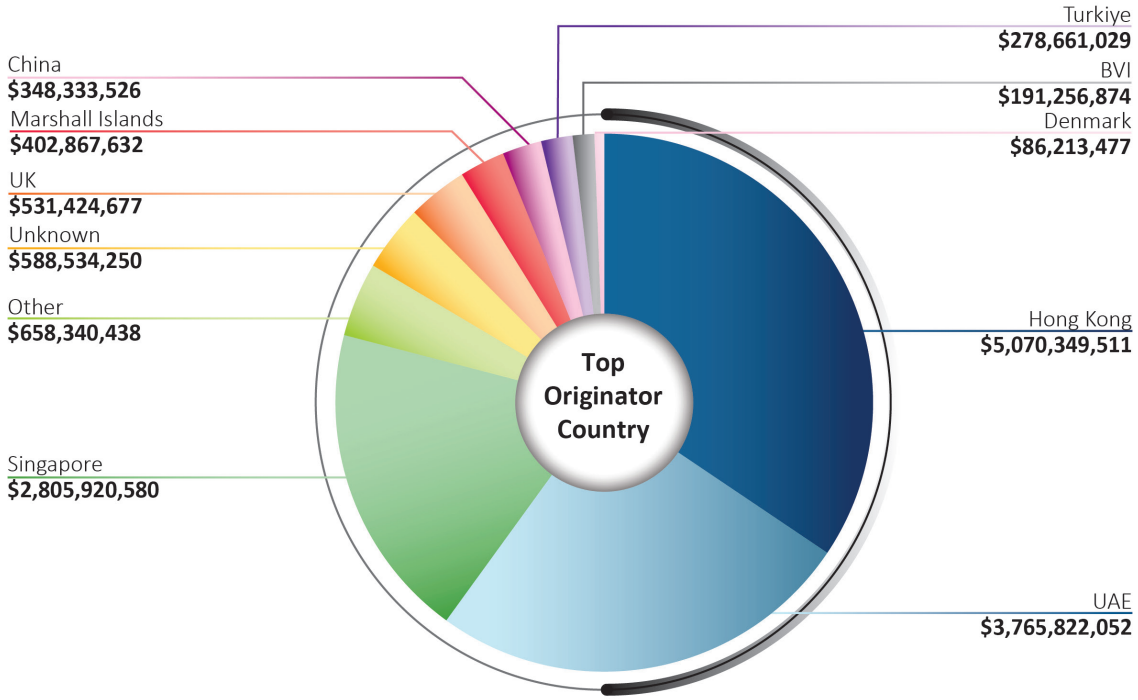
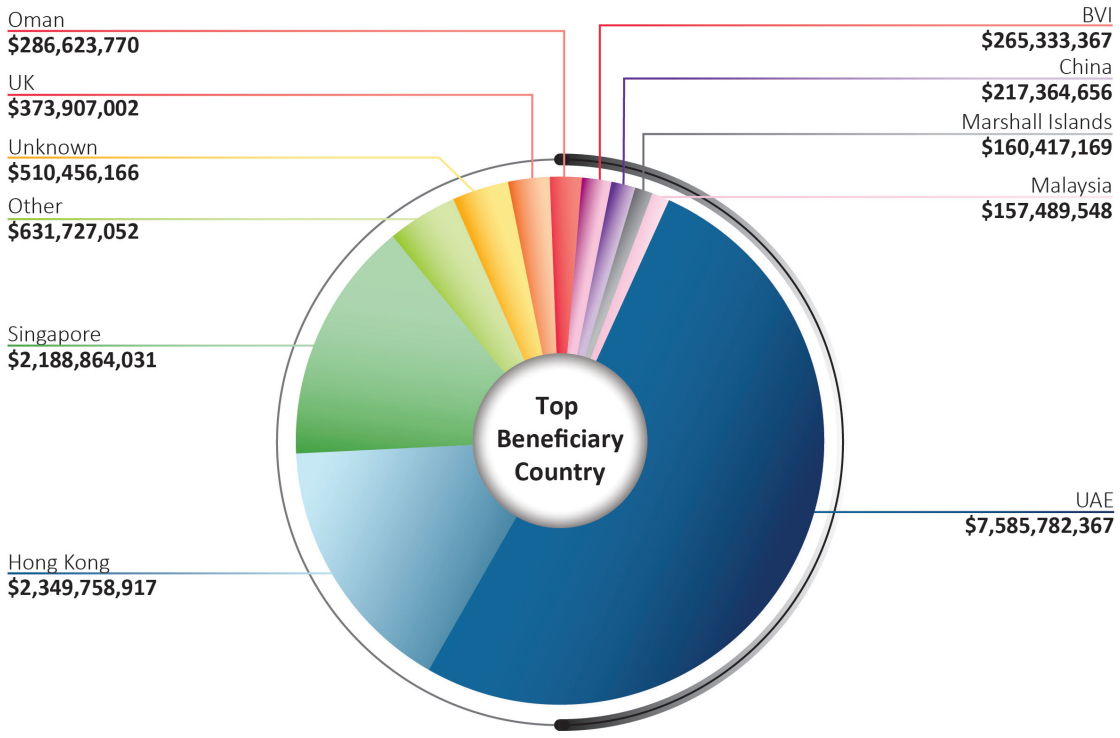
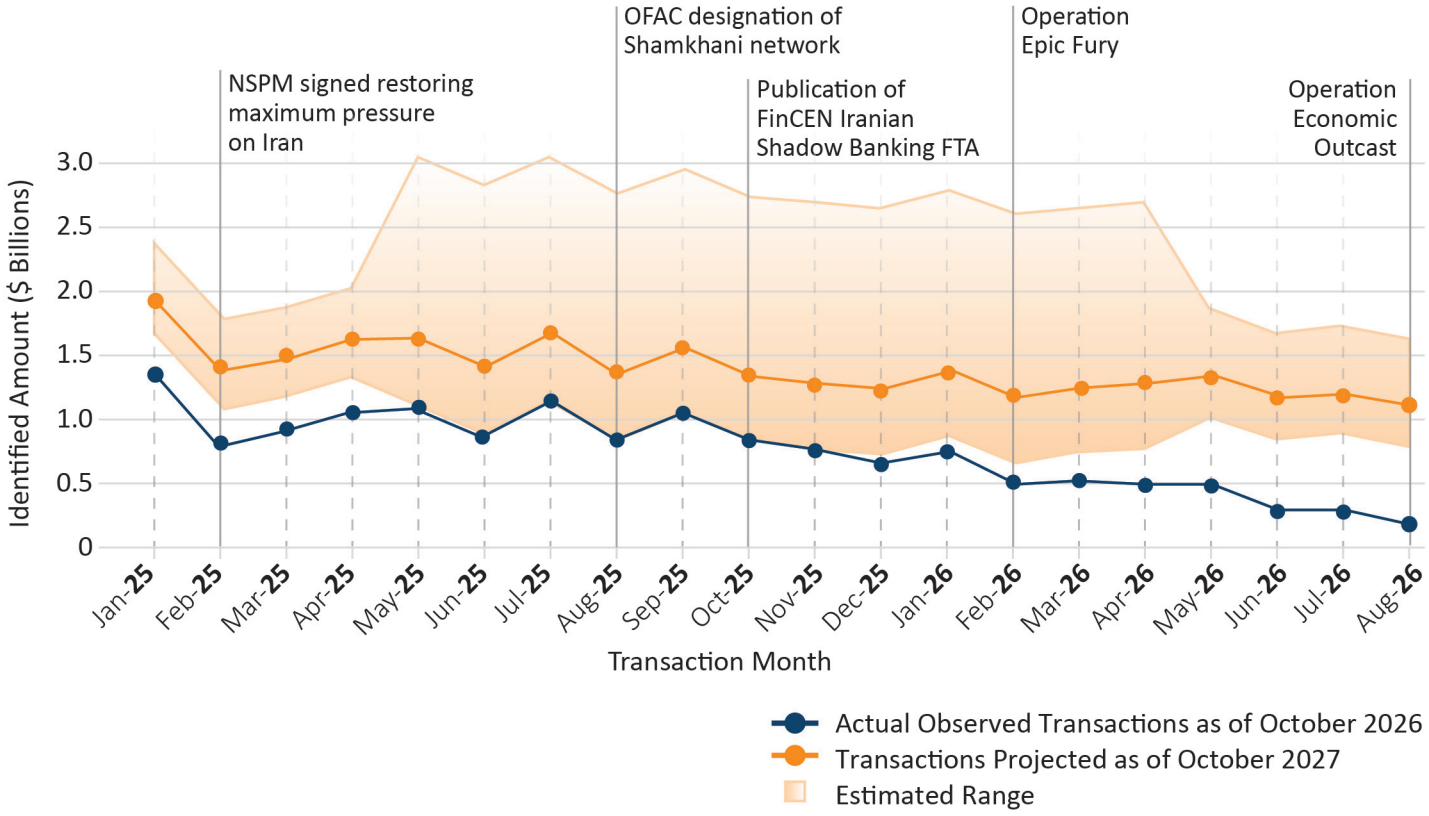


Figure 4: Top Beneficiary Registration Countries, by Transaction Value (USD), January 2025 – August 2026



6. Percentage of total actual value ($14.7 billion) identified during the review period.

Figure 5: Estimates of Potential Iranian Shadow Banking Network Transaction Values (USD), by Month



Model Methodology for Figure 5: FinCEN's ability to attribute a particular transaction to potential Iranian shadow banking, when not specifically identified by the filer, relies on establishing links using open source information including indictments, commercially acquired data, the Office of Foreign Assets Control's Specially Designated Nationals and Blocked Persons list, as well as other information available to FinCEN. There is an attribution lag between the time a transaction occurs and when FinCEN or FinCEN sources attribute it to Iran. To provide recent information while at the same time accounting for this attribution lag, FinCEN used a statistical approach to estimate the potential total value of transactions associated with potential Iranian shadow banking that may not be fully reflected yet in FinCEN's Iranian shadow banking dataset.[7] The model shows estimates of additional transaction amounts potentially associated with the network that FinCEN may identify through its analysis of transaction activity that occurred during the relevant time period. Importantly, these estimates do not represent new transactions but rather additional transactions that may be identified and attributed to Iranian shadow banking for the relevant time period based on additional FinCEN analysis.

7. The Development Model uses historical patterns to estimate additional transaction amounts that may be identified over time. This approach is based on concepts from actuarial loss development methods. For additional information on these methods, *see* https://www.actexmadriver.com/Assets/ClientDocs/prod_preview/A105RC.pdf.

FinCEN welcomes feedback on this report, particularly from financial institutions. Please submit feedback to the FinCEN Regulatory Support Section at www.fincen.gov/contact.

Reporting Suspicious Iran-Related Activity

FinCEN, through its Financial Institution Advisory Program, issues advisories to financial institutions concerning money laundering or terrorist financing threats and vulnerabilities for the purpose of enabling financial institutions to guard against such threats. These publications can be found at https://www.fincen.gov/resources/advisoriesbulletinsfact-sheets. FinCEN highlighted red flags on Iran-linked actors in one advisory and three alerts: *FinCEN Advisory on the Iranian Regime's Illicit Oil Smuggling Activities, Shadow Banking Networks, and Weapons Procurement Efforts* (FIN-2025-A002 on 6 June 2025); *FinCEN Alert on the Use of Front Companies, Financial Facilitators, and Digital Asset Infrastructure by Iran's Islamic Revolutionary Guard Corps to Evade Sanctions and Launder Proceeds* (FIN-2026-Alert002 on 11 May 2026); *FinCEN Alert to Counter Iranian Procurement Efforts for its Commercial Aviation Industry* (FIN-2026-Alert006 on 8 September 2026), and *FinCEN Alert to Counter Iranian Abuse of Religious Charity Networks*, (Fin-2026-Alert008 on 15 October 2026).

FinCEN's Whistleblower Program is accepting tips on Iran-related illicit finance: *FinCEN Whistleblower Bulletin: Blow the Whistle on Iran-Related Illicit Finance*.