



FinCEN, OFAC & FBI Joint Notice

FIN-2024-NTC2

July 16, 2024

FinCEN, OFAC, and FBI Joint Notice on Timeshare Fraud Associated with Mexico-Based Transnational Criminal Organizations

Suspicious Activity Report (SAR) Filing Request:

FinCEN requests that financial institutions reference this joint Notice by including the key term “**FIN-2024-NTC2**” in SAR field 2 (Filing Institution Note to FinCEN) and the narrative and select SAR field 34(z) (Fraud – Other) and include the term “**TimeshareMX**” in the text box.

The U.S. Department of the Treasury’s (Treasury) Financial Crimes Enforcement Network (FinCEN) is issuing this joint Notice with Treasury’s Office of Foreign Assets Control (OFAC) and the Federal Bureau of Investigation (FBI) to financial institutions,¹ urging them to be vigilant in detecting, identifying, and reporting timeshare² fraud perpetrated by Mexico-based transnational criminal organizations (TCOs).³ According to the FBI, since at least 2012, the Jalisco New Generation Cartel (CJNG)⁴ and other Mexico-based TCOs have increasingly targeted U.S. owners of timeshare properties in Mexico.⁵ Older adults,⁶ including retirees, are frequent victims in these schemes. The TCOs use proceeds

from timeshare fraud to diversify their revenue streams and finance other criminal activities, including the manufacturing and trafficking of illicit fentanyl and other deadly synthetic drugs into the United States.⁷

1. See 31 U.S.C. § 5312(a)(2); 31 CFR § 1010.100(t).

2. According to the American Resort Development Association, a trade association for the timeshare industry, timesharing “describes a method of use and/or shared ownership of vacation real estate where purchasers acquire a period of time (often a week) in a condominium, apartment or other type of vacation accommodation.” See generally American Resort Development Association, [Timeshare Terminology](#).

3. This joint Notice focuses on how TCOs are targeting U.S. owners of timeshares in Mexico. However, FinCEN is also aware of timeshare fraud schemes that defraud U.S. owners of timeshares in the United States. See generally Federal Trade Commission (FTC), “[Timeshares, Vacation Clubs, and Related Scams](#)” (Dec. 2023).

4. CJNG is a Mexico-based TCO and drug trafficking organization based in the Mexican state of Jalisco with strongholds in many cities and towns associated with Mexico’s tourism industry, such as Puerto Vallarta. According to U.S. law enforcement, CJNG is one of the predominant Mexico-based TCOs perpetrating timeshare fraud schemes. CJNG is also one of the TCOs that is primarily responsible for trafficking the majority of illicit fentanyl into the United States. Countering the CJNG and other Mexico-based TCOs is a top priority of the U.S. Government. See U.S. Drug Enforcement Administration (DEA), “[2024 National Drug Threat Assessment](#)” (May 2024), at pp. 12-15.

5. See generally FBI, “[Mexican Cartels Target Americans in Timeshare Fraud Scams, FBI Warns](#)” (June 7, 2024); FBI, [Timeshare Fraud](#); FBI Internet Crime Complaint Center (IC3), “[Scammers Targeting Owners of Timeshares in Mexico](#)” (Mar. 2, 2023).

6. For purposes of this joint Notice and to be consistent with the Elder Abuse Prevention and Prosecution Act, an older adult is considered an individual 60 years of age or older. See Pub. L. No. 115-70, 131 Stat. 1208 (2017).

7. See generally *supra* note 5.

FinCEN, OFAC & FBI Joint Notice

Based on reporting to the FBI Internet Crime Complaint Center (IC3) and the Federal Trade Commission (FTC) Consumer Sentinel Network Database, approximately 6,000 U.S. victims reported losing a total of nearly \$300 million between 2019 and 2023 to timeshare fraud schemes in Mexico. According to the FBI, this figure likely underestimates the total losses, as an estimated 80 percent of victims choose not to report the scam due to embarrassment, lack of resources, or other reasons.

As highlighted by Treasury in the 2024 National Money Laundering Risk Assessment, fraud of all kinds continues to be the largest source of illicit proceeds in the United States, with timeshare fraud and elder financial exploitation (EFE) becoming an increasing money laundering threat to the U.S. financial system.⁸ As identified by FinCEN, combating fraud and TCO activity are U.S. Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) National Priorities.⁹ Treasury is a key implementer of whole-of-government efforts to combat illicit finance associated with TCOs, including the operating capital needed to sustain the illicit fentanyl supply chain.¹⁰ Pursuant to Executive Order (E.O.) 14059, OFAC sanctioned multiple Mexico-based timeshare fraud networks affiliated with CJNG, depriving those illicit actors of their ill-gotten funds that finance the TCO and their drug trafficking operations into the United States.¹¹

FinCEN is jointly issuing this Notice with OFAC and the FBI to help financial institutions identify and report suspicious activity potentially associated with timeshare fraud in Mexico. This joint Notice (i) provides an overview of methodologies associated with these schemes and related financial typologies, (ii) highlights red flag indicators, and (iii) reminds financial institutions of their reporting requirements under the Bank Secrecy Act (BSA). In addition to filing BSA reports, financial institutions are critical partners in preventing their customers from becoming victims of timeshare fraud in Mexico, assisting those that become victims, and—in the case of older customers—reporting suspected EFE to law enforcement, their state-based Adult Protective Services,¹² and any other appropriate authorities.

-
8. See Treasury, “[2024 National Money Laundering Risk Assessment](#)” (Feb. 2024), at pp. 5, 14-15.
 9. See generally FinCEN, “[Anti-Money Laundering and Countering the Financing of Terrorism National Priorities](#)” (June 30, 2021).
 10. See generally The White House, “[2022 National Drug Control Strategy](#)” (Apr. 21, 2022); The White House, “[FACT SHEET: The Biden Administration Launches New Efforts to Counter Transnational Criminal Organizations and Illicit Drugs](#)” (Dec. 15, 2021); see also FinCEN, FIN-2024-A002, “[Supplemental Advisory on the Procurement of Precursor Chemicals and Manufacturing Equipment Used for the Synthesis of Illicit Fentanyl and Other Synthetic Opioids](#)” (June 20, 2024).
 11. See, e.g., Treasury, “[Treasury Sanctions CJNG-Run Timeshare Fraud Network](#)” (Mar. 2, 2023); Treasury, “[Treasury Sanctions Fugitive, Others Linked to CJNG Timeshare Fraud Network](#)” (Apr. 27, 2023); Treasury, “[Treasury Takes Third Action Against CJNG Timeshare Fraud Network Centered in Puerto Vallarta](#)” (Nov. 30, 2023).
 12. According to the National Center on Elder Abuse (NCEA), National Adult Protective Services Association (NAPSA), and the Keck School of Medicine of the University of Southern California (USC), “Adult Protective Services (APS) programs promote the safety, independence, and quality-of-life for vulnerable adults who are, or are in danger of, being abused, neglected by self or others, or financially exploited, and who are unable to protect themselves. APS is a social service program authorized by law in every state to receive and investigate reports of elder or vulnerable adult maltreatment and to intervene to protect the victims to the extent possible.” See generally NCEA, NAPSA, and Keck School of Medicine of USC, [Fact Sheet: Adult Protective Services, What You Must Know](#).

The information contained in this joint Notice is derived from FinCEN’s analysis of BSA data, open-source reporting, and information provided by the FBI and other law enforcement partners.

Methodologies of Timeshare Fraud Schemes in Mexico

According to the FBI, Mexico-based TCOs are targeting U.S. owners of timeshares in Mexico through complex, often yearslong telemarketing scams.¹³ These schemes operate in TCO-controlled call centers in Mexico staffed by telemarketers¹⁴ who are fluent in English (hereafter “scammers”). CJNG-controlled call centers are generally located in Jalisco, Mexico. Victims of these schemes can include any U.S. owners of timeshares in Mexico,¹⁵ but, according to the FBI, older adults with high-end timeshares that they no longer or infrequently use are especially vulnerable.¹⁶

Targeting U.S. Owners of Timeshares in Mexico

The TCOs generally obtain information about U.S. owners of timeshares in Mexico from complicit insiders at timeshare resorts. The price a TCO will pay for a timeshare owner’s personally identifiable information (PII) often corresponds with the value of the owner’s timeshare interests. After obtaining information on timeshare owners, the TCOs, through their scammers, contact victims by phone or email and claim to be U.S.-based third-party timeshare brokers, attorneys, or sales representatives in the timeshare, travel, real estate, or financial services industries.¹⁷ In some cases, scammers impersonate representatives of well-known U.S.-based timeshare, travel, real estate, or financial services companies. Scammers will often communicate in English and may use and reference real or fraudulent websites, business names, addresses, and registrations with government officials and trade groups in the timeshare industry to persuade victims that they are a legitimate U.S.-based company and gain their trust.¹⁸ Scammers may also exploit victims’ stolen PII and timeshare records, such as details about the property name or timeshare location, to further establish trust and credibility before beginning their initial timeshare pitch.

Initial Timeshare Pitch

After establishing trust and credibility with timeshare owners, scammers will claim to represent ready buyers, renters, or investors and then exploit victims’ trust through timeshare exit, re-rent, and investment scams.¹⁹

13. See generally *supra* note 5.

14. According to U.S. law enforcement, some telemarketers may be professional scammers, while others are hired under false pretenses but continue to work at the call centers even after realizing they are perpetrating scams.

15. Victims of timeshare fraud in Mexico are predominantly U.S. nationals. However, victims can also include Canadians and nationals of any other nations with significant tourism travel to Mexico.

16. See generally *supra* note 5.

17. See, e.g., U.S. Department of Justice (DOJ), U.S. Attorney’s Office, Eastern District of Louisiana (USAO-EDLA), “[Six Mexican Nationals Indicted in Timeshare Telemarketing Scam](#)” (Oct. 4, 2019); Indictment, [United States v. Martin Alonso Aceves Custodio, et al.](#), Case No. 2:19-cr-00202 (E.D. La. Oct. 3, 2019).

18. See generally *supra* note 5.

19. *Id.*

- *Timeshare Exit Scams* (also known as *Timeshare Resale Scams*): Scammers offer to purchase timeshares at or above market rates on behalf of ready buyers.²⁰
- *Timeshare Re-Rent Scams*: Scammers offer to rent out victims' timeshares to ready renters at or above market rates. In this variation, scammers may highlight an upcoming holiday or tourism event near the victims' timeshares to convince them that the offers are legitimate.²¹
- *Timeshare Investment Scams*: Scammers claim that the victims are entitled to supposed shares of stock associated with their timeshares and offer to broker the sale of the equity to ready investors.²²

As part of their sales pitch, scammers often provide fraudulent offer letters and other real estate or investment documents on behalf of purported buyers, renters, or investors. They also use high-pressure sales tactics, claiming that the offer is time-sensitive to convince the victims to act quickly.²³ Scammers will then request upfront "taxes" (such as capital gains and income taxes) and "fees" (such as closing costs, earnest money, escrow fees, transfer fees, maintenance fees, attorney's fees, and title insurance) that will supposedly be held in escrow and reimbursed after the transaction is finalized, to ostensibly expedite the sale.

Once the victims make the initial payments, scammers either cease contacting the victims or, more frequently, continue exploiting the victims' trust and demand additional taxes or fees to purportedly finalize the transaction.²⁴ Scammers may also provide the victims a spoofed²⁵ online bank account dashboard showing false balances to reassure the victims that the escrow account is legitimate and convince them to send additional payments. However, the timeshare interests are never actually sold or rented, and the victims never receive the supposed sale or rental proceeds. Scammers continue demanding payments until the victims either liquidate all their assets, including retirement accounts, max-out their credit accounts, or recognize the scam and cease communicating with the scammers.

Re-Victimization Through Additional Impersonation and Advance-Fee Schemes

Victims of timeshare fraud in Mexico are also at risk of being victimized again long after the initial timeshare exit, re-rent, or investment scam. These "re-victimization" schemes generally involve scammers targeting their prior victims from past timeshare fraud and using various cyber-enabled technologies to mask their identities to further deceive the victims in additional impersonation and advance-fee schemes.²⁶

20. See generally *supra* note 11.

21. See generally *supra* note 5.

22. See generally U.S. Securities and Exchange Commission (SEC), "[FBI and OIEA Warn Public that Fraudsters are Targeting Owners of Timeshares in Mexico](#)" (Sep. 17, 2020). See also [Investor.gov](#) for a search tool to verify if a broker is registered with the SEC.

23. See generally *supra* note 5.

24. *Id.*

25. According to the FBI, "spoofing is when someone disguises an email address, sender name, phone number, or website URL—to convince you that you are interacting with a trusted source." See generally FBI, [Spoofing and Phishing](#).

26. See generally *supra* note 5.

Scammers generally first reestablish contact with victims by impersonating U.S.-based law firms who have knowledge about the initial fraud and then offer to assist the victims in recovering their funds. Scammers will often say that the “timeshare fraud scammers” were identified, charged with fraud, or held civilly liable from a lawsuit in the United States or Mexico and that the victims are owed restitution in a settlement. However, the victims are then told that they must first pay supposed legal or court fees to the law firms for access to the settlement.²⁷ At the same time or afterwards, scammers may also impersonate U.S. or Mexican government authorities and demand that the victims pay additional fees to receive their funds from the settlement.

Once the victims pay these fees, scammers will then often impersonate other U.S. and Mexican government authorities, including OFAC²⁸ and Mexico’s financial intelligence unit (FIU), Unidad de Inteligencia Financiera (UIF), or international organizations such as the International Criminal Police Organization (INTERPOL), claiming that the victims’ initial payments were flagged as “suspicious” or “blocked” due to links with money laundering operations or terrorism.²⁹ Still posing as government authorities, scammers will then demand additional taxes or fees to supposedly release the funds and clear the victims’ names and will often threaten imprisonment by U.S., Mexican, or international authorities if the victims do not send funds immediately.³⁰ Revictimization scams often continue to target the same victims for many years with new variations of impersonation and advance fee schemes that prey on these victims’ emotional distress and exploit their financial losses.

Financial Typologies of Timeshare Fraud in Mexico and Associated Money Laundering

Victims of timeshare fraud schemes in Mexico generally send payments to scammers through wire transfers via U.S. correspondent banks to Mexican shell companies³¹ with accounts at Mexican banks or brokerage houses (*casas de bolsa*).³² The recipient accounts in such transactions are often relatively new and were typically opened in the preceding six months. The shell companies used are directly or indirectly controlled by the TCOs, often recently formed or registered to conduct business in Mexico, and generally appear related to the timeshare, travel, real estate, or financial services industries.³³ However, in some cases, the shell companies may appear to be in business sectors unrelated to timeshares.³⁴ Victims often send wire transfers from retirement accounts or

27. See generally *supra* note 5.

28. See generally OFAC, “[Notice of Fraudulent Communications Requesting Payments Involving OFAC](#)” (Mar. 2, 2023).

29. See generally *supra* note 5.

30. *Id.*

31. Shell companies are typically non-publicly traded corporations, limited liability companies, or other types of entities that have no physical presence beyond a mailing address, generate little to no independent economic value, and generally are created without disclosing their beneficial owners. See FinCEN, [Beneficial Ownership Information Reporting Requirements](#), 87 Fed. Reg. 59,501 (Sept. 30, 2022); see also Treasury, “[2024 National Money Laundering Risk Assessment](#)” (Feb. 2024).

32. See Secretaria de Hacienda y Credito Publico (SHCP), Comisión Nacional Bancaria y de Valores (CNBV), “[Overview of the Mexican Financial System and its AML/CFT Regulation and Supervision](#)” at p. 25; SHCP, CNBV, [Casas de Bolsa](#).

33. See generally *supra* note 11.

34. *Id.*

trust accounts held at U.S. banks, mutual fund companies, or broker-dealers, though the victims may first transfer the funds to their checking and savings accounts before wiring the funds to Mexico.

Once the timeshare fraud payments are wired to the shell companies in Mexico, scammers will further obfuscate the ill-gotten funds through bank transfers to additional Mexican shell companies and trusts (*fideicomisos*) that the TCOs control either directly or indirectly through cartel members, family members, or third-party money launderers, including complicit accountants and other professionals. The TCOs will then use those Mexican shell companies and trusts to send bank transfers or withdrawal cash to either (1) finance drug trafficking operations and make payments to cartel members or (2) purchase luxury real estate or construct timeshare resorts in Mexico to use in future timeshare fraud schemes, particularly in resort towns, including Puerto Vallarta and the surrounding area.³⁵

Case Study

Six Mexican Nationals Indicted in Timeshare Telemarketing Scam

Six Mexican nationals were indicted on October 3, 2019, by a federal grand jury for one count of conspiracy to commit wire fraud in the U.S. District Court for the Eastern District of Louisiana. The indictment alleges that from at least January 1, 2016, to the indictment date, the defendants conspired together and with others to commit wire fraud in connection with a telemarketing scheme that targeted and victimized persons in the United States, Canada, and South America. As part of the elaborate scheme, the conspirators made unsolicited phone calls to owners of resort timeshare properties to induce them to pay fees associated with the bogus sale of their property. The defendants misrepresented the existence of a buyer for their timeshare and solicited money from the victims to facilitate the sale. They solicited the timeshare owners to enter into agreements to sell their timeshares and pay for alleged “closing costs” with electronic wire transfers from banking institutions within the United States to Mexican banks. There were no interested buyers, the closings did not occur, and the timeshares were not resold. Instead, the conspirators simply pocketed the advanced fees. Of the U.S. victims, 40 were age 60 and older, and the total estimated loss is at least \$10 million. The defendants, who are all based in Mexico, operated under the business names Planet Travel and Newport International Investments, and at other times used the following business names: Advance Travel INC, All American Real Estate, American International Investment Group, Bear Claw Travel, Best Investment Services, Champion Properties, Closing Source LLC, Equity Closing Services Group, Global Offshore Services, NSC Holding, Peach Title, Sandia Title, Travel and Acquisitions, Travel Innovations, Travel Plus Acquisitions, Travel Right, and World Travelers, Inc.³⁶

35. See generally *supra* note 11.

36. See generally DOJ, USAO-EDLA, “[Six Mexican Nationals Indicted in Timeshare Telemarketing Scam](#)” (Oct. 4, 2019); Indictment, [United States v. Martin Alonso Aceves Custodio, et al.](#), Case No. 2:19-cr-00202 (E.D. La. Oct. 3, 2019); see also DOJ, USAO-EDLA, “[Two Mexican Nationals Plead Guilty to Timeshare Telemarketing Scam](#)” (June 17, 2020); DOJ, USAO-EDLA, “[Mexican National Sentenced to 18 Months for Timeshare Telemarketing Scam](#)” (Sept. 17, 2020); DOJ, USAO-EDLA, “[Two More Mexican Nationals Are Sentenced After Pleading Guilty to International Timeshare Telemarking Scam](#)” (Sept. 30, 2021).

Treasury Sanctions Puerto Vallarta-Based Accountants Assisting CJNG Timeshare Fraud

Building on the three actions taken in 2023, on July 16, 2024, OFAC sanctioned additional Mexican individuals and companies pursuant to E.O. 14059 that are linked, directly or indirectly, to CJNG's timeshare activities. These individuals and entities are located in Puerto Vallarta, Jalisco, Mexico, which is a CJNG strategic stronghold for drug trafficking and various other illicit activities.

OFAC sanctioned Mexican accountants **Griselda Margarita Arredondo Pinzon (Arredondo)**, **Xeyda Del Refugio Foubert Cadena (Foubert)**, and **Emiliano Sanchez Martinez (Sanchez)** pursuant to E.O. 14059 for being owned, controlled, or directed by, or having acted or purported to act for on behalf of, directly or indirectly, CJNG, a person sanctioned pursuant to E.O. 14059. These Puerto Vallarta-based accountants assist CJNG's timeshare fraud activities and have familial relationships with previously designated persons. Arredondo is the half-sister of senior CJNG member Julio Cesar Montero Pinzon (a.k.a. "El Tarjetas"), whom OFAC designated pursuant to E.O. 14059 on [June 2, 2022](#). Foubert is Sanchez's spouse and is the sister of Manuel Alejandro Foubert Cadena, a Mexican attorney linked to CJNG's timeshare activities and whom OFAC designated on November 30, 2023.

OFAC also sanctioned four Mexican companies pursuant to E.O. 14059. OFAC sanctioned **Constructora Sandgris, S. de R.L. de C.V.**—purported to be engaged in wholesale trade—for being owned, controlled, or directed by, or having acted or purported to act for or on behalf of, directly or indirectly, Arredondo, a person sanctioned pursuant to E.O. 14059. Additionally, OFAC sanctioned **Pacific Axis Real Estate, S.A. de C.V. and Realty & Maintenance BJ, S.A. de C.V.**—purported to be engaged in real estate activities—for being owned, controlled, or directed by, or having acted or purported to act for or on behalf of, directly or indirectly, Foubert, a person sanctioned pursuant to E.O. 14059. Finally, OFAC sanctioned **Bona Fide Consultores FS S.A.S.**, an accounting firm, for being owned, controlled, or directed by, or having acted or purported to act for or on behalf of, directly or indirectly, Sanchez, a person sanctioned pursuant to E.O. 14059.³⁷

Red Flag Indicators

FinCEN has identified the following red flag indicators to help detect, prevent, and report potential suspicious activity related to timeshare fraud in Mexico. Because no single red flag is determinative of illicit or other suspicious activity, financial institutions should consider the surrounding facts and circumstances, such as a customer's historical financial activity, whether the transactions are in line with prevailing business practices, and whether the customer exhibits multiple red flags before determining if a behavior or transaction is suspicious or otherwise indicative of timeshare fraud in Mexico.

37. See generally Treasury, "[Treasury Sanctions Cartel Accountants, Announces Joint Notice on Timeshare Fraud in Mexico](#)" (July 16, 2024).

Behavioral and Financial Red Flags of Victims of Timeshare Fraud in Mexico

- 1 A customer is uncharacteristically wiring funds to Mexico and indicates the need to send the funds immediately to pay “taxes” or “fees” to apparent timeshare brokers or else risk losing an urgent financial opportunity regarding their timeshare.
- 2 A customer is uncharacteristically sending international wire transfers from retirement accounts or trust accounts to Mexican financial institutions directly or by first sending the funds to their personal checking or savings accounts either through an internal transfer within their financial institution or by a wire transfer to their accounts held at another financial institution and then immediately wiring the funds to Mexico.
- 3 A customer is sending multiple, structured, or repetitive wire transfers to Mexican financial institutions with the same memo line denoting “taxes” or “fees” regarding a timeshare.
- 4 A customer suddenly begins sending an unusual volume of wire transfers to Mexican banks or brokerage houses despite no previous related transaction activity.

Red Flags of Counterparties Involved in Timeshare Fraud in Mexico

- 5 A counterparty in a transaction is a new or recently formed or registered Mexican company in the timeshare, travel, real estate, or financial services industries with minimal to no online presence.
- 6 A counterparty in a transaction is a new or recently formed or registered Mexican company that has indicators of being a shell company used for illicit activity.
- 7 A counterparty in a transaction is a new or recently formed or registered Mexican company with an account opened within the previous six months at a Mexican bank or brokerage house.
- 8 A counterparty in a transaction is a new or recently formed or registered Mexican company that is receiving repeated, or an unusual volume of, wire transfers from U.S. personal bank accounts, retirement accounts, or trust accounts with memo lines describing “taxes” or “fees” regarding timeshares in Mexico.
- 9 A counterparty in a transaction is a new or recently formed or registered Mexican company that appears to do business in the timeshare industry but has previously done business as a company whose name is associated with complaints by consumer protection and law enforcement agencies.³⁸

38. See Indictment, *United States v. Martin Alonso Aceves Custodio, et al.*, Case No. 2:19-cr-00202 (E.D. La. Oct. 3, 2019), at p. 4.

- 10 A counterparty in a transaction is a Mexican company with beneficial owners associated with timeshare fraud or drug-related U.S. Department of Justice (DOJ) indictments or OFAC designations.

Increasing Information Sharing Relating to Timeshare Fraud in Mexico

Information sharing among financial institutions is critical to identifying, reporting, and preventing timeshare fraud in Mexico or other specified unlawful activities that apply to a money laundering offense. U.S. financial institutions and associations of U.S. financial institutions sharing information under the safe harbor authorized by section 314(b) of the USA PATRIOT Act are reminded that they may share information with each other regarding individuals, entities, organizations, and countries for purposes of identifying, and, where appropriate, reporting activities that may involve possible terrorist activity or money laundering.³⁹ FinCEN strongly encourages such voluntary information sharing as it relates to money laundering or possible terrorist financing in connection with timeshare fraud in Mexico or other specified unlawful activities.

Given the transnational nature of illicit activity related to timeshare fraud in Mexico, FinCEN also encourages U.S. financial institutions to continue to use, and potentially expand, their existing processes to collect and share information with foreign financial institutions in furtherance of investigations that involve cross-border activity.⁴⁰ FinCEN also reminds U.S. financial institutions that the sharing of underlying account or transaction information does not violate Suspicious Activity Report (SAR) confidentiality restrictions in the BSA and FinCEN's regulations unless such sharing would potentially reveal the existence of a SAR.⁴¹

Reporting Timeshare Fraud in Mexico to U.S. Law Enforcement and Recovering Funds

In addition to filing a SAR when appropriate, financial institutions are encouraged to refer their customers who may be victims of timeshare fraud in Mexico to file a complaint with the FBI's [IC3](#). Victims and financial institutions can report suspected timeshare fraud by contacting their nearest [FBI field office](#). In the case of older victims of timeshare fraud in Mexico, financial institutions may also refer their customers to DOJ's [National Elder Fraud Hotline](#) at 833-FRAUD-11 or 833-372-8311.

39. See generally FinCEN, "[Section 314\(b\) Fact Sheet](#)" (Dec. 2020); 31 CFR § 1010.540.

40. See, e.g., FinCEN, "[Prepared Remarks of FinCEN Director Andrea Gacki During the SIFMA AML Conference](#)" (May 6, 2024).

41. See, e.g., 31 CFR § 1020.320(e) (noting that the prohibition from disclosing SARs, or any information that would reveal the existence of a SAR, explicitly does not include "[t]he underlying facts, transactions, and documents upon which a SAR is based..."). The final rule on the Confidentiality of Suspicious Activity Reports stated that "[d]ocuments that may identify suspicious activity, but that do not reveal whether a SAR exists (e.g., a document memorializing a customer transaction such as an account statement indicating a cash deposit or a record of a funds transfer), should be considered as falling within the underlying facts, transactions, and documents upon which a SAR is based, and need not be afforded confidentiality." See FinCEN, [Confidentiality of Suspicious Activity Reports](#), 75 Fed. Reg. 75595 (Dec. 3, 2010).

A victim of cyber-enabled fraud, including timeshare fraud in Mexico, or the victim's financial institution, is encouraged to file a complaint with federal law enforcement to activate FinCEN's Rapid Response Program (RRP), which is a globally collaborative program to interdict fraudulently stolen funds. The RRP is a partnership with FinCEN, U.S. law enforcement (including the FBI, the U.S. Secret Service, Homeland Security Investigations, and the U.S. Postal Inspection Service), and foreign partner agencies that, like FinCEN, are the FIUs of their respective jurisdictions, including Mexico's UIF. FinCEN uses its authority to share financial intelligence rapidly with counterpart FIUs and encourages foreign authorities to interdict the fraudulent transactions, freeze funds, and stop and recall payments using their authorities under their own respective legal and regulatory frameworks. The RRP has been used to combat fraud involving over 88 foreign jurisdictions and has the capacity to reach more than 160 foreign jurisdictions through FIU-to-FIU channels. Through these collaborative efforts, FinCEN has successfully assisted in the freezing of over \$1.4 billion. For more information, please see FinCEN's [Fact Sheet on the Rapid Response Program](#).

Additional resources for victims of timeshare fraud in Mexico can be found at [FBI's victim resources webpage](#).

Reminder of Relevant BSA Obligations and Tools for U.S. Financial Institutions

*Suspicious Activity Reporting
Law Enforcement Filing Tips
Other Relevant BSA Reporting*

Suspicious Activity Reporting

A financial institution is required to file a SAR if it knows, suspects, or has reason to suspect a transaction conducted or attempted by, at, or through the financial institution involves funds derived from illegal activity; is intended or conducted to disguise funds derived from illegal activity; is designed to evade regulations promulgated under the BSA; lacks a business or apparent lawful purpose; or involves the use of the financial institution to facilitate criminal activity.⁴² All statutorily defined financial institutions may voluntarily report suspicious transactions under the existing suspicious activity reporting safe harbor.⁴³

When a financial institution files a SAR, it is required to maintain a copy of the SAR and the original or business record equivalent of any supporting documentation for a period of five

42. See 31 CFR §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, 1030.320.

43. See 31 U.S.C. § 5318(g)(3). Financial institutions may report suspicious transactions regardless of amount involved and still take advantage of the safe harbor.

years from the date of filing the SAR.⁴⁴ Financial institutions must provide any requested documentation supporting the filing of a SAR upon request by FinCEN or an appropriate law enforcement or supervisory agency.⁴⁵ When requested to provide supporting documentation, financial institutions should take special care to verify that a requestor of information is, in fact, a representative of FinCEN or an appropriate law enforcement or supervisory agency. A financial institution should incorporate procedures for such verification into its BSA compliance or AML program. These procedures may include, for example, independent employment verification with the requestor's field office or face-to-face review of the requestor's credentials.

SAR Filing Instructions

SARs, and compliance with other BSA requirements, are crucial to identifying and stopping timeshare fraud schemes in Mexico. FinCEN requests that financial institutions indicate a connection between the suspicious activity being reported and the activities highlighted in this joint Notice by including the key term “**FIN-2024-NTC2**” in SAR field 2 (Filing Institution Note to FinCEN), as well as in the narrative. Financial institutions may highlight additional advisory, alert, or notice keywords in the narrative, if applicable.

Financial institutions should select SAR field 34(z) (Fraud – Other) as the associated suspicious activity type and include the term “**TimeshareMX**” in the text box. Financial institutions also should select all other relevant suspicious activity fields, such as those in SAR fields 36 (Money Laundering) and 38 (Other Suspicious Activities), if applicable.

Financial institutions should include all available information relating to the account(s) and location(s) involved in the reported activity, identifying information and descriptions of any legal entities or arrangements involved and associated beneficial owners, and any information about related persons or entities involved in the activity. Financial institutions also should provide all available information regarding other domestic and foreign financial institutions involved in the activity; where appropriate, financial institutions should consider filing a SAR jointly on shared suspicious activity.⁴⁶

Law Enforcement Filing Tips for SARs on Timeshare Fraud in Mexico

FinCEN notes that the tips below are best practices regarding filing a SAR for suspected timeshare fraud in Mexico and do not represent supervisory expectations or regulatory obligations:

- Provide a justification for why the financial institution is filing the SAR (e.g., the financial institution suspects the customer is a victim of timeshare fraud in Mexico).

44. See 31 CFR §§ 1020.320(d), 1021.320(d), 1022.320(c), 1023.320(d), 1024.320(c), 1025.320(d), 1026.320(d), 1029.320(d), 1030.320(d).

45. *Id.*; see also FinCEN, “[Suspicious Activity Report Supporting Documentation](#)” (June 13, 2007).

46. See 31 CFR §§ 1020.320(e)(1)(ii)(A)(2)(i), 1021.320(e)(1)(ii)(A)(2)), 1022.320(d)(1)(ii)(A)(2), 1023.320(e)(1)(ii)(A)(2)(i), 1024.320(d)(1)(ii)(A)(2), 1025.320(e)(1)(ii)(A)(2), 1026.320(e)(1)(ii)(A)(2)(i), 1029.320(d)(1)(ii)(A)(2), 1030.320(d)(1)(ii)(A)(2).

- Do not include a victim's information as the subject of the SAR.
- Include a victim's information (including contact information) in the SAR narrative.
- Provide a statement in the SAR narrative documenting the age and location (county/city) of the target or victim. Provide details about the reporting entity's response, *e.g.*, whether accounts were closed, whether the person was warned that transactions appear to involve fraud, if the person was not permitted to conduct new transactions, etc.
- Provide details about the amounts involved and whether any amounts were refunded to the customer (as of the submission date of the SAR).
- Expedite responses to law enforcement requests for SAR supporting documents.
- Clearly lay out all accounts and beneficiaries the funds were wired to in the SAR narrative.
- Take advantage of the law enforcement contact field to indicate if the suspicious activity was also reported to law enforcement or Adult Protective Services, as well as the name and phone number of the contact person.
- Provide direct liaisons or points of contact at the reporting entity related to the SAR so investigators can ask questions and request additional documentation in a timely manner.

Other Relevant BSA Reporting Requirements

Financial institutions and other entities or persons may also have other relevant BSA reporting requirements to provide information in connection with the subject of this joint Notice. These include obligations related to the Currency Transaction Report (CTR),⁴⁷ Report of Cash Payments Over \$10,000 Received in a Trade or Business (Form 8300),⁴⁸ Report of Foreign Bank and Financial Accounts (FBAR),⁴⁹ Report of International Transportation of Currency or Monetary Instruments (CMIR),⁵⁰ Registration of Money Services Business (RMSB),⁵¹ and Designation of Exempt Person (DOEP).⁵² These standard reporting

47. A report of each deposit, withdrawal, exchange of currency, or other payment or transfer, by, through, or to a financial institution that involves a transaction in currency of more than \$10,000. Multiple transactions may be aggregated when determining whether the reporting threshold has been met. *See* 31 CFR §§ 1010.310-313, 1020.310-313, 1021.310-313, 1022.310-313, 1023.310-313, 1024.310-313, and 1026.310-313.
48. A report filed by a trade or business that receives currency in excess of \$10,000 in one transaction or two or more related transactions. The transactions are required to be reported on a joint FinCEN/Internal Revenue Service form when not otherwise required to be reported on a CTR. *See* 31 CFR §§ 1010.330-331. A Form 8300 also may be filed voluntarily for any suspicious transaction, even if the total amount does not exceed \$10,000.
49. A report filed by a U.S. person that has a financial interest in, or signature or other authority over, foreign financial accounts with an aggregate value exceeding \$10,000 at any time during the calendar year. *See* 31 CFR § 1010.350; FinCEN Form 114.
50. A form filed to report the transportation of more than \$10,000 in currency or other monetary instruments into or out of the United States. *See* 31 CFR § 1010.340.
51. A form filed to register a money services business (MSB) with FinCEN, or to renew such a registration. *See* 31 CFR § 1022.380.
52. A report filed by banks to exempt certain customers from currency transaction reporting requirements. *See* 31 CFR § 1010.311.

requirements may not have an obvious connection to illicit finance, but may ultimately prove highly useful to law enforcement.

Form 8300 Filing Instructions

When filing a Form 8300 involving a suspicious transaction relevant to this joint Notice, FinCEN requests that the filer select *Box 1b* (“suspicious transaction”) and include the key term “FIN-2024-NTC2” in the “*Comments*” section of the report.

Due Diligence

Banks, brokers or dealers in securities, mutual funds, and futures commission merchants and introducing brokers in commodities (FCM/IBs) are required to have appropriate risk-based procedures for conducting ongoing customer due diligence that include, but are not limited to: (i) understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and (ii) conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information.⁵³ Covered financial institutions are required to identify and verify the identity of beneficial owners of legal entity customers, subject to certain exclusions and exemptions.⁵⁴ Among other things, this facilitates the identification of legal entities that may be owned or controlled by foreign politically exposed persons (PEPs).

Senior foreign political figures and due diligence obligations for private banking accounts

In addition to these due diligence obligations, under section 312 of the USA PATRIOT Act (31 U.S.C. § 5318(i)) and its implementing regulations, covered financial institutions must implement due diligence programs for private banking accounts held for non-U.S. persons that are designed to detect and report any known or suspected money laundering or suspicious activity conducted through or involving such accounts.⁵⁵ Covered financial institutions must establish risk-based controls and procedures for ascertaining the identities of nominal and beneficial owners of such accounts and ascertaining whether any of these owners are senior foreign political figures, and for conducting enhanced scrutiny on accounts held by senior foreign political figures that is reasonably designed to detect and report transactions that may involve the proceeds of foreign corruption.⁵⁶

53. See 31 CFR §§ 1020.210(a)(2)(v), 1023.210(b)(5), 1024.210(b)(6), 1026.210(b)(5).

54. See 31 CFR §§ 1010.230, 1010.650(e)(1) (defining “covered financial institution”).

55. See 31 CFR § 1010.620. The definition of “covered financial institution” is found in 31 CFR § 1010.605(e)(1). The definition of “private banking account” is found in 31 CFR § 1010.605(m). The definition of “non-U.S. person” is found in 31 CFR § 1010.605(h).

56. See 31 CFR § 1010.620(c).

AML/CFT program and correspondent account due diligence requirements

Financial institutions are reminded of AML/CFT program requirements,⁵⁷ and covered financial institutions are reminded of correspondent account due diligence requirements under Section 312 of the USA PATRIOT Act (31 U.S.C. § 5318(i)) and implementing regulations.⁵⁸ As described in FinCEN Interpretive Release 2004-1, the AML/CFT program of a money services business (MSB) must include risk-based policies, procedures, and controls designed to identify and minimize risks associated with foreign agents and counterparties.⁵⁹

For Further Information

FinCEN's website at www.fincen.gov contains information on how to register for FinCEN Updates. Questions or comments regarding the contents of this joint Notice should be addressed to the FinCEN Regulatory Support Section at frc@fincen.gov.

The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit use, combat money laundering and its related crimes including terrorism, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.

57. See 31 CFR §§ 1010.210, 1020.210, 1021.210, 1022.210, 1023.210, 1024.210, 1025.210, 1026.210, 1027.210, 1028.210, 1029.210, 1030.210.

58. See 31 CFR § 1010.610.

59. See FinCEN, [Anti-Money Laundering Program Requirements for Money Services Businesses with Respect to Foreign Agents or Foreign Counterparties](#), Interpretive Release 2004-1, 69 Fed. Reg. 74,439 (Dec. 14, 2004). See also FinCEN, [“Guidance on Existing AML Program Rule Compliance Obligations for MSB Principals with Respect to Agent Monitoring”](#) (Mar. 11, 2016).