Compliance Conversations
ProBank Education Services

July 20, 2026

Compliance Conversations

ProBank Education Services

Presenters

Mark Burnside, CRCM

Director, Kentucky

Mark Dever, AAP, CAMS

Director, Kentucky

ECOA Final Rule – April 22, 2026 – Effective date July 21, 2026

- On April 22, 2026, the Consumer Financial Protection Bureau issued a final rule that amends provisions related to disparate impact under Regulation B. The agency states:
- **Disparate Impact**: Explicitly states that ECOA does not authorize disparate impact liability. Historically, federal agencies could rely on an "effects test," where neutral lending practices could be deemed discriminatory if they disproportionately harmed protected groups. The new rule states that enforcement requires proof of intentional discrimination.
- **Discouragement**: Limits "discouragement" to instances of "overt" discouragement of an applicant where specific, objective oral or written statements directed at applicants or prospective applicants are made and where "intent" to discourage is evident. (The creditor knew their statement would communicate discriminatory outcomes.)
- **Special Purpose Credit Programs (SPCP)**: For-profit SPCPs cannot use race, color, national origin, or sex as program eligibility criteria. Requires institutions to provide evidence that a participant would have been denied credit in the absence of the program
- 91 FR 21620 – 21670 (04/22/2026)

ECOA (Small Business Lending – 1071)
Final Rule May 1, 2026 – Effective June 30, 2026

- Raises the origination threshold for being a “covered financial institution” to 1,000 covered credit originations (from 100) in each of the two preceding calendar years (excludes Farm Credit System (FCS) lenders from coverage altogether).
- Lowers the gross annual revenue threshold in the definition of “small business” from $5 million or less to $1 million or less.
- Adds three new categories of transactions to the list of “excluded transactions” that do not require data reporting:
  - Merchant cash advances (MCAs). Agreements where a small business receives a lump-sum payment in exchange for the right to receive a percentage of the small business’ future sales or income up to a certain amount.
  - Agricultural lending. Lending to fund production of crops, fruits, vegetables, and livestock, or the purchase or refinance of capital assets such as farmland, machinery and equipment, breeder livestock, and farm real estate improvements.
  - Small dollar business credit. Credit in an amount of $1,000 or less, subject to inflation adjustment.
- Eliminates several discretionary data points: (1) application method, (2) application recipient, (3) denial reasons, (4) pricing information, and (5) number of workers.
- Revises the format for collecting demographic information about principal owners and the business ownership status.
- 91 FR 23530 – 23626 (05/01/2026)

CFPB Statement on Ability to Repay and Immigration Status – June 8, 2026

- "[A] creditor's awareness of a consumer's immigration status may implicate a creditor's reasonable expectations about whether a consumer's income from U.S.-based employment will remain available for repayment. For example, a creditor may regard a credit applicant who is neither lawfully present nor permitted to work in the United States as being subject to removal, in light of the Administration's stated policy of removing any person unlawfully present in the United States. Indications that an individual may not be lawfully present, and therefore may be at risk of removal, may come from various sources, including direct inquiry or the consumer's reliance on atypical identification methods, such as an Individual Taxpayer Identification Number (ITIN), typically issued to taxpayers to individuals who lack proof of legal residency.

- To the extent a creditor's information regarding the borrower's immigration status indicates that the borrower may be an unlawfully present individual and removed from the United States, there is a danger that removal would render any such borrower unable to earn income derived from employment that requires physical presence in the United States. Accordingly, considering whether information regarding an applicant's immigration status indicates a reasonably expected change in future income is a matter of sound compliance practice. The Bureau expects compliance with the law and failure to account for such a reasonably expected change in income may not comply with a creditor's obligation to reasonably assess a borrower's ability to repay the loan or line of credit sought."
- 91 FR 34607 – 34609 (06/08/2026)

CFPB Statement on Ability to Repay and Immigration Status (cont.)

- "Of course, there are a wide variety of lawful immigration statuses in the United States. Assessing how each status might bear on a lender's reasonable expectation that a consumer has the ability to repay an obligation with U.S.-based employment income is varied, and it cannot be assumed that consumers with different lawful statuses have identical abilities to repay. Accordingly, the Bureau cannot, and does not, provide a comprehensive analysis of variations in immigration status and the consequent reasonable expectations as to a consumer's ability to repay a loan through expected income from U.S.-based employment. Rather, the Bureau reminds creditors when future changes in borrower income must be considered under Regulation Z.

- Regulation Z enables lenders to make these judgments by affirming their ability to lawfully consider the consumer's immigration status, lawful presence, authorization to work, and other factors that may indicate risk of removal insofar as it bears on their current or reasonably expected income from U.S.-based employment."

Compliance Conversations
ProBank Education Services

The FDIC is inviting public comment on a proposed rule that would amend the assessment regulations in 12 CFR Part 327 – Comment Period Closes 08/31/2026

- *The Federal Deposit Insurance Corporation (FDIC), is soliciting comments on a proposal that would update the $10 billion asset threshold in the definitions of small and large institutions to $30 billion and adjust the threshold every four years to reflect inflation.*

- The proposed rule would also, if enacted, decrease initial base deposit insurance assessment rate schedules by 2 basis points for small institutions and by 1 basis point for large and highly complex institutions, provide a downward resolution readiness adjustment to assessment rates for large and highly complex institutions, and remove obsolete provisions from 12 CFR Part 327.

- 91 FR 39794 – 39838 (06/30/2026)

Compliance Conversations
ProBank Education Services

The FDIC is inviting public comment on a proposed rule that would update, clarify, and supplement the FDIC's disclosure of confidential information by the FDIC and other parties – Comment Period Closes 08/31/2026

- *The Federal Deposit Insurance Corporation (FDIC), is soliciting comments on a proposal that would enhance the ability of insured depository institutions to share confidential information with affiliates and certain other entities for appropriate business purposes without seeking prior authorization from the FDIC.*
- The proposed rule would also significantly simplify and clarify the requirements and restrictions applicable to the FDIC's discretionary disclosure of confidential information and would update and simplify the FDIC's rules regarding disclosures under the Freedom of Information Act (FOIA).
- 91 FR 39726 – 39752 (06/30/2026)

The FDIC is inviting public comment on a proposed rule that would revise its regulations that require resolution submissions by insured depository institutions (IDIs) with at least $50 billion in total assets. – Comment Period Closes 08/31/2026

- *The Federal Deposit Insurance Corporation (FDIC), is soliciting comments on a proposal that would modify the current rule by raising and automatically updating the dollar threshold that determines the scope of applicability.*

- The proposed rule would also reduce the requirements regarding the content of resolution submissions provided to the FDIC, with a focus on information that most directly supports the FDIC's resolution readiness in the event of material distress and failure of a covered IDI

- 91 FR 39546 – 39568 (06/30/2026)

The OCC Request Comments on Proposal to Implement Certain Requirements pursuant to the GENIUS Act – Comment Period Closes 07/24/2026

- *The Office of the Comptroller (OCC), is soliciting comments on a proposal that would implement certain requirements pursuant to the Guiding and Establishing National Innovation for U.S. Stablecoins (GENIUS) Act pertaining to appropriate Bank Secrecy Act (BSA) and sanctions compliance standards for permitted payment stablecoin issuers (PPSIs) subject to the OCC's jurisdiction.*

- The proposed rule would add a new paragraph (c) in Part 15, of the March 02, 2026, proposed rule which if enacted, would require PPSIs to comply with the BSA Sections 4(a)(5) and 4(a)(6)(B) of the GENIUS Act, and applicable regulations at 31 CFR chapters V and X, including any AML/CFT programs, sanctions programs, and reporting requirements.

- 91 FR 37840 – 37848 (06/24/2026)

The “Agencies” Request Comments on Proposal to Implement Certain Requirements pursuant to the GENIUS Act – Comment Period Closes 08/21/26

- *The Financial Crimes Enforcement Network (FinCEN), Federal Deposit Insurance Corporation (FDIC) Office of the Comptroller (OCC), Federal Reserve System (FRB), and the National Credit Union Administration (NCUA) are soliciting comments on a proposal that would implement certain requirements pursuant to the Guiding and Establishing National Innovation for U.S. Stablecoins (GENIUS) Act.*

- The proposed rule would treat permitted payment stablecoin issuers (PPSIs) as financial institutions under the Bank Secrecy Act and require PPSIs to maintain an effective customer identification program.

- 91 FR 37234 – 18272 (06/22/2026)

The FDIC is issuing a proposed rule to implement provisions of the Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act). Comment Period Closes August 04, 2026.

- *Specifically, this proposal would implement the appropriate Bank Secrecy Act (BSA) and sanctions compliance standards applicable to FDIC-supervised permitted payment stablecoin issuers (PPSI).*

- The proposed rule aims to establish appropriate principles-based BSA and sanctions compliance requirements that are tailored to the business model and risk profile of PPSIs and consistent with applicable law, which includes requirements promulgated by FinCEN and OFAC. The FDIC believes the proposed rule would establish supervisory expectations for PPSIs, help combat illicit finance risk, and continue to support the responsible growth and use of digital assets and related technologies in the banking sector.

- 91 FR 34171 – 34178 (06/05/2026)

ProBank Education Services

The NCUA is issuing a supplemental proposed rule to implement provisions of the Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act). Comment Period Closes July 17, 2026.

- *Specifically, this proposal supplements the proposal issued in February 2026.*
- The supplemental proposal would govern the issuance of Payment Stablecoins and certain related activities by entities subject to the NCUA's jurisdiction. This supplemental proposal would also make amendments to address share insurance coverage, tokenized shares, and other conforming and clarifying amendments.
- 91 FR 28956 – 29035 (05/18/2026)

Compliance Conversations
ProBank Education Services

The Financial Stability Board has issued a set of proposed “Sound Practices for Responsible Adoption of Artificial Intelligence (AI)." The Comment Period Closes July 22, 2026.

- *Specifically, this proposal identifies sound practices to help all types of financial institutions navigate benefits and risks responsibly as they adopt AI.*

- Financial institutions are rapidly adopting, using, and innovating with AI to reap efficiency gains, transform their business models, improve the services offered to clients, and enhance risk management capabilities. The significant benefits that can arise from AI adoption, however, usually come with additional risks. Managing these risks well will promote sustained value creation by financial institutions through AI adoption.

- https://www.fsb.org/2026/06/sound-practices-for-responsible-adoption-of-artificial-intelligence-ai-consultation-report/

Compliance Conversations
ProBank Education Services

The FFIEC has issued a proposal to revise the Uniform Financial Institutions Rating System (UFIRS), commonly referred to as the CAMELS rating system. The Comment Period Closes August 17, 2026.

- *Specifically, this proposal would strengthen the link between CAMELS ratings and an institution's safety and soundness.*
- The proposal seeks to focus component and composite ratings on factors that materially affect an institution's financial condition and risk profile, and to improve the transparency of CAMELS ratings.
- 91 FR 29128 – 29139 (05/19/2026)

Compliance Conversations

ProBank Education Services

BSA/AML and Financial Crime Trends

FinCEN Supplemental Alert –

Fuel Smuggling and Tax Evasion Schemes on the Southern Border Associated with Mexico-Based Cartels

FinCEN Advisory –

Non-Work Authorized Populations and Their Employers and Risks to the Integrity of the U.S. Financial System

FinCEN Notice –

Threat of Human Trafficking During the 2026 FIFA World Cup

FinCEN Alert –

Use of Front Companies, Financial Facilitators, and Digital Asset Infrastructure by Iran's IRGC to Evade Sanctions and Launder Proceeds

Updated Section 311 "designee" – Huione Group – H-Pay Service PLC and any successor entity

Latest FATF listing of "jurisdictions under Increased Monitoring (*e.g.*, the "grey list")

Updated 314(b) Guidance

"Introduction to OFAC" Guide & "Reconsideration" Portal

2026 SAR Activity Distribution - 1st Quarter
565,135 // 1,043,051 (+ 7.28 % // + 6.79%)
https://www.fincen.gov/reports/sar-stats

1	Transaction with No Apparent Economic, Business, or Lawful Purpose	159,449	9.57%
2	Suspicion Concerning the Source of Funds	156,741	9.41%
3	Suspicious EFT/Wire Transfers	150,266	9.02%
4	Transaction(s) Below CTR Threshold	147,702	8.87%
5	Suspicious use of multiple transaction locations	113,932	6.84%
6	Check	104,914	6.30%
7	Transaction Out of Pattern for Customer(s)	93,673	5.62%
8	Credit/Debit Card	82,748	4.97%
9	Other Fraud (Type)	61,206	3.67%
10	ACH	58,258	3.50%
11	Suspicious Use of Multiple Accounts	58,062	3.49%
12	Identity Theft	52,400	3.15%

2026 SAR Activity Distribution - 1st Quarter
565,135 // 1,043,051 (+ 7.28 % // + 6.79%)
https://www.fincen.gov/reports/sar-stats

13	Counterfeit Instrument	44,262	2.66%
14	Wire	38,165	2.29%
15	Elder Financial Exploitation	38,084	2.29%
16	Two or More Individuals Working Together	37,234	2.24%
17	Other Hovione Suspicious Activities	29,688	1.78%
18	Suspicious Use of Noncash Monetary Instruments	25,238	1.52%
19	Account Takeover	23,864	1.43%
20	Other Money Laundering	23,418	1.41%
21	Consumer Loan	20,826	1.25%
22	Provided Questionable or False Documentation	20,711	1.24%
23	Transaction(s) Involving Foreign High-Risk Jurisdiction	17,092	1.03%
24	Forgeries	16,484	0.99%

2026 SAR Activity Distribution - 1st Quarter
565,135 // 1,043,051 (+ 7.28 % // + 6.79%)
https://www.fincen.gov/reports/sar-stats

25	Mass-Marketing	12,116	0.73%
26	Funnel Account	8,896	0.53%
27	Against Financial Institution Customer(s)	8,241	0.49%
28	Alters or Cancels Transaction to Avoid CTR Requirement	6,422	0.39%
29	Provided Questionable or False Identification	5,852	0.35%
30	Transaction(s) Below BSA Recordkeeping Threshold	4,948	0.30%
31	Mail	4,259	0.26%
32	Refused or Avoided Request for Documentation	3,411	0.20%
33	Suspicious Receipt of Government Payments/Benefits	3,366	0.20%
34	Embezzlement/Theft/Disappearance of Funds	2,738	0.16%
35	Other Gaming Activities	2,662	0.16%
36	Little or No Concern for Product Performance Penalties, Fees, or Tax Consequences	2,392	0.14%

2026 SAR Activity Distribution - 1st Quarter
565,135 // 1,043,051 (+ 7.28 % // + 6.79%)
https://www.fincen.gov/reports/sar-stats

41	Other Cyber Event	1,517	0.09%
45	Unlicensed or Unregistered MSB	1,262	0.08%
47	Human Trafficking	995	0.06%
50	Healthcare/Public or Private Health Insurance	892	0.05%
52	Business Loan	865	0.05%
53	Against Financial Institution(s)	851	0.05%
63	Ponzi Scheme	107	0.01%
64	Known or Suspected Terrorist/Terrorist Organization	97	0.01%
69	Suspected Public/Private Corruption (Domestic)	82	0.00%
70	Suspected Public/Private Corruption (Foreign)	63	0.00%
72	Human Smuggling	57	0.00%
73	Other Terrorist	54	0.00%
74	Pyramid Scheme	35	0.00%

FinCEN ALERT

FIN-2026-Alert003

June 30, 2026

FinCEN Supplemental Alert on Fuel Smuggling and Tax Evasion Schemes on the Southern Border Associated with Mexico-Based Cartels

Suspicious Activity Report (SAR) Filing Request:

FinCEN requests that financial institutions reference this supplemental Alert in SAR field 2 (Filing Institution Note to FinCEN) and the narrative by including the key term **"FIN-2026-FISCALFUELTHEFT."**

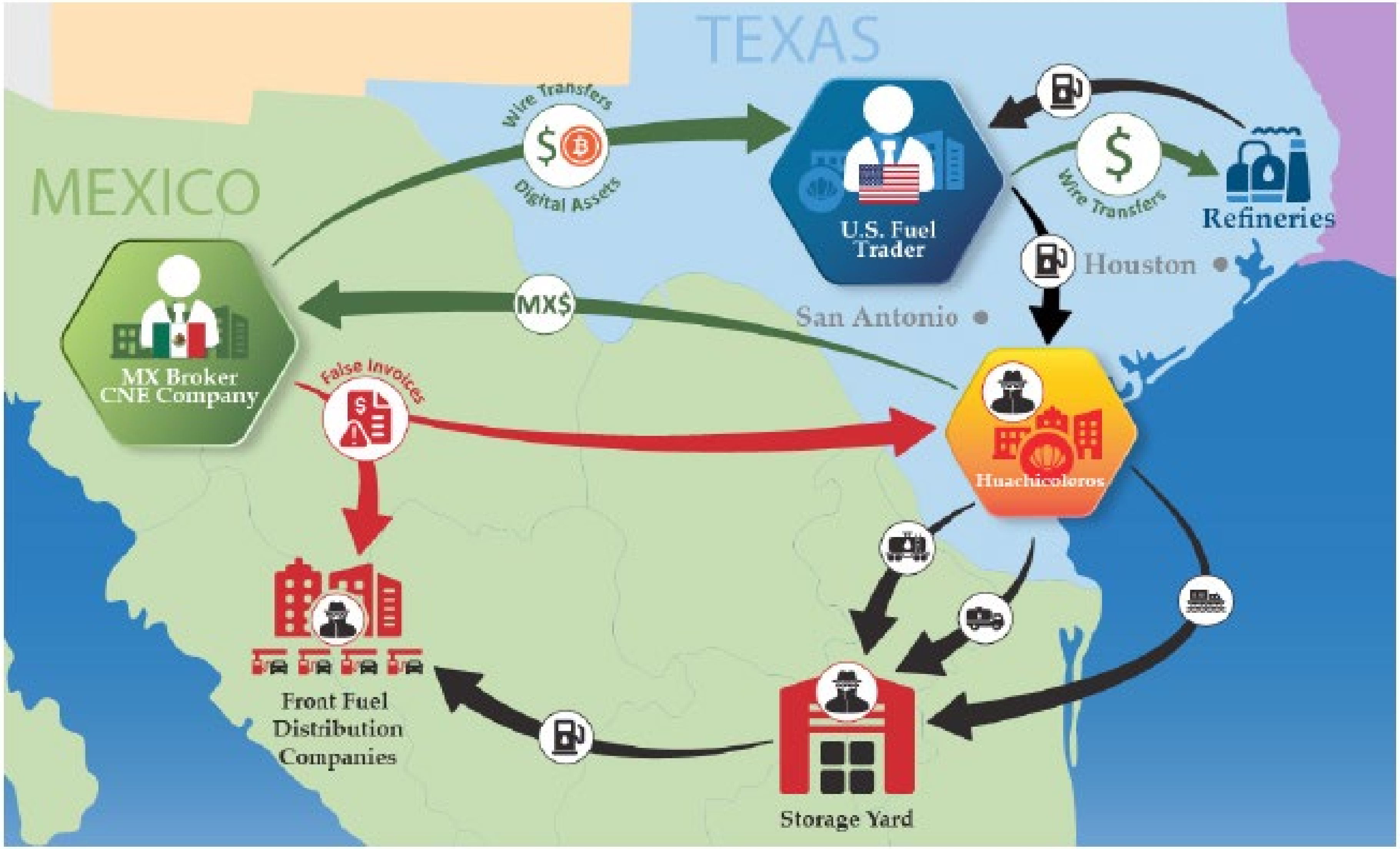
The U.S. Department of the Treasury's (Treasury) Financial Crimes Enforcement Network (FinCEN) is issuing this supplemental Alert to advise financial institutions[1] to be vigilant in detecting, identifying, and reporting suspicious activity connected to the Jalisco New Generation Cartel (CJNG), Sinaloa Cartel, Gulf Cartel, and other Mexico-based transnational criminal organizations (TCOs)—frequently referred to as the "Cartels"—smuggling gasoline, diesel, naphtha,[2] and other fuel from the United States across the U.S. southern border or through U.S. ports into Mexico in schemes involving Mexican tax evasion known as fiscal fuel theft (*huachicol fiscal*). This publication supplements FinCEN's May 2025 Alert on *Oil Smuggling Schemes on the U.S. Southwest Border Associated with Mexico-Based Cartels* (May 2025 Cartel Oil Smuggling Alert).[3]

Fiscal fuel theft refers to the circumvention of Mexican taxes on fuel that is illicitly imported from the United States via various smuggling methods. These schemes reflect an evolution of traditional fuel and oil theft (*huachicol*)[4] in Mexico. Fiscal fuel theft and traditional fuel and oil theft have, together, become the most significant non-drug illicit revenue source for the Cartels. In recent years, the Cartels and their fuel smugglers (*huachicoleros*) are increasingly purchasing and smuggling fuel from complicit U.S. fuel distribution companies (hereafter "U.S. fuel traders") for sale on the Mexican black market, with public reporting estimating that a quarter to a third of all fuel sold in Mexico may be illicit.[5] Smuggling methods can vary; however, smuggled fuel is typically misclassified in customs documentation, often masked by bribed Mexican government officials, including customs and tax officials, or concealed in other ways to circumvent Mexican taxes on imported fuel. Through these schemes, the Cartels are diverting tens of billions of dollars a year in tax revenue from the Government of Mexico and undercutting Mexico's state-owned energy company, Petróleos Mexicanos (Pemex),[6] and other legitimate Mexican and U.S. energy companies. According to Federal law enforcement agencies, the Cartels' smuggling schemes also fuels rampant corruption and violence that sustains their global drug trafficking operations and control in Mexico.

Exploiting the U.S.-Mexico Energy Trade and Mexican Energy and Fiscal Framework

Fiscal fuel theft schemes exploit the U.S. and Mexican energy trading relationship and Mexico's energy and fiscal framework to generate tens of billions of dollars for the Cartels every year at the expense of the Government of Mexico, Pemex, and other legitimate Mexican and U.S. energy companies. As described in FinCEN's May 2025 Cartel Oil Smuggling Alert, despite being one of the largest oil producers in the world and averaging nearly a million and a half barrels per day in 2024, Mexico lacks the capacity to refine its sour and heavy crude oil[14] into enough gasoline, diesel, and other fuel for the Mexican economy.[15] This has resulted in the U.S. and Mexican energy trading relationship becoming highly integrated, with Mexico exporting over 400,000 barrels of crude oil per day to refineries in the United States and importing nearly 2 million barrels per day of refined fuel—equating to over 70 percent of Mexico's fuel consumption.[16] The key U.S. ports for seaborne refined products are Houston, Beaumont/Port Arthur, and Corpus Christi, Texas according to commercial source reporting. Those imports of fuel are subject at customs to a significant Mexican import tax known as the Special Tax on Products and Services (*Impuesto Especial sobre Producción y Servicios*) (IEPS),[17] and other taxes, which often leads to significantly higher fuel prices in Mexico than in the United States and other jurisdictions.[18]

Figure 1. General Depiction of a Fiscal Fuel Theft Scheme



7

forvis mazars

FinCEN ADVISORY

FIN-2026-A002 **June 5, 2026**

Joint Advisory on Non-Work Authorized Populations and Their Employers and Risks to the Integrity of the U.S. Financial System

Suspicious Activity Report (SAR) Filing Request:

FinCEN requests that financial institutions reference this Advisory by including the key term "**FINANCIALINTEGRITY-2026-A002**" in SAR field 2 (Filing Institution Note to FinCEN) and the narrative.

The U.S. Department of the Treasury's (Treasury) Financial Crimes Enforcement Network (FinCEN), jointly with the Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, and National Credit Union Administration, (collectively, the Agencies), is issuing this Advisory in coordination with the Internal Revenue Service (IRS) to advise financial institutions[1]—in particular, banks[2]—to be vigilant against fraud schemes and other suspicious or potentially criminal activities involving the unlawful employment of illegal aliens and the associated risks to the integrity of the U.S. financial system.[3] Through these schemes, aliens and the associated risks to the integrity of the U.S. financial system.[3] Through these schemes, employers can gain an unfair advantage over legitimate U.S. businesses; depress wages; facilitate identity theft of people who are authorized to work in the United States, including American citizens; and steal millions of dollars in Federal and state payroll tax revenue meant for government benefit programs. Non-work authorized populations and their employers often rely on access to the U.S. financial system. In certain instances, the access to financial services and unlawfully obtained wages can be leveraged to facilitate the financing of transnational criminal organizations (TCOs)—several of which have been designated as Foreign Terrorist Organizations (FTOs)—and their global criminal enterprises, including drug trafficking, human trafficking, and other illegal activity in the United States.[4]

FinCEN NOTICE

FIN-2026-NTC1 May 11, 2026

FinCEN Notice on the Threat of Human Trafficking During the 2026 FIFA World Cup

Suspicious Activity Report (SAR) Filing Request:

FinCEN requests that financial institutions reference this Notice in SAR field 2 (Filing Institution Note to FinCEN) and the narrative by including the key term "FIN-2026-HTWORLDCUP" and select SAR Field 38(h) (human trafficking).

The U.S. Department of the Treasury's (Treasury) Financial Crimes Enforcement Network (FinCEN) is issuing this Notice to urge financial institutions[1] to be vigilant in detecting, identifying, and reporting suspicious activity connected to human trafficking[2] associated with the 2026 Fédération Internationale de Football Association (FIFA) World Cup.[3] While human trafficking is an ever-present threat in the United States, major events such as the 2026 FIFA World Cup can create a concentrated demand for licit and illicit services, including commercial sex acts and involuntary servitude, resulting in increased vulnerability for human trafficking.[4] Individuals visiting or residing near World Cup host cities may be vulnerable to trafficking by perpetrators seeking to exploit increased economic activity surrounding such events.

The United States, along with Canada and Mexico, will host the 2026 FIFA World Cup from June 11 to July 19, 2026, in Atlanta, Boston, Dallas, Houston, Kansas City, Los Angeles, Miami, New York/New Jersey, Philadelphia, the San Francisco Bay Area, and Seattle; as well as Toronto and Vancouver in Canada; and Guadalajara, Mexico City, and Monterrey in Mexico.[5] FinCEN is issuing this Notice to support Federal and state law enforcement agencies in protecting victims and identifying suspicious activity potentially indicative of human trafficking around the 2026 FIFA World Cup. FinCEN recommends increased vigilance by financial institutions located in and around host city locations associated with the 2026 FIFA World Cup. It is also critical that customer-facing financial institution staff are aware of behavioral indicators that may indicate human trafficking, as victims of human trafficking may have no contact with people outside of their traffickers other than when visiting financial institutions.[6]

FinCEN ALERT

FIN-2026-Alert002

May 11, 2026

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

Suspicious Activity Report (SAR) Filing Request:

FinCEN requests that financial institutions reference this Alert in SAR field 2 ("Filing Institution Note to FinCEN") and the narrative by including the key term "**FIN-2026-Alert002.**"

The U.S. Department of the Treasury's (Treasury) Financial Crimes Enforcement Network (FinCEN) is issuing this Alert to assist financial institutions[1] in identifying actors suspected of funding and facilitating procurement networks supporting the Islamic Revolutionary Guard Corps (IRGC) and mitigating those risks through the filing of suspicious activity reports (SARs).[2] The IRGC was created after the Iranian Revolution as a parallel organization to Iran's regular armed forces that reports directly to Iran's Supreme Leader and is charged with defending the Iranian regime. The IRGC includes ground, naval, and air forces, along with the Basij internal security militia, and the IRGC-Qods Force (IRGC-QF). The IRGC-QF conducts covert operations abroad and supports terrorism by supplying funding, training, and weapons to aligned groups.[3] Since its inception, the IRGC has engaged in terrorist activity with the support of the Iranian government and is a designated Foreign Terrorist Organization (FTO).[4]

As described in FinCEN's 2025 Iran Advisory, the IRGC relies on complex financial facilitation networks comprised of exchange houses, front companies, financial facilitators, and other service providers operating across multiple jurisdictions to obscure beneficial ownership, disguise the origin of funds, and enable movement of proceeds linked to sanctions evasion and other illicit activity.[5] In addition, recent analysis of Bank Secrecy Act (BSA) data indicates that the IRGC relies on networks of shell companies and financial facilitators to launder digital asset proceeds through layered corporate structures and cross-border transactions. These entities function as instruments of the IRGC by moving funds, converting assets, or otherwise acting on behalf of sanctioned actors, even where the companies themselves are not formally identified as IRGC-owned. This structure allows the IRGC and its affiliates to access the financial system and disguise control while avoiding direct attribution.

PRESS RELEASES

Treasury Further Dismantles Overseas Scam Operations Targeting Americans

June 23, 2026

WASHINGTON—Today, the U.S. Department of the Treasury took coordinated action to further disrupt the Prince Group Transnational Criminal Organization (Prince Group TCO). The Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned nine individuals and 26 entities linked to Prince Group TCO, including TCO leadership, investors in scam compounds, and front companies. In parallel, Treasury's Financial Crimes Enforcement Network (FinCEN) proposed amending its October 2025 Huione Group Final Rule to include H-Pay Service PLC and any successor entity. Huione Group served as a critical node for laundering proceeds of cyber heists and virtual currency investment scams and was used by the Prince Group to transfer and consolidate scam-derived assets.

91 FR 38340 – 38350
06/25/2026
Comments Close
07/27/2026

forvis mazars

Together, today's actions build on Treasury's October 2025 designation of Prince Group TCO and guard against Huione Group's attempts to circumvent being cut off from the U.S. financial system.

On October 14, 2025, OFAC, in coordination with the United Kingdom's (UK) Foreign, Commonwealth and Development Office, designated Prince Group as a TCO for its role in a global criminal enterprise built on scam compounds, fraud, and money laundering. Prince Group TCO members own and reap substantial profits from scam compounds where fraud operations target victims in the United States and around the world. Prior to its designation, Prince Group TCO oversaw a worldwide money laundering network and invested criminal proceeds across a wide range of businesses, including real estate, aviation, and luxury cigars. Following Treasury's action, countries around the world mobilized against this vicious syndicate, seizing properties, making arrests, and freezing assets with a combined value in the billions of dollars. In January, Chen Zhi, the leader of Prince Group TCO and mastermind behind its sprawling criminal empire, was stripped of his titles and Cambodian citizenship.

forvis mazars

SOPHISTICATED SCAMS TARGETING AMERICANS

Transnational criminal organizations based in Southeast Asia, like the Prince Group TCO and with support of their enablers like Huione Group, continue to target Americans through large-scale cyber-enabled fraud and scam operations. A U.S. government estimate reported that Americans lost at least $10 billion in 2024 to Southeast Asia-based scam operations, a 66 percent increase over the prior year. While these operations employ a variety of techniques to cheat victims out of their savings, one of the most common and lucrative schemes involves digital asset investment fraud. According to FinCEN's September 2023 alert on these scams, perpetrators send text messages directly to potential targets' phones and often use the promise of potential romantic relationships or friendships to gain the trust of their victims. They then convince their targets to make purported "investments" in digital assets on websites that are designed to look like legitimate investment platforms but are actually controlled by the scammers themselves. Ultimately, these scammers steal the funds deposited on the platforms under their control.

Southeast Asia-based criminal organizations often recruit individuals to work in scam centers under false pretenses, such as by offering fake technology or customer service jobs at the centers' connected casinos, resorts, and front companies. Once the individuals arrive at the compounds, the operators confiscate their passports and use debt bondage, physical violence, the threat of forced prostitution, and other methods to coerce them to scam strangers online. The scam operators specifically look to recruit individuals with English language skills to target American victims. Former scammers have reported they were directed to specifically target Americans, and some even had quotas for the number of targets per day. Individual U.S. victims of these scams have in some cases lost their entire life savings.

FATF Statements / https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html

- FATF – "High-Risk and Non-Cooperative Jurisdictions (HRNCJ). On 06/19/26 FATF publicly identified countries with remaining AML deficiencies:

- Call to Action – (a/k/a *black list*):
  - Countermeasures: Democratic People's Republic of North Korea & Iran – all jurisdictions are encouraged to follow FATF statement of 02/20/20 and Executive Orders (E.O.s) 13810, 13949, and 13876, and apply effective counter-measures to protect their financial sectors from ML/FT risks emanating from North Korea and Iran.
  - EDD – Myanmar – (In 02/2020 Myanmar added to Due Diligence section – due to lack of progress and most action items were not addressed one year after the deadline – focus elevated in 10/2022)

- Jurisdictions Under Increased Monitoring – (*a/k/a grey list*):
  - Due Diligence / Commitments Made – *Strategic Deficiencies* Noted: Angola; Bolivia; Bosnia & Herzegovina; Bulgaria; Cameroon; Cote D'Ivoire; Democratic Republic of Congo (DRC); Haiti; Iraq; Kenya; Kuwait; Lao PDR; Lebanon; Monaco; Nepal; Papua New Guinea; South Sudan; Syria; Venezuela; Vietnam; Virgin Islands (UK); and Yemen.
  - Commitments Satisfied – Algeria, Namibia

https://www.fincen.gov/system/files/shared/314bfactsheet.pdf

PRESS RELEASES

FinCEN Issues Guidance to Help Financial Institutions Eliminate Fraud Through Information Sharing

June 12, 2026

WASHINGTON—Today, the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) issued updated guidance to clarify how financial institutions can share information with each other about suspected fraud under section 314(b) of the USA PATRIOT Act.

FinCEN's updated guidance clarifies that a financial institution may share information about activity involving suspected fraud, money laundering, terrorist financing, or other specified unlawful activities, and that it may share that information with any other financial institution eligible to participate in the section 314(b) program to identify illicit financial activity. The fact sheet includes examples of the type of information related to fraud and other criminal activity that financial institutions can share with each other under section 314(b), including video surveillance footage, cyber-related data, such as IP addresses; and fraud indicators like newly added payees followed by large transfers, multiple accounts with the same or similar identifying information, and login activity from geographically distant places.

Among other things, information sharing pursuant to section 314(b) allows financial institutions to respond to threats—activities a financial institution suspects may involve possible terrorist activity or money laundering, such as fraud and other criminal activity—that are carried out by repeat actors moving across financial institutions to evade detection. The section 314(b) program provides financial institutions with the flexibility and connectivity needed to counter these threats and prevent bad actors from exploiting gaps between institutions.

[Updated June 12, 2026]

information that may be shared. Financial institutions and associations of financial institutions could share, for example, transaction information; video surveillance footage; cyber-related data (such as IP addresses and geolocations); device identification numbers; decisions related to account creation, maintenance, closure, or services (and related research and analytical materials); transaction monitoring system alerts; and indicators that activity may be suspicious, including newly added payees followed by large transfers, multiple accounts with the same or similar identifying information, and login activity from geographically distant locations.

sets Control

SANCTIONS LISTS ⌄ SANCTIONS PROGRAMS ⌄ SUBMIT A REPORT CONTA

OF INTRODUCTION TO OFAC GUIDE

Publication of Introduction to OFAC Guide

06/01/2026

Today, the Department of the Treasury's Office of Foreign Assets Control (OFAC) is publishing an "Introduction to the Office of Foreign Assets Control" guide, to provide U.S and foreign persons a foundational understanding of how OFAC sanctions work and how to comply with them, including how to request a license from OFAC, how persons may be removed from an OFAC sanctions list, and how OFAC enforces its sanctions. This guidance is intended as a resource the public can use to better understand OFAC's expectations and thereby continue strengthening the effectiveness of OFAC sanctions.


OFAC
Office of Foreign Assets Control
Introduction to the
Office of Foreign Assets Control
THE DEPARTMENT OF THE TREASURY
1789

https://ofac.treasury.gov/media/935656/download?inline

Introduction to the

Office of Foreign Assets Control

June 1, 2026

Launch of OFAC Reconsideration Portal

06/29/2026

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is launching a new online Reconsideration Portal for the submission of requests to be removed from an OFAC sanctions list. This portal is intended to streamline the petitions process by guiding submitters to provide necessary information upfront, rather than through a series of questionnaire/answer exchanges that can delay efficient adjudication of a delisting petition. Listed persons can also request certain unclassified, non-privileged information underlying their sanctions determination (a "courtesy document") through the Reconsideration Portal. To accompany this new portal, OFAC is updating its website with additional information on the petitions process.

OFAC is updating Frequently Asked Question (FAQ) 897, adding new FAQ 1261, and publishing two quick-reference guides on Delisting Petitions Best Practices and What to Include in a Delisting Petition.

Additional Information +

Submit a Request for Reconsideration or Record Request

Reconsideration Portal

PRESS RELEASE

UNODC World Drug Report 2026: Global drug markets transforming rapidly as technology, novel drug types and instability present traffickers with new opportunities

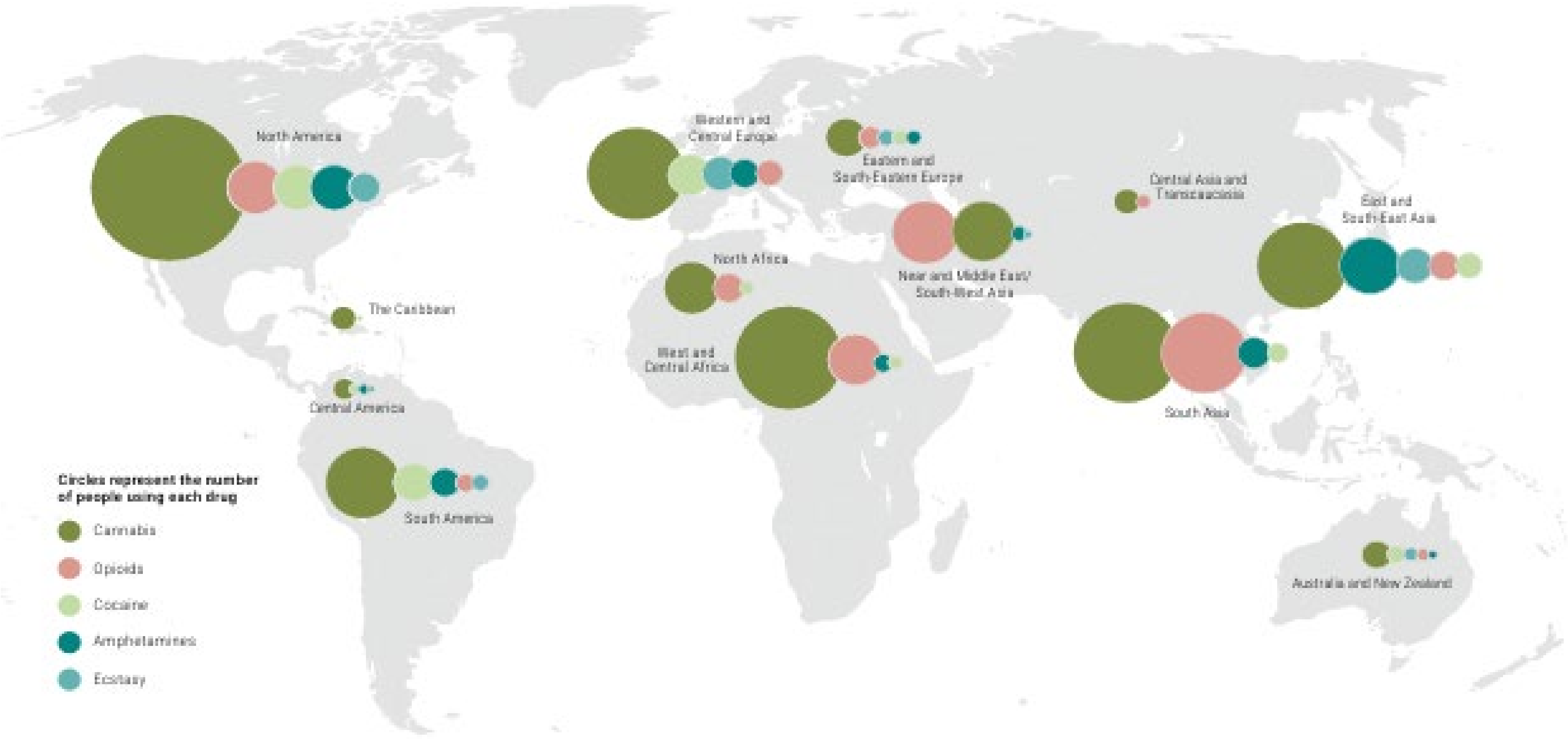
Vienna, 26 June 2026

Drug traffickers are exploiting technologies and global instability to introduce novel drugs, experiment with different trade routes and methods, and aggressively push into new markets, said the United Nations Office on Drugs and Crime (UNODC) in its World Drug Report 2026 released today.

"We have seen an unprecedented spike in new types of drugs on the market, and worryingly, some are more potent or dangerous than before," said Monica Juma, Executive Director of UNODC. "And, we are already suffering the impact: millions of premature deaths and healthy years of life needlessly lost; drug trafficking networks that are distorting economies; the destruction of lives, communities and livelihoods; and the compounding of insecurity and violence. The imperative to focus on stopping organized crime groups has never been greater. We must surge deterrence efforts, increase intelligence-sharing and coordinate joint operations, while investing more in prevention and treatment."

An estimated 331 million people used a drug in 2024, or 6.2 per cent of the global population aged between 15 and 64, compared to 5.2 per cent in 2014. Cannabis remains the most widely used drug by far, with 256 million users in 2024, followed by opioids (63 million), amphetamines (32 million), cocaine (25 million) and ecstasy (21 million).

Estimated number of people who use specific drugs, in selected subregions for which estimates are available, 2024



The boundaries and names shown and the designations used on this map do not imply official endorsement or acceptance by the United Nations.

Compliance Conversations
ProBank Education Services

Payments / Fraud Trends

2026 ACH Volumes – Another New Record

NACHA – Availability of Non-Same-Day Credits - 09/18/26

NACHA – Fraud Monitoring – Phase 1 & 2

IAT Contact within the “ACH Contact Registry” – 01/01/27

FTC “Alerts”

2026 – 1st Quarter

- Total Volume 8.9 Billion Entries - + 4.8% over 1Q’25:
- Total Value of Payments - $24.1 Trillion - + 9.3% over 1Q’25:
  - Same-Day ACH volume + 23.6% (403 million Entries with value of $ 1.1 trillion);
  - B2B + 9.4% (2.1 billion Payments)
  - Direct Deposit + 1.7%% (2.2 billion)
  - Healthcare + 4.9% (131.0 million)
  - WEB Entries + 5.4% (2.9 billion)
  - P2P + 18.5% (129.3 million)

Availability of Non-Same Day ACH Credits - 09/18/26

- NACHA Rules – Article 3.3.1.1. is modified to require “For a credit Entry that is not a Same Day Entry the RDFI must make the amount of the credit Entry available to the Receiver for withdrawal no later than 9:00 a.m. (RDFI’s local time) on the Settlement Date”;
- The current ACH Rule reads any forward ACH Entry made available to the RDFI by 5:00 p.m. on the preceding business day must be made available for withdrawal no later than “OOB” (opening of business) on settlement day.
- “Hopefully” everyone has memo-post capability, and most are already doing this.

Fraud Monitoring – Both Phases – In Effect Now

- “Risk-based” processes and procedures reasonably intended to identify ACH Entries initiated due to fraud;
- Ex-Post not real-time monitoring;
- For an ODFI: For Entries with a high potential for fraud:
  - Stop further processing of the flagged transaction;
  - Consult with the Originator to determine validity;
  - Consult with other internal monitoring teams;
  - Contact the RDFI.
- For an RDFI: Monitoring Incoming Transactions could include:
  - Account Type and SEC Code mismatch;
  - High-Dollar transaction atypical for the receiving account;
  - Series of similar credit entries received within a short period of time, such as multiple payroll or benefit payments;
  - Any of these to a new account, dormant account, or to an account acting as a money mule.
- ODFIs – Note: You are warranting that your Originating clients are complying as well.
- Next NACHA Target – “First-Party Fraud” !

Consumer Alert

Animal lovers: learn to spot and avoid this breed of pet scams

By: BCP Staff | June 24, 2026

Scammers have been taking advantage of how much people love animals. They'll steal and manipulate pet images, videos, and even use AI-generated deepfakes to help them trick you into giving them your money or personal information. Fortunately, there are ways to help you detect and avoid these kinds of scams:

Recent Consumer Alerts

Animal lovers: learn to spot and this breed of pet scams
June 24, 2026

- Scammers pretend to be law enforcement or an animal hospital, claiming to have your pet who's had an emergency. They might have seen a flyer for a missing pet, or know from social media that you're away from home. They might even use AI to create fake photos or videos of your pet in distress. But it's all a lie. If someone says the **only** way to pay for your pet's treatment is with a gift card, a payment app, cryptocurrency, or a wire transfer service, you're dealing with a scammer.

- Scammers impersonate real animal shelters and hospitals collecting donations for pets in need. They might create fake webpages and posts using stolen or AI-generated images of pets in need of forever homes. If someone asks you to donate, check ftc.gov/charity for advice on how to donate safely. And, as part of your research, do a reverse image search to see if the images are stolen.

- Scammers want you to think you won a prize because you previously donated to help animals. The name of the prize or organization might sound real but it's another lie. If you have to pay to collect a prize or sweepstakes winnings, you know it's a scam.

Don't let scammers rush you into making a decision. Slow down and talk to someone you trust. And if you spot one of these scams, tell the FTC at ReportFraud.ftc.gov.

Home / News and Events / News / Press Releases

FTC Data Show
Open file

See more

For Release

FTC Data Show People Reported Losing $3.5 Billion to Imposter Scams in 2025

Imposter scams were the most reported fraud last year, with reported losses increasing nearly three times since 2020

June 15, 2026

Tags: Consumer Protection | Bureau of Consumer Protection | Imposter | deceptive/misleading conduct | Government

New data from the Federal Trade Commission reveal that people reported losing a staggering $3.5 billion to imposter scams in 2025, with reported losses increasing nearly three times since 2020.

FTC data also show that people reported imposter scams more than any other fraud category in 2025—nearly one in three fraud reports were about imposter scams. These scams lured consumers through text, phone, email, social media, search engine results and other means. Some of the costliest impersonation scams start with a fake security alert, often from a bank. People are convinced to move money to "protect" it, with their losses often limited only by their available funds.

For Consumers

Blog: Help fight imposter scams this World Elder Abuse Awareness Day

Last year, people reported losing nearly $1 billion to business impersonators with the highest reported losses to bank impersonators—and about $920 million to government impersonators, up from $866 million and $789 million respectively in 2024.

The FTC has seen a striking increase in reported fraud losses to all types of fraud—about $16 billion was reported lost in 2025, the highest on record and an increase of about 25% compared to the 2024 figure.

"Consumers derive enormous benefits from competitive markets built on truthful information. But fraud undermines that foundation, impeding the market process and preventing markets from operating efficiently," said Christopher Mufarrige, Director of the Bureau of Consumer Protection. "The FTC will use every tool available to combat one of the most pernicious forms of fraud—government and business impersonation—and to protect the integrity of the digital economy."

The data underscore the importance of the FTC's work with the Elder Justice Coordinating Council (EJCC), which is working to help raise awareness of imposter scams and other scams impacting older adults as well as other consumers. This year, the FTC, along with the Department of Justice, Department of Health and Human Services and members of the EJCC, is leading the Never Ever campaign, a public-private coordinated consumer education effort to raise awareness of government and business imposter scams.

In addition to the federal agency members of the EJCC, the campaign also includes private sector representatives such as the American Bankers Association, USTelecom, Google and Microsoft.

FEDERAL TRADE COMMISSION
CONSUMER ADVICE

Shopping and Donating | Credit, Loans, and Debt | Jobs and Making Money | Unwanted Calls, Emails, and Texts | Identity Theft and Online Security | Scams

Home / Consumer Alerts

Vea esta página en español

Consumer Alert

A real FTC employee won't text you their photo ID to "verify" their identity

By: BCP Staff | June 3, 2026

Scammers lie and pretend to be an FTC employee to trick you into giving them money, access to your financial accounts, or your personal information. In a new twist, they falsely claim they're an FTC "agent" that can help you recover money you lost in a scam.

Here's how this new FTC impersonator scam works:

- You get an unexpected message from a contact you don't know
- They say they're an FTC employee or "agent" (they're not) and they can help you "recover losses" (they can't) from a previous scam
- To "verify" their identity and gain your trust, they send you a photo of an employee ID and a badge (all fake)

Don't buy the story. It's really an FTC impersonator trying to get money or financial information from you with a refund and recovery scam.

Recent Consumer Alerts

Animal lovers: learn to spot and avoid this breed of pet scams
June 24, 2026

Making a family plan for summer screen time
June 22, 2026

How to avoid a travel scam this summer
June 17, 2026

Browse by Topic

Buying and Owning a Car (46)

forvis mazars

How can you know if someone really works at the FTC?

Knowing what a **real FTC employee *won't* do** can help you spot an FTC impersonator.

1. A **real FTC employee won't** contact you by text message or a messaging app like WhatsApp.
2. A **real FTC employee won't** text you a photo of their employee ID to "verify" their identity.
3. A **real FTC employee won't** claim to help you recover money you lost in a scam and ask you to pay them, move your money into an account they specify, or give them your financial information.

What to do if you paid a scammer

If you gave a scammer your financial information or paid them — by wiring money through a company (like Western Union or MoneyGram) or your bank, through a money transfer app, or with cryptocurrency — try to cancel or reverse the transaction as soon as you can. See What To Do if You Were Scammed for specific steps to take.

FEDERAL TRADE COMMISSION
CONSUMER ADVICE

Shopping and Donating | Credit, Loans, and Debt | Jobs and Making Money | Unwanted Calls, Emails, and Text

Home / Consumer Alerts

Consumer Alert

Are you ready for hurricane season?

By: BCP Staff | June 1, 2026

Hurricane season starts today. Are you prepared? Wherever you live, scammers follow whatever weather emergencies may strike. So as this hurricane season gets started, check over your family's emergency plan and restock your supply kit. And then check out the FTC's Dealing with Weather Emergencies article so you're prepared to avoid scams in case a hurricane (and scammers) cross your path.

Here are four things to do to prepare for hurricane season while avoiding scams.

1. **Sign up for alerts and warnings in your area.** Public safety officials use systems to alert you about severe weather and disasters.

2. **Check your insurance policy.** To avoid surprises, check to make sure your insurance policy is current, and find out what's covered — and what isn't.

3. **Secure important documents.** Use a lockable fireproof box to gather important documents — like Social Security and health insurance cards, and copies of deeds, titles, wills, birth and marriage certificates — so they're ready to go if you have to leave quickly. Or, use personal cloud storage to upload scanned PDFs of important documents. Make sure access requires a strong password and multifactor authentication.

4. **Guard your personal information.** Year-round, know that only scammers will say they're a government official and then demand money or your credit card, bank account, or Social Security number.

Bookmark ftc.gov/WeatherEmergencies so you always know how to avoid a scam during hurricane season, and please share this information with your family and community.

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Enforcement | Policy | Advice and Guidance | News and Events | About the FTC

Home / News and Events / News / Press Releases

For Release

New FTC Data Show People Have Lost Billions to Social Media Scams

Social media was the costliest fraud contact method in 2025 and reported losses increased eightfold since 2020

April 27, 2026

Tags: Consumer Protection | Bureau of Consumer Protection | Imposter | Investment | Jobs | Online Dating | Shopping | Advertising and Marketing | Online Advertising and Marketing | Social Media

New data from the Federal Trade Commission show that, in 2025, nearly 30% of people who reported losing money to a scam said that it started on social media, with reported losses reaching a staggering $2.1 billion.

Related resources

Data Spotlight: Reported losses to scams on social media eight times higher than in 2020

For Consumers

forvis mazars

Social media scams produced far more in losses—an eightfold increase since 2020—than any other contact method used by scammers to reach consumers, according to the new data.

The Data Spotlight notes that social media creates easy access to billions of people from anywhere in the world, making a scammer's job easier at very little cost. Scammers may hack a user's account, exploit what a user posts to figure out how to target them, or buy ads and use the same tools used by real businesses to target people by age, interests or shopping habits.

Reports show that in 2025, people reported losing more money to scams that started on Facebook than on any other social media platform. WhatsApp and Instagram were a distant second and third. In 2025, people reported losing far more money to scams on Facebook alone than they reported losing to text or email scams.

The data also show that all age groups, with the exception of those 80 and over, reported losing more money to scams that started on social media than any other contact method. And social media ranked second after phone calls for those 80 and over.

According to FTC data, social media scams come in different forms, including:

- **Investment scams:** People reported losing the most amount of money last year to investment scams that originated on social media, with losses of $1.1 billion, more than half of the total amount lost to social media scams, according to FTC data. These scams often started with an ad or post offering a program to teach you how to invest. Other scammers posed as friendly advisers or created WhatsApp groups full of "successful investors" sharing fake testimonials.

- **Shopping scams:** Shopping scams were the most reported type of social media scam last year, with more than 40% of people who lost money to a scam on social media reporting that they ordered something they saw in a social media ad—everything from clothes and makeup to car parts and even puppies. Many of these ads led to unfamiliar websites, while others sent people to sites impersonating well-known brands that claimed to offer big discounts.

- **Romance scams:** Reports show romance scams also thrive on social media—nearly 60% of people who reported losing money to a romance scam in 2025 said it started on a social media platform. According to reports, scammers often tailored their pitch based on people's profiles, later inventing a crisis requiring money or casually offering investment advice to draw them onto a fake investment platform.

To help steer clear of scams on social media the FTC advises consumers to:

- Limit who can see your posts and contacts on social media. Visit your privacy settings to set some restrictions so scammers have less to work with.
- Never let someone you have met only on social media direct your investment decisions. Instead, learn more about spotting investment scams.
- Before you buy, check out the company. Search online for its name plus "scam" or "complaint."

To learn more about how to spot, avoid, and report scams—and how to recover money if you've paid a scammer—visit ftc.gov/scams. If you spot a scam, report it to the FTC at ReportFraud.ftc.gov.

The Federal Trade Commission works to promote competition and protect and educate consumers. The FTC will never demand money, make threats, tell you to transfer money, or promise you a prize. Learn more about consumer topics at consumer.ftc.gov, or report fraud, scams, and bad business practices at ReportFraud.ftc.gov. Follow the FTC on social media, read consumer alerts and the business blog, and sign up to get the latest FTC news and alerts.

Action Items and Next Steps

Review your compliance programs for alignment with new guidance.

Submit comments on proposed rules where relevant.

Prepare for upcoming deadlines.

Regulation	Agency	Compliance Deadline	Summary	Status
FDIC Signage Rule – Digital Channels (Part 328)	FDIC	**April 1, 2027**	Requires FDIC signage on digital platforms and ATMs.	Compliance date for Parts 328.4 & .5 extended to April 1, 2027.
Records Preservation Program – Record Retention Guidelines	NCUA	**July 16, 2026**	Updates to the vital records preservation program, clarifies the purpose of 12 CFR Part 749, and updates the definition included therein.	Final Rule – Request for Comments was issued 03/11/26
User Fee Schedule – FBI Criminal Justice Information Services	FBI	**October 1, 2026**	Increase in the fees charged for providing fingerprint-based and name-based criminal history record information (CHRI) checks.	Reimburse FBI for the costs in providing the service – noncriminal justice purposes including employment and licensing.
Small Business Lending Data Collection (Section 1071, Reg B)	CFPB	**July 1, 2026 (Tier 1)**	Requires large lenders to collect/report small business loan data.	Enforcement paused. CFPB stated it will not enforce until rule is rewritten.
		January 1, 2027 (Tier 2)	Moderate-volume lenders begin data collection.	Same as above.
		October 1, 2027 (Tier 3)	Smallest lenders begin data collection.	Same as above.

Thank you for participating in our discussion today!

Questions?

Contact

Let's stay in touch!

Scan the QR code to connect with me on LinkedIn.

Mark Burnside

Director

Mark Dever

Director

The information set forth in this presentation contains the analysis and conclusions of the author(s) based upon his/her/their research and analysis of industry information and legal authorities. Such analysis and conclusions should not be deemed opinions or conclusions by Forvis Mazars or the author(s) as to any individual situation as situations are fact-specific. The reader should perform their own analysis and form their own conclusions regarding any specific situation. Further, the author(s)' conclusions may be revised without notice with or without changes in industry information and legal authorities.

forvis mazars

ProBank Education Services

As a leading provider of continuing education programs for financial professionals, we train thousands of financial industry employees annually through our tailored programs. Our services are available throughout the United States or virtually and include compliance seminars, webinars, and in-house training courses specifically designed for accountants, branch managers, BSA officers, compliance officers, customer service, executive management, loan processors, mortgage brokers, new accounts personnel, operations officers, risk management, and directors.

Seminars

ProBank Education Services provides a wide range of bank regulatory compliance seminars throughout the United States – whether In-Person (On-Site) or Remote (Virtual) – choose what is best for you.

Webinars

ProBank Education Services provides insightful and engaging webinars in a format that is right for you and your employees, including Live and On-Demand options.

Publications – Newsletters & Manuals

We offer a wide variety of publications ranging from a quarterly newsletter to a growing list of in-depth manuals on specific topics. Our newsletter, InCompliance™, helps keep you informed about recent regulatory pronouncements and current issues, and provides helpful compliance and management tips.

Compliance Schools & Conferences

ProBank Education Services personnel routinely serve as instructors at banking schools and conferences across the United States. Because of the breadth of our experience, we can adjust our presentations to fit the needs of the specific audience at the basic, intermediate, or advanced level. In addition, we provide regional regulatory compliance conferences throughout the year.

Association-Sponsored Seminars

For many years, ProBank Education Services has presented programs under the auspices of many state, community, and independent banker associations, credit union leagues and other industry groups on specific areas of interest, such as compliance, deposits, lending, AML/BSA, fair lending, CRA, compliance risk management and more. These programs are presented on a "turn-key" basis.

Speakers Bureau

One of our most valued educational assignments is to serve as instructors at schools, conferences, and conventions across the United States. Our well-received presentations rely on the depth of experience of our team and are designed to help sharpen attendees' regulatory compliance acumen and banking skills. We customize each presentation to meet the needs of a specific audience which ranges from basic to intermediate to advanced levels of information on compliance topics.

In-House Training

Our educational programs and professional instructors are available to come to you. Each year, we work with financial institutions who request educational programs on-site at their institution for their employees. These programs provide the benefits of our national seminar events but are delivered with a more customized approach.

ProBank Advisor©

ProBank Advisor© is a compliance advisory service that can offer you the compliance advice you need. Connecting with an experienced compliance professional is simple through ProBank Advisor's easy-to-navigate platform.

Tammy Carter | Managing Director | 502.479.5229 | tammy.carter@us.forvismazars.com | probank.com

Register Today


Compliance Conversations with ProBank Education Services
Q4 2026
Monday, October 19 ▪ 2–3 p.m. ET
forvis mazars