Compliance Conversations / Second Installment
ProBank Education Services

July 14, 2025

forvis mazars

Compliance Conversations
ProBank Education Services

Meet the Presenters

Mark Burnside, CRCM
Director, Kentucky

Ginger McCullough, CRCM
Manager, Missouri

Mark Dever, AAP, CAMS
Director, Kentucky

K. Natalie Straus, CRCM, JD
Director, Kentucky

Kylee Durbin, CRCM
Manager, Kentucky

1

Compliance Conversations

Regulatory Change Management

An effective change management process is essential in a financial institution. It provides a structured framework for identifying, assessing, & implementing new or amended rules & regulations.

Compliance Conversations
Regulatory Change Management

Key Elements

- Identify Change
- Analyze Impact & Risk
- Establish Responsible Parties
- Create an Action Plan
- Clearly Communicate
- Evaluate Effectiveness

Compliance Conversations
Regulatory Change Management

Identify Change

May 12, 2025

The Consumer Financial Protection Bureau announced it is withdrawing 67 guidance documents.

Federal Register: Interpretive Rules, Policy Statements, & Advisory Opinions; Withdrawal

- ✓ What happens when the changes are not to the law or statute?

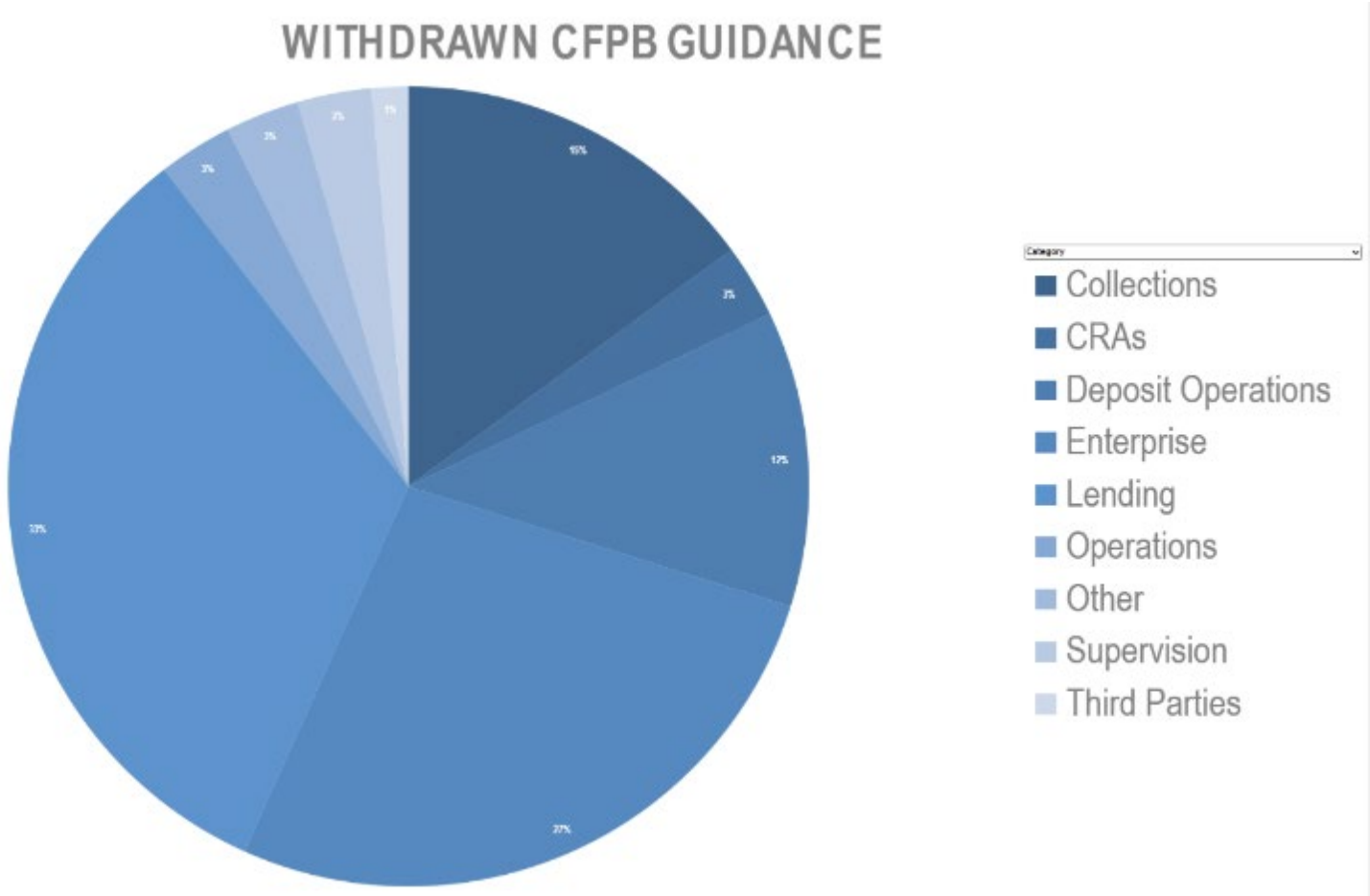
Analyze Impact & Risk

Element	Role in Compliance Risk Management
Laws & Statutes	Outlines the mandatory requirements.
Interpretive Guidance	Provides context & expectations.

Compliance Conversations
Regulatory Change Management

Establish Responsible Parties / Create An Action Plan / Clearly Communicate

Category	Total
Advisory Opinion	13
Bulletin	22
Circular	16
Guidance	1
Interpretive Rule	7
Policy Statement	8



2

Compliance Conversations

Deposits

Monitoring deposit compliance for changes to rules, guidance, & industry trends can help institutions avoid regulatory action & consumer harm.

Compliance Conversations
Deposits

Regulatory Change Management / Regulation CC Thresholds

As of July 1, 2025	Minimum Amount	$275
Inflation-adjusted Dollar Thresholds	Cash Withdrawal	$550
	New Account	$6,725
	Large Deposit	$6,725
	Repeatedly Overdrawn	$6,725

Compliance Conversations
Deposits

Notice Requirements

Electronic delivery is permitted where the institution has complied with the requirements of the Electronic Signatures in Global & National Commerce Act (15 U.S.C. 7001 *et seq.* ("E-Sign Act")). *See* comment 229.15(a)-1.

(e) ***Changes in policy.*** A bank shall send a notice to holders of consumer accounts at least 30 days before implementing a change to the bank's availability policy regarding such accounts, except that a change that expedites the availability of funds may be disclosed not later than 30 days after implementation.

Commentary

1. This paragraph requires banks to send notices to their customers when the banks change their availability policies with regard to consumer accounts. A notice may be given in any form as long as it is clear & conspicuous. If the bank gives notice of a change by sending the customer a complete new availability disclosure, the bank must direct the customer to the changed terms in the disclosure by use of a letter or insert, or by highlighting the changed terms in the disclosure.

Supplementary Information to Final Rule

Electronic delivery is permitted where the institution has complied with the requirements of the Electronic Signatures in Global & National Commerce Act (15 U.S.C. 7001 *et seq.* ("E-Sign Act")). *See* comment 229.15(a)-1.

3

Compliance Conversations

Flood Insurance

Content Coverage Discussion

Compliance Conversations
Flood Insurance – Contents

In the Business/Commercial lending space, we are more likely to secure building contents when taking commercial buildings as collateral.

If we determine that the building is in a Special Flood Hazard Area, we are required to have “contents” coverage in addition to building coverage when we secure contents as part of the transaction.

Regulation does not require that the security interest in contents be “perfected.”

One of the best discussions around content coverage was included in the Second Issue (2022) of Consumer Compliance Outlook

https://www.consumercomplianceoutlook.org/2022/second-issue/commercial-flood-insurance-compliance/

4

Compliance Conversations

AML/CFT (BSA) & Fraud

Staying informed on the Anti-Money Laundering/Countering the Financing of Terrorism (BSA) & Fraud risks helps financial institutions better detect & prevent money laundering, terrorist financing, & other illicit financial activities.

Compliance Conversations
AML/CFT (BSA) & Fraud

RFI – Payments & Check Fraud

90 FR 26293–26298
06/20/25
Comments Due
09/18/25

About the Fed | News & Events | Monetary Policy | Supervision & Regulation | Financial Stability | Payment Systems | Econom Researc

Joint Press Release

June 16, 2025

Federal bank regulatory agencies seek comment to address payments and check fraud

Federal Deposit Insurance Corporation

Federal Reserve Board

Office of the Comptroller of the Currency

For release at 5:00 p.m. EDT

Share

The federal bank regulatory agencies today announced a request for comment on potential actions to help consumers, businesses, and financial institutions mitigate risk of payments fraud, with a particular focus on check fraud. For purposes of the request for information, payments fraud generally refers to the use of illegal means to make or receive payments for personal gain, including scams.

Because payments fraud may involve multiple institutions and payment methods, no single agency or private-sector entity can address payments fraud on its own. Therefore, the agencies are seeking public comment on discrete actions, collectively or independently, to mitigate payments fraud, including check fraud, within their respective bank regulation and payments authorities.

Compliance Conversations
AML/CFT (BSA) & Fraud

RFI – Payments & Check Fraud (cont.)

Input is requested on five potential areas for improvement and collaboration:

- External collaboration among the agencies, Federal Reserve Banks, and industry stakeholders;
- Consumer, business, and industry education by the agencies and Federal Reserve Banks to educate about payments fraud;
- Regulation and supervision to mitigate payments fraud, including opportunities the Board may have related to check fraud;
- Payments fraud data collection and information sharing; and
- Federal Reserve Banks' operator tools and services to reduce payments fraud.

In addition to seeking public input, the agencies will also continue looking for additional opportunities to effectively collaborate across other state and federal agencies given the importance of interagency coordination to help mitigate payments fraud.

Alternative TIN Collection Method – CIP

ORDER

ORDER granting an exemption for all accounts at all banks subject to the jurisdiction of the Agencies from a Customer Identification Program (CIP) Rule requirement implementing section 326 of the USA PATRIOT Act, 31 U.S.C. § 5318(l) related to a bank obtaining Taxpayer Identification Number (TIN) information from the customer. The exemption in this ORDER permits a bank to use an alternative collection method to obtain TIN information from a third-party rather than from the customer, provided that the bank otherwise complies with the CIP Rule, which requires written procedures that: (1) enable the bank to obtain TIN information prior to opening an account; (2) are based on the bank's assessment of the relevant risks; and (3) are risk-based for the purpose of verifying the identity of each customer to the extent reasonable and practicable, enabling the bank to form a reasonable belief that it knows the true identity of each customer.[1]

Alternative TIN Collection Method – CIP (cont.)

Issue Date: June 27, 2025

By ORDER, under the authority set forth in 31 C.F.R. § 1020.220(b) implementing section 326(a) of the USA PATRIOT Act, 31 U.S.C. § 5318(l)(5), the Office of the Comptroller of the Currency (OCC), the Federal Deposit Insurance Corporation (FDIC), and the National Credit Union Administration (NCUA) (each an "Agency" and collectively the "Agencies"), with the concurrence of the Financial Crimes Enforcement Network (FinCEN), hereby grant an exemption from a requirement of the CIP Rule implementing section 326 of the USA PATRIOT Act, 31 U.S.C. § 5318(l), in the circumstances specified below.[2] Specifically, this ORDER provides an exemption from the requirement for banks subject to the jurisdiction of the Agencies[3] to obtain TIN[4] information from the customer prior to opening an account in the situations discussed herein.[5] This ORDER permits banks, for all accounts[6] at all banks (and their subsidiaries[7]) subject to the Agencies' jurisdiction, to instead use an alternative collection method to obtain TIN information from a third-party source rather than the customer, provided

Alternative TIN Collection Method – CIP (cont.)

that the bank otherwise complies with the CIP Rule, which requires written procedures that: (1) enable the bank to obtain TIN information prior to opening an account; (2) are based on the bank's assessment of the relevant risks; and (3) are risk-based for the purpose of verifying the identity of each customer to the extent reasonable and practicable, enabling the bank to form a reasonable belief that it knows the true identity of each customer. The use of this exemption by banks is optional; banks are not required to use an alternative collection method for TIN information.

Section 2313a Orders – 06/25/25

Issued: June 25, 2025

Subject: Section 2313a Orders Prohibit Certain Transmittals of Funds Involving CIBanco, Intercam, and Vector

On June 25, 2025, FinCEN issued three orders, pursuant to 21 U.S.C. 2313a[1] (section 2313a), finding, respectively, CIBanco S.A., Institutión de Banca Multiple (CIBanco)[2], Intercam Banco S.A., Institución de Banca Multiple (Intercam)[3], and Vector Casa de Bolsa, S.A. de C.V. (Vector),[4] to be financial institutions operating outside of the United States that are of primary money laundering concern in connection with illicit opioid trafficking. These orders further impose a prohibition on certain transmittals of funds involving CIBanco, Intercam, or Vector by any covered financial institution (see question 6). These are the first orders issued under section 2313a.

FinCEN expects covered financial institutions to: (1) implement procedures to ensure compliance with the terms of the orders; and (2) exercise reasonable due diligence to prevent engaging in transmittals of funds involving CIBanco, Intercam, or Vector.

Section 2313a Orders – 06/25/25 (cont.)

1) What is section 2313a?

In 2024, Congress enacted the FEND Off Fentanyl Act,[5] which, among other things, added 21 U.S.C. 2313a. Section 2313a grants the Secretary of the Treasury (Secretary) the authority to make a finding that "reasonable grounds exist for concluding" that any of the following is of primary money laundering concern in connection with illicit opioid trafficking:

(i) One or more financial institutions operating outside of the United States;

(ii) One or more classes of transactions within, or involving, a jurisdiction outside of the United States; or

(iii) One or more types of accounts within, or involving, a jurisdiction outside of the United States.[6]

Upon making such a finding, the Secretary is authorized to require domestic financial institutions and domestic financial agencies to take certain "special measures." The six special measures are safeguards that may be employed to defend the United States financial system from money laundering risks connected to illicit opioid trafficking.[7] The Secretary may impose one or more of these special measures to protect the U.S. financial system from such threats. The authority of the Secretary to administer section 2313a has been delegated to FinCEN.[8]

Section 2313a Orders – 06/25/25 (cont.)

06/30/25

CIBanco – 90 FR 27770–27777

Intercam Banco S.A. –
90 FR 27777–27783

Vector Casa de Bolsa S.A. de C.V.
90 FR 27763–27770

Effective 07/21/25

3. Transmittals of Funds

The order defines transmittals of funds as the sending and receiving of funds, including convertible virtual currency.

4. Meaning of Other Terms

All terms used but not otherwise defined herein shall have the meaning set forth in 31 CFR Chapter X, 31 U.S.C. 5312, and 21 U.S.C. 2302.

B. Prohibition on Transmittals of Funds Involving CIBanco

A covered financial institution is prohibited from engaging in any transmittal of funds from or to CIBanco.

Compliance Conversations
AML/CFT (BSA) & Fraud

311's, 9714a's, & 2313a's

- Burma (Myanmar);
- Democratic People's Republic of Korea (North Korea);
- Islamic Republic of Iran

➢Vector Casa de Bolsa, S.A. de C.V. – 06/30/25 - § 2313a;

➢CLBanco S.A. – 06/30/25 - § 2313a;

➢Intercam Banco S.A., Institucio'n de Banca Multiple – 06/30/25 - § 2313a

- Al-Huda Bank – 07/03/24, 89FR55051-55055;
- Bank of Dandong;
- Bitzlato - § 9714a – 01/23/23;
- Commercial Bank of Syria – removed 05/23/25;
- FBME Bank Ltd;
- Halawi Exchange Company;
- Huione Group – 05/05/25 – 90FR18934 – 18949
- Kassem Rmeiti & Co for Exchange.
- PM2BTC – § 9714a – 10/11/24 – 89FR82499 - 82506

Compliance Conversations
AML/CFT (BSA) & Fraud

FATF – "High-Risk Jurisdictions" (Black List) // Jurisdictions under Increased Monitoring (Gray List) – 06/13/25

- Call to Action:
  - Countermeasures: Democratic People's Republic of North Korea & Iran – all jurisdictions are encouraged to follow FATF statement of 02/20/20 & Executive Orders (E.O.s) 13810, 13949, & 13876, & apply effective counter-measures to protect their financial sectors from ML/FT risks emanating from North Korea & Iran.

  - EDD – Myanmar – (In 02/2020 Myanmar added to Due Diligence section – due to lack of progress & most action items were not addressed one year after the deadline – focus elevated in 10/2022)

- Jurisdictions Under Increased Monitoring –
  - Due Diligence/Commitments Made – *Strategic Deficiencies* Noted: Algeria; Angola; Bolivia; Bulgaria; Burkina Faso; Cameroon; Cote D'Ivoire; Democratic Republic of Congo (DRC); Haiti; Kenya; Lao PDR; Lebanon; Monaco; Mozambique; Namibia; Nepal; Nigeria; South Africa; South Sudan; Syria; Venezuela; Vietnam; Virgin Islands (UK); & Yemen.

  - Commitments Satisfied – Croatia; Mali; Tanzania.

Compliance Conversations
AML/CFT (BSA) & Fraud

FTC – Military Consumer Month 2025

Compliance Conversations
AML/CFT (BSA) & Fraud

FTC – Military Consumer Month 2025 (cont.)

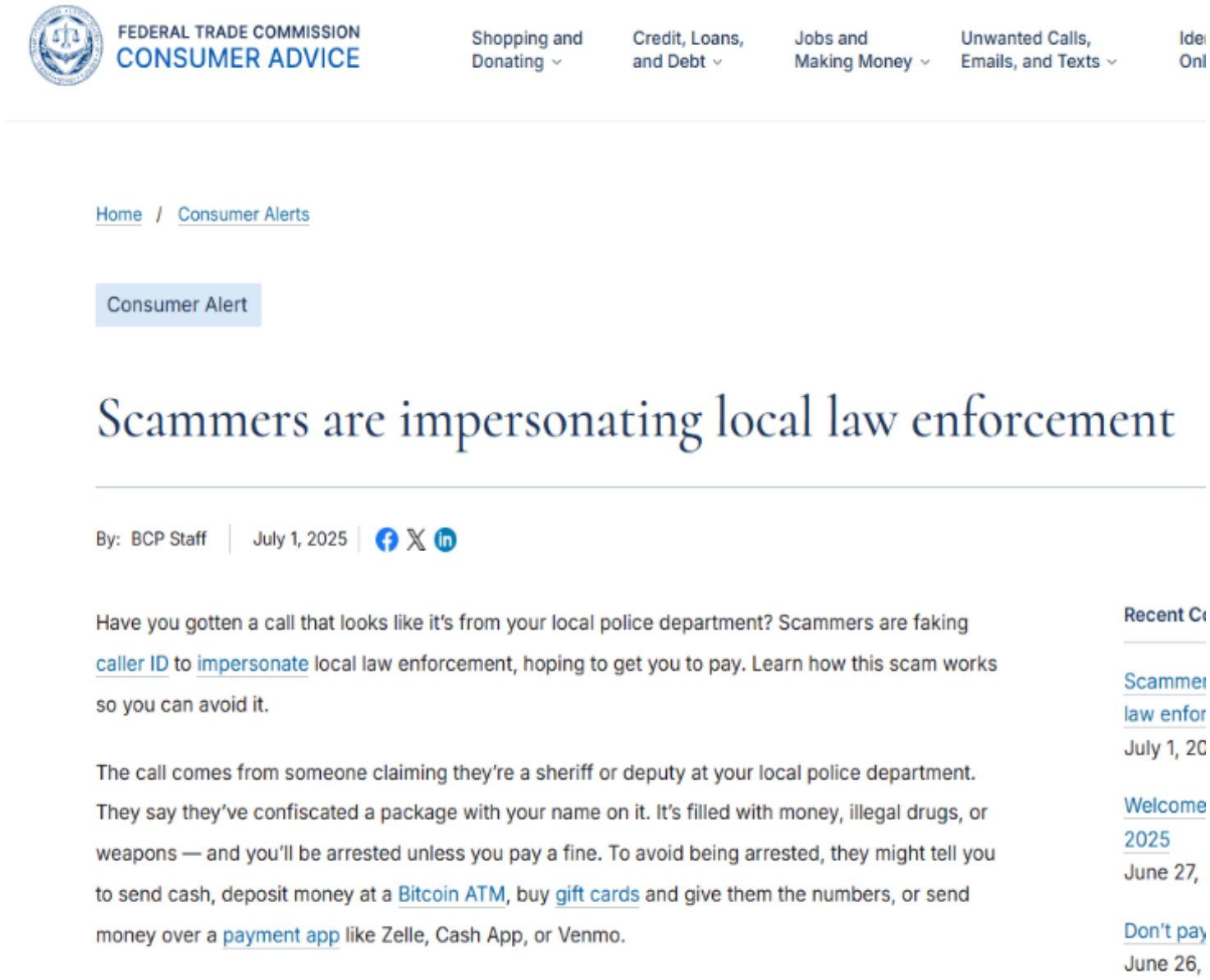
Sometimes people don't even know they've experienced a scam until they've already lost money. Military consumers reported losing $584 million to fraud in 2024 — an enormous loss. That's why, throughout the month of July, the FTC is giving you tools to raise the volume on practical advice to help yourself — and your buddies — spot, avoid, and report scams. Here's where to start:

- At your next battalion huddle, bring up a scammy text about problems with an online order or money owed on an account. Use it to explain how **scammers send unexpected messages** to steal your personal information and your money.
- Before a deployment, brief your loved ones about **scammers that use social media** to send urgent messages about fake problems or supposed once-in-a-lifetime investment opportunities.
- Remind older veterans in your community to **slow down** before responding to unexpected phone calls and emails. Tell them only **scammers insist you pay in specific ways**, like using cryptocurrency, wiring money through a company like MoneyGram or Western Union, using a payment app, or by putting money on a gift card.
- Know someone who accidentally paid a scammer? Show them how to try and get their money back.

Check MilitaryConsumer.gov/MCM2025 every week in July to get graphics, blogs, and social media messages to start conversations like these. Encourage everyone you know to report scams to the FTC at ReportFraud.ftc.gov.

Compliance Conversations
AML/CFT (BSA) & Fraud

FTC Fraud Data – Law Enforcement Impersonation



FEDERAL TRADE COMMISSION
CONSUMER ADVICE

Shopping and Donating | Credit, Loans, and Debt | Jobs and Making Money | Unwanted Calls, Emails, and Texts | Ide Onl

Home / Consumer Alerts

Consumer Alert

Scammers are impersonating local law enforcement

By: BCP Staff | July 1, 2025

Have you gotten a call that looks like it's from your local police department? Scammers are faking caller ID to impersonate local law enforcement, hoping to get you to pay. Learn how this scam works so you can avoid it.

The call comes from someone claiming they're a sheriff or deputy at your local police department. They say they've confiscated a package with your name on it. It's filled with money, illegal drugs, or weapons — and you'll be arrested unless you pay a fine. To avoid being arrested, they might tell you to send cash, deposit money at a Bitcoin ATM, buy gift cards and give them the numbers, or send money over a payment app like Zelle, Cash App, or Venmo.

Recent C

Scammer law enfor July 1, 20

Welcome 2025 June 27,

Don't pay June 26,

forvis mazars

FTC Fraud Data – Law Enforcement Impersonation (cont.)

Even if the caller uses the name of a real officer, has a real number show up on caller ID, or has information about you (like your address), that's not a real officer calling. It's a scammer trying to steal your money. Here's what to know:

- Real law enforcement officers won't call to say you're going to be arrested (or threaten to arrest you if you hang up).
- Real law enforcement officers won't call to insist that you pay fines by cash, gift card, cryptocurrency, payment app, or a wire transfer service — and never as a way to buy your way out of a "crime."

If you get a call like this, hang up. Don't call the number back. If you want to check it out, contact your local police department, but use a website or phone number you know is real. Then report it to the FTC at ReportFraud.ftc.gov.

Compliance Conversations
AML/CFT (BSA) & Fraud

FTC Fraud Data – Text Scams

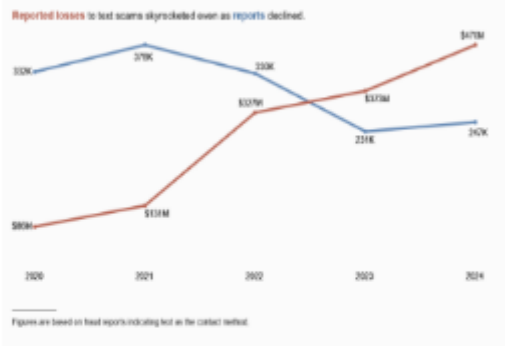
New FTC Data Show Top Text Message Scams of 2024; Overall Losses to Text Scams Hit $470 Million

Fake package delivery issues and phony job opportunities were most frequently reported

April 16, 2025

Tags: Consumer Protection | Bureau of Consumer Protection | Consumer Sentinel Network

New data from the Federal Trade Commission show that in 2024, consumers reported losing $470 million to scams that started with text messages. This amount is five times higher than what was reported in 2020, even though the number of reports declined.



The most commonly reported type of text scam was fake package delivery, where scammers send alerts about a supposed issue with an incoming delivery. Bogus job opportunities were also common, including "task scams," which involve promises of online work requiring people to complete a series of online tasks and end up with requests for people to invest their own money.

Related resources

Data Spotlight: Top text scams of 2024

For Consumers

Blog: Is that unexpected text a scam?

For Businesses

Blog: New FTC Data Spotlight highlights text scams that may target your business

Topics

Report Identity Theft

FTC Fraud Data – Text Scams (cont.)

1) Fake package delivery problems

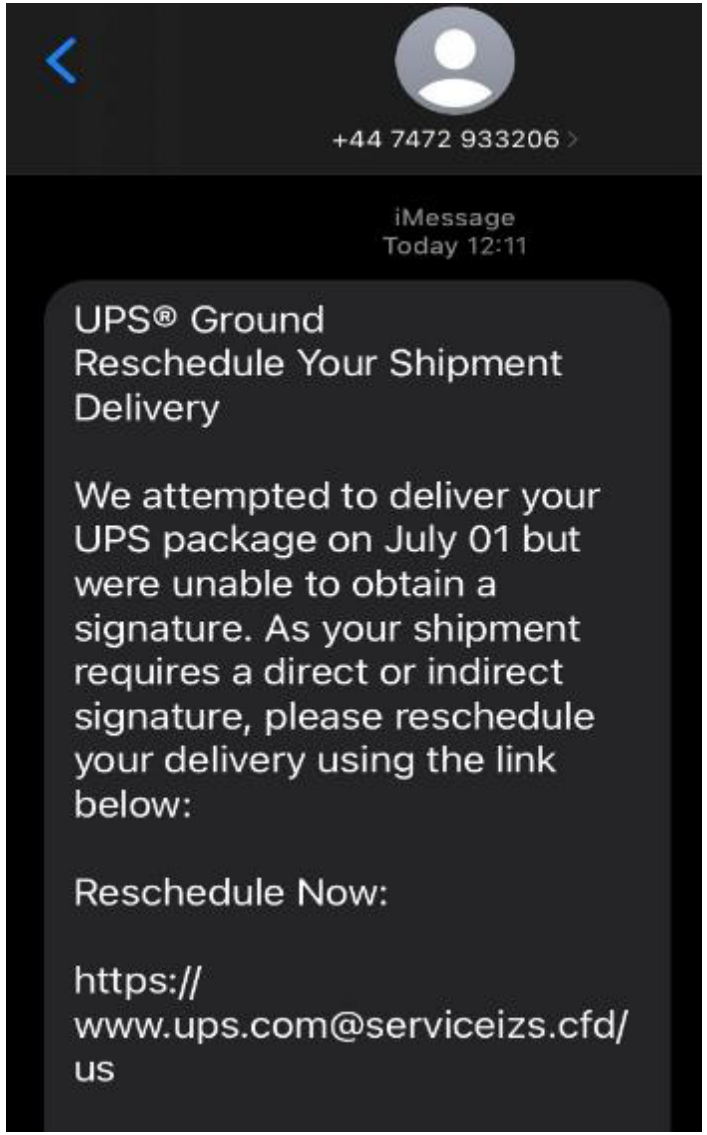
Messages about package deliveries, usually from someone pretending to be from the U.S. Postal Service, were the most reported text scam last year. These messages say there's a problem with a delivery and link to a website that looks like the real USPS site – but isn't. Many people reported paying a small "redelivery fee" that turned out to be a trick to get their credit card or even Social Security number.

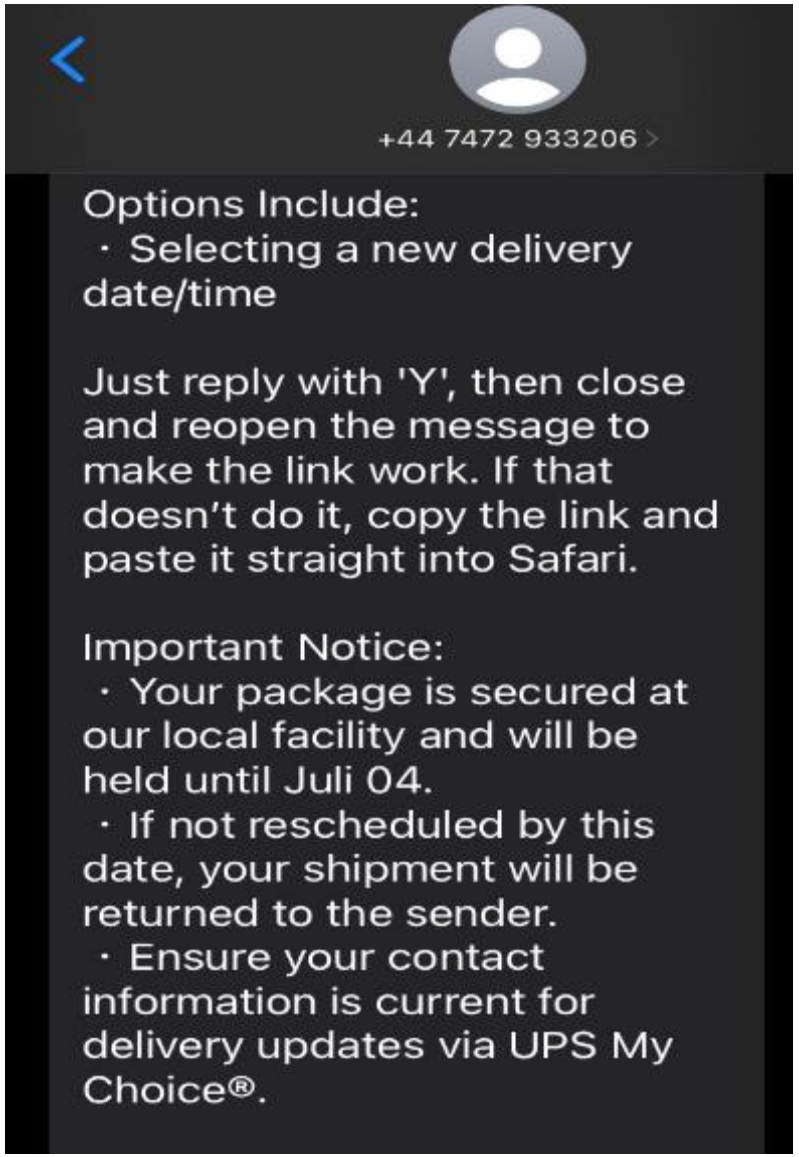
2) Phony job opportunities

Scammers posing as recruiters to take people's money isn't new. But in 2024, reports of a new "task scam" took off.[5] These scams often start with an unexpected text offering work without specifics. The "job" is to complete simple repetitive tasks like rating products or apps. But it's all fake. At some point, people are told to send money to finish their tasks and withdraw their supposed earnings. But people who sent money said that they didn't get it back.

Compliance Conversations
AML/CFT (BSA) & Fraud

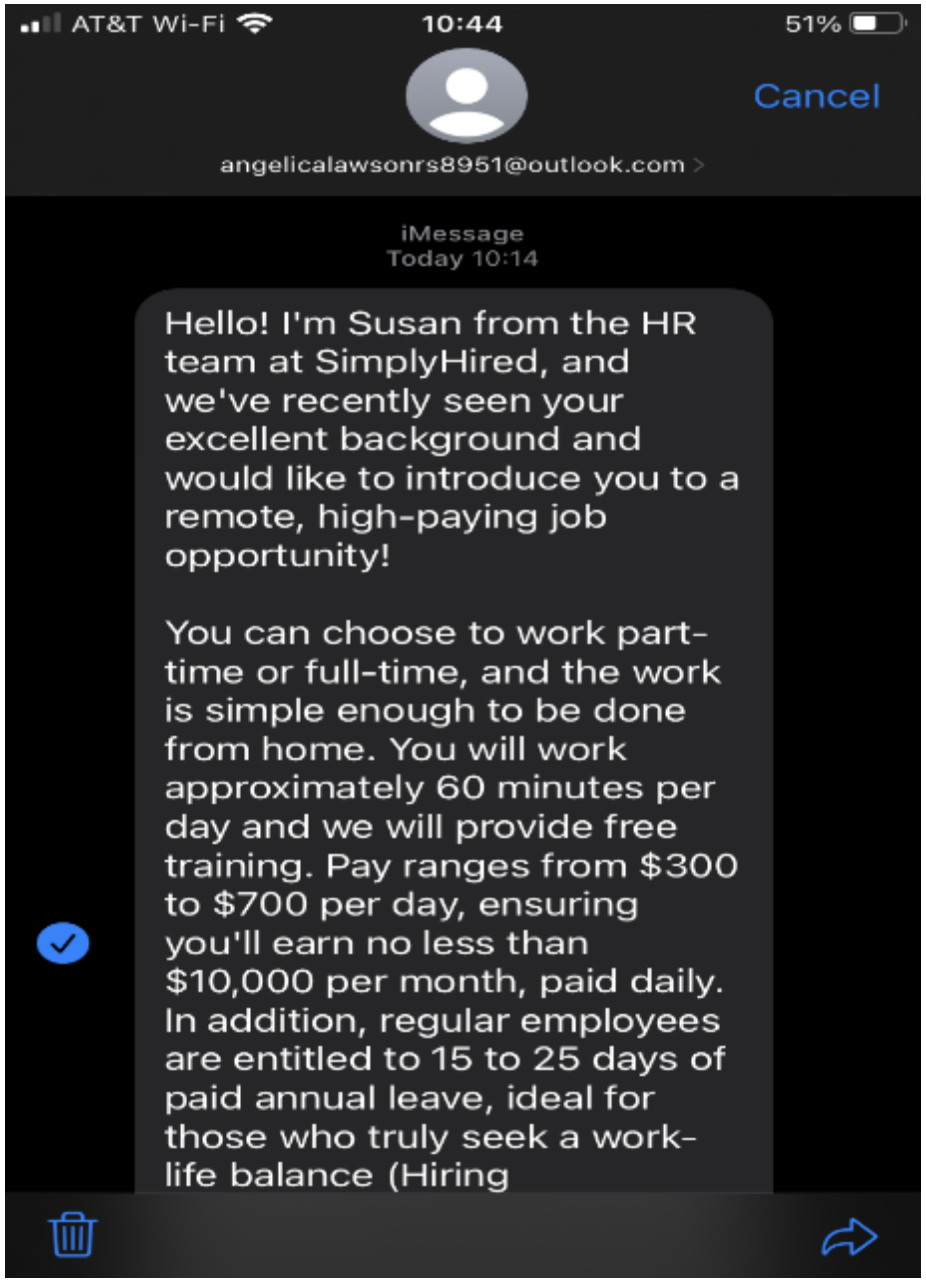
FTC Fraud Data – Text Scams (cont.)





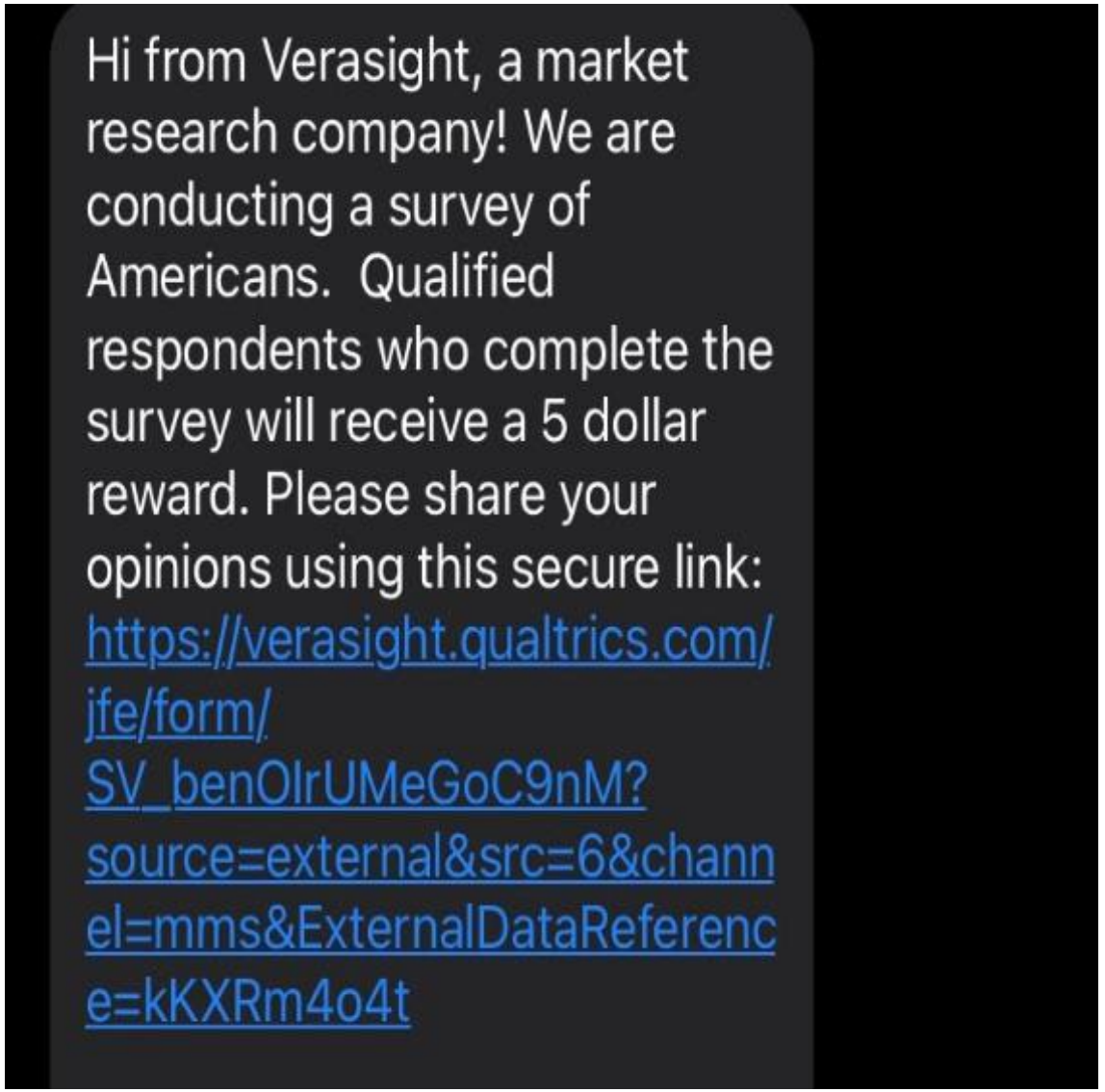
Compliance Conversations
AML/CFT (BSA) & Fraud

FTC Fraud Data – Text Scams (cont.)



Compliance Conversations
AML/CFT (BSA) & Fraud

FTC Fraud Data – Text Scams (cont.)



FTC Fraud Data – Text Scams (cont.)

3) Fake fraud alerts

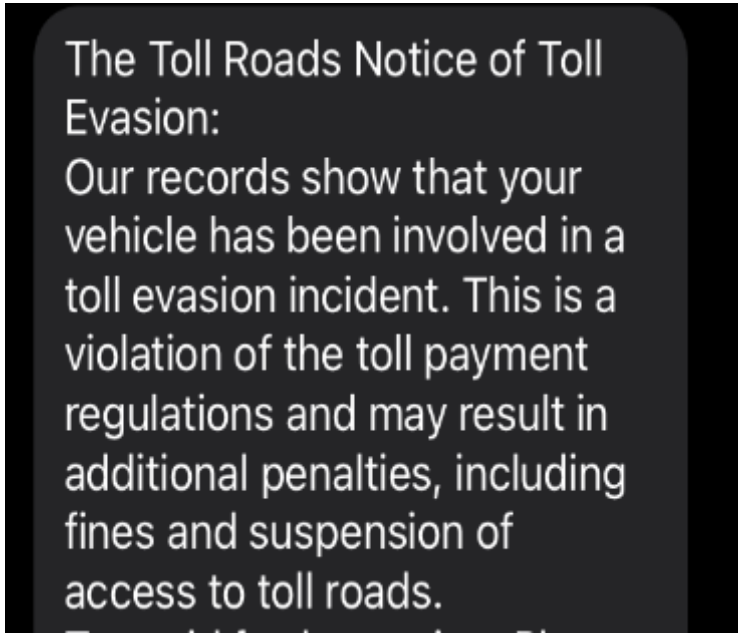
Many people reported texts about so-called suspicious activity or a big purchase they didn't make. These texts often look like they're from a bank or Amazon. They might give a number to call. Or they might say to reply YES or NO to verify a large transaction. People who reply are connected to the (fake) fraud department for "help" fixing the made-up problem. These scammers quickly up the ante, often telling people all their money is at risk. The scammers then pressure people into moving money out of their accounts to supposedly keep it safe, but it really goes to the scammers. And people who move that money do not get any of it back.

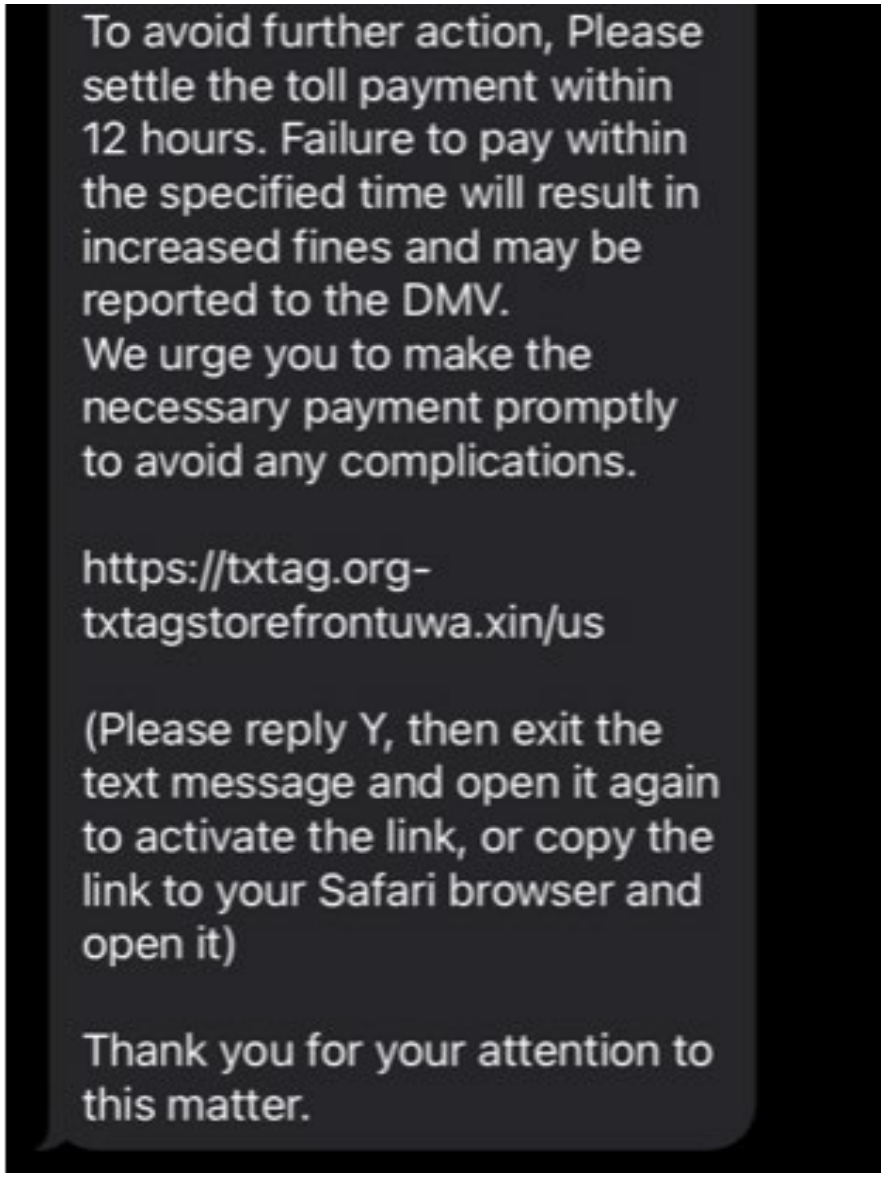
4) Bogus notices about unpaid tolls

Scammers are sending texts that look like they're from highway toll programs all over the country, from SunPass in Florida to FasTrak in San Francisco. These scammers tell people to click a link to pay an unpaid balance, but neither the charges nor the message are legit. Reports show these scammers are really after credit card and even Social Security numbers.

Compliance Conversations
AML/CFT (BSA) & Fraud

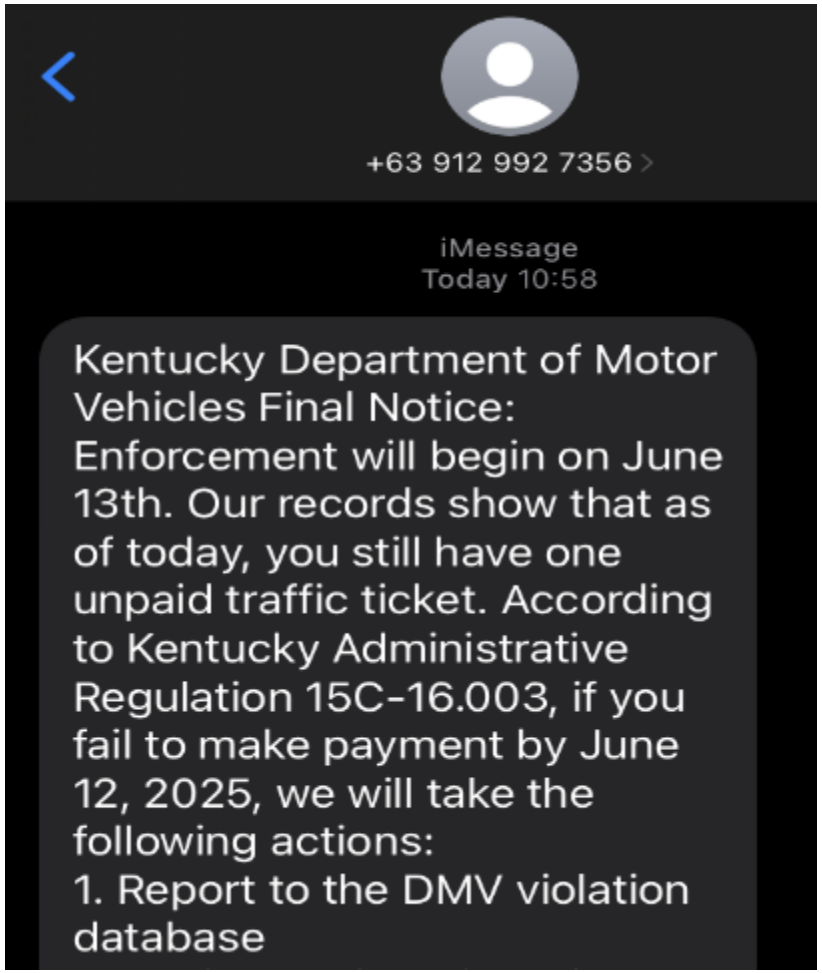
FTC Fraud Data – Text Scams (cont.)

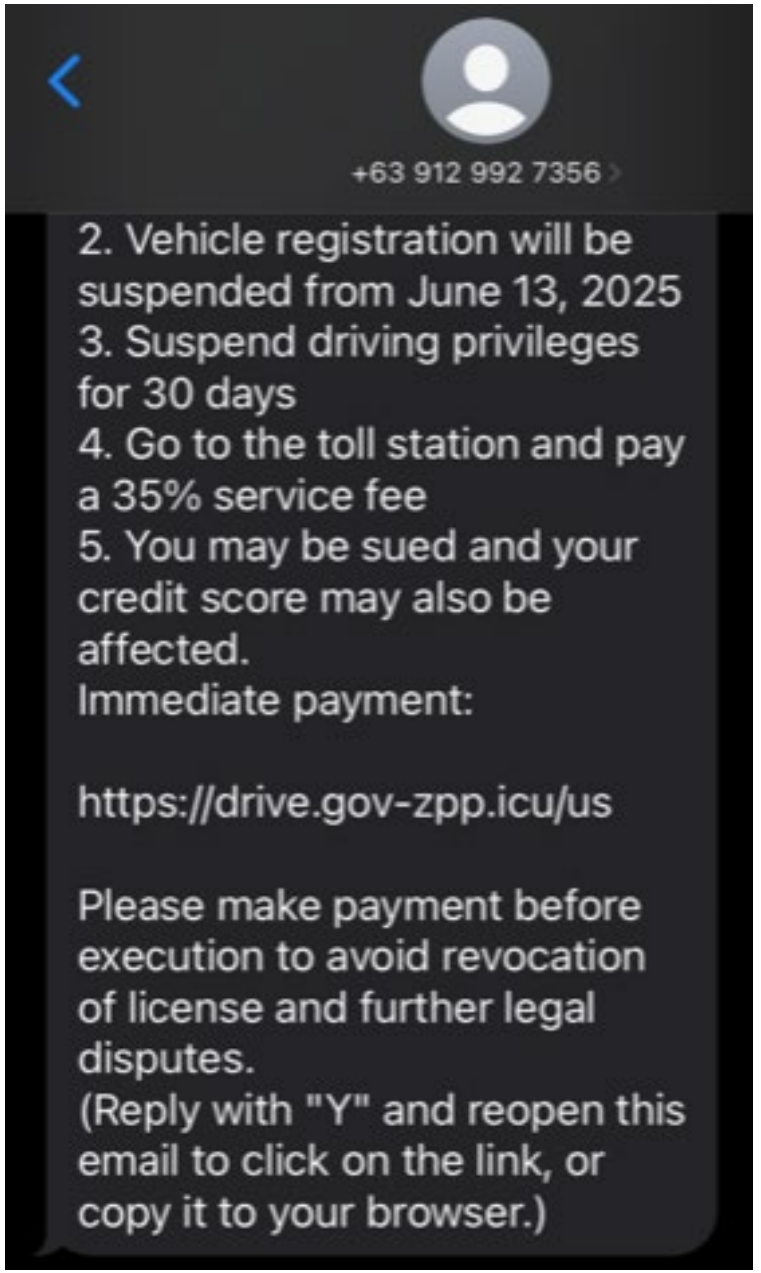




Compliance Conversations
AML/CFT (BSA) & Fraud

FTC Fraud Data – Text Scams (cont.)



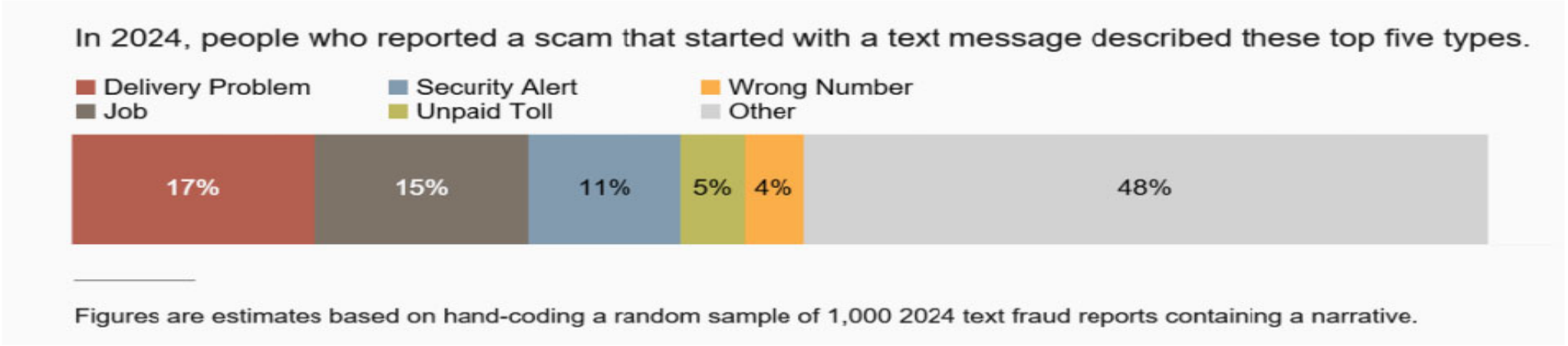


Compliance Conversations
AML/CFT (BSA) & Fraud

FTC Fraud Data – Text Scams (cont.)

5) "Wrong number" texts that aren't

Wrong number scams start with an out-of-the-blue message that looks innocent enough – it might just say "hello" or "do you want to get a coffee?" But a simple act of kindness – responding to let a stranger know they have the wrong number – can be the start of a very costly scam. Reports show these scammers strike up a fake friendship, often with romantic undertones. Next, they claim to be successful investors, offering to share their tricks and directing people to bogus investment platforms. People report losing all the money they "invest," often tens of thousands of dollars.



Compliance Conversations
AML/CFT (BSA) & Fraud

2025 World Drug Report

Compliance Conversations
AML/CFT (BSA) & Fraud

2025 World Drug Report (cont.)

United Nations | Office on Drugs and Crime

Search the site

Topics | What we do | Information For | About us | Field Offices | Quick Links | Executive Director | Media Centre

PRESS RELEASE

UNODC World Drug Report 2025: Global instability compounding social, economic and security costs of the world drug problem

Vienna, 26 June 2025

A new era of global instability has intensified challenges in addressing the world drug problem, empowering organized crime groups and pushing drug use to historically high levels, says the UN Office on Drugs and Crime (UNODC) in the World Drug Report 2025 launched today.

"This edition of the World Drug Report shows that organized drug trafficking groups continue to adapt, exploit global crises, and target vulnerable populations," said Ghada Waly, Executive Director of UNODC. "We must invest in prevention and address the root causes of the drug trade at every point of the illicit supply chain. And we must strengthen responses, by leveraging technology, strengthening cross-border cooperation, providing alternative livelihoods, and taking judicial action that targets key actors driving these networks. Through a comprehensive, coordinated approach, we can dismantle criminal organizations, bolster global security, and protect our communities."

316 million people used a drug (excluding alcohol and tobacco) in 2023, or six per cent of the population aged between 15 and 64, compared to 5.2 per cent of the population in 2013. With 244 million users, cannabis remains the most widely used drug, followed by opioids (61 million), amphetamines (30.7 million), cocaine (25 million) and ecstasy (21 million). New groups of vulnerable people fleeing hardship, instability and conflict could cause these numbers to increase further, the report warns.

The report includes special chapters on drug trafficking and organized crime; the impact of drug use on the health of people who use drugs, their families, communities, and society; and the impact of drugs on the environment in Europe.

Compliance Conversations
AML/CFT (BSA) & Fraud

2025 World Drug Report (cont.)

Global cocaine market breaking its own records

Production, seizures, and use of cocaine all hit new highs in 2023, making cocaine the world's fastest-growing illicit drug market. Illegal production skyrocketed to 3,708 tons, nearly 34 per cent more than in 2022. Global cocaine seizures reached a record high at 2,275– a 68 per cent rise over 2019-2023. Use of cocaine, meanwhile, has grown from 17 million users in 2013 to 25 million users in 2023.

Cocaine traffickers are breaking into new markets across Asia and Africa, the report notes. The vicious violence and competition characterizing the illicit cocaine arena, once confined to Latin America, is now spreading to Western Europe as organized crime groups from the Western Balkans increase their influence over the market.

Synthetic drug market continues to expand

Due to factors like low operational costs and reduced risks of detection, the synthetic drug market continues to expand globally, dominated by Amphetamine-type stimulants (ATS) like methamphetamine and amphetamine (including "captagon"). Seizures of ATS reached a record high in 2023 and accounted for almost half of all global seizures of synthetic drugs, followed by synthetic opioids, including fentanyl.

The fall of the Assad regime in Syria has created uncertainty around the future of the captagon trade. Following the political transition, large captagon manufacturing sites in the country were uncovered. Though the discovery could possibly disrupt the drug's supply, the latest seizure data from 2024 and 2025 confirm that captagon is continuing to flow -primarily to countries of the Arabian peninsula – possibly indicating the release of previously-accumulated stockpiles or continued production in different locations.

Drug trafficking brings in staggering profits

Though estimates vary, the illicit drug trade generates hundreds of billions of dollars per year. Criminal groups innovate constantly, through boosting production, finding new ways to chemically conceal their drugs, and using technology to conceal communications and increase distribution.

Though resilient, organized criminal networks can be disrupted – but a deeper understanding of the aims and structures of drug trafficking groups is required. Mapping criminal groups can highlight their vulnerabilities, key actors, enablers, and pinpoint possible areas for intervention. Law enforcement agencies could also consider investing in technology and skills training that matches the sophistication of tools used in the drug supply chain.

Compliance Conversations
AML/CFT (BSA) & Fraud

2025 World Drug Report (cont.)

Drug trafficking brings in staggering profits

Though estimates vary, the illicit drug trade generates hundreds of billions of dollars per year. Criminal groups innovate constantly, through boosting production, finding new ways to chemically conceal their drugs, and using technology to conceal communications and increase distribution.

Though resilient, organized criminal networks can be disrupted – but a deeper understanding of the aims and structures of drug trafficking groups is required. Mapping criminal groups can highlight their vulnerabilities, key actors, enablers, and pinpoint possible areas for intervention. Law enforcement agencies could also consider investing in technology and skills training that matches the sophistication of tools used in the drug supply chain.

Impact of drug use

Drug use disorders already impose a huge cost on individuals, communities, and health systems, and the rising turn away from multilateralism and reallocation of resources could intensify the problem, the report notes.

The cost of failing to tackle drug use disorders is steep – nearly half a million deaths and 28 million healthy years of life lost due to disability and premature deaths (DALY) in 2021. Just one in 12 people with drug use disorders were estimated to have received any form of drug treatment in 2023. Factors such as policies and availability of evidence-based health and social services can help mitigate the health impact of drug use on people and communities.

How drugs affect the environment

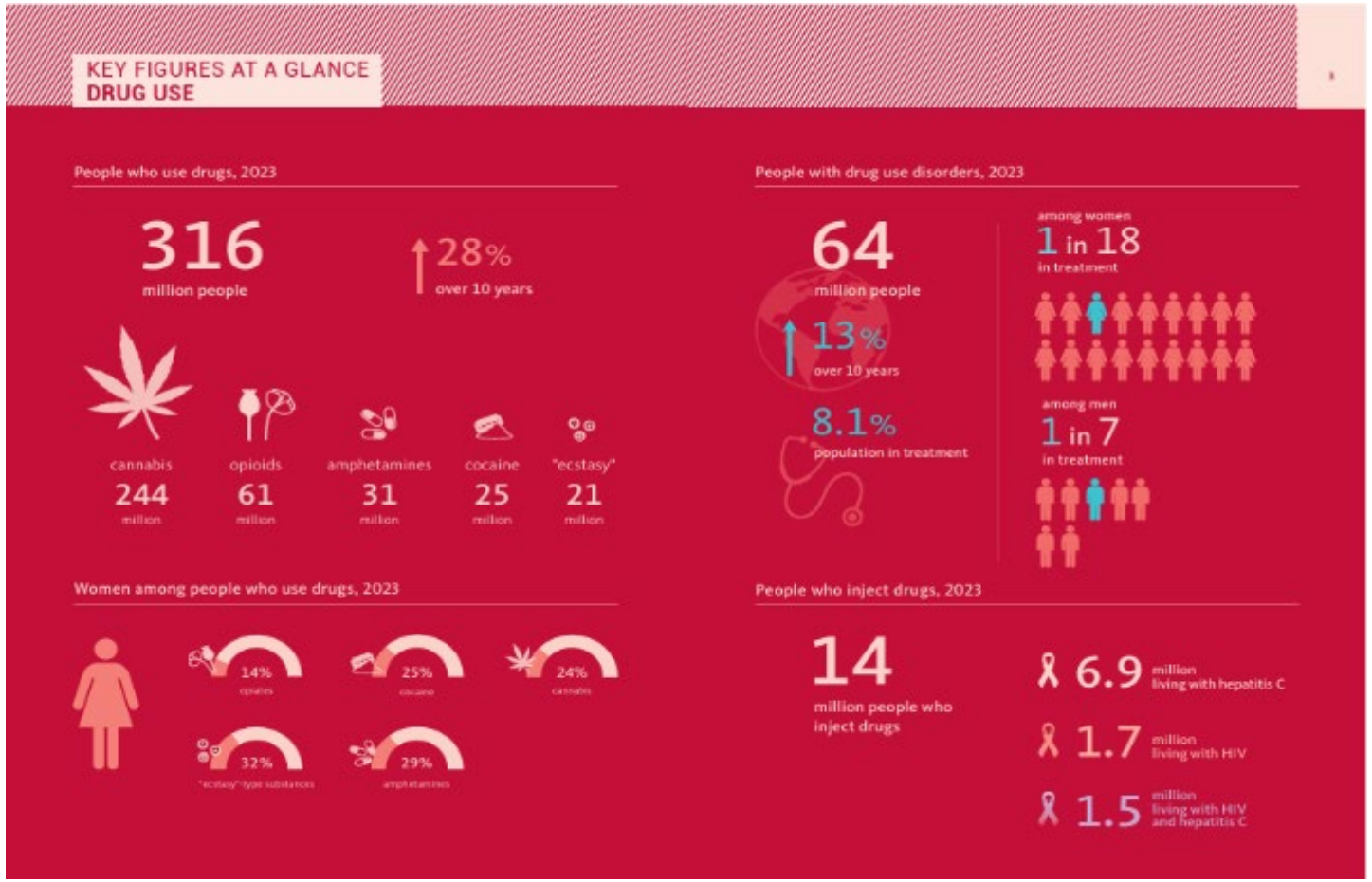
The report finds that drug use; drug cultivation and trafficking; and the policy responses enacted to address illicit drug economies are all impacting the environment in Europe. Potential consequences of drug cultivation/production can include deforestation and other land-use change as well as air, land and water pollution – which can be significant at the local level.

The number of dismantled clandestine drug laboratories increased in Europe between 2013 and 2023. This manufacture produces significant amounts of waste and can result in considerable clean-up and ecosystem restoration costs. Nevertheless, the report finds that environmental harm is not a priority when designing and implementing drug policy responses, and that much of the waste and other environmental impacts are unaccounted for.

Read the full report here: www.unodc.org/wdr

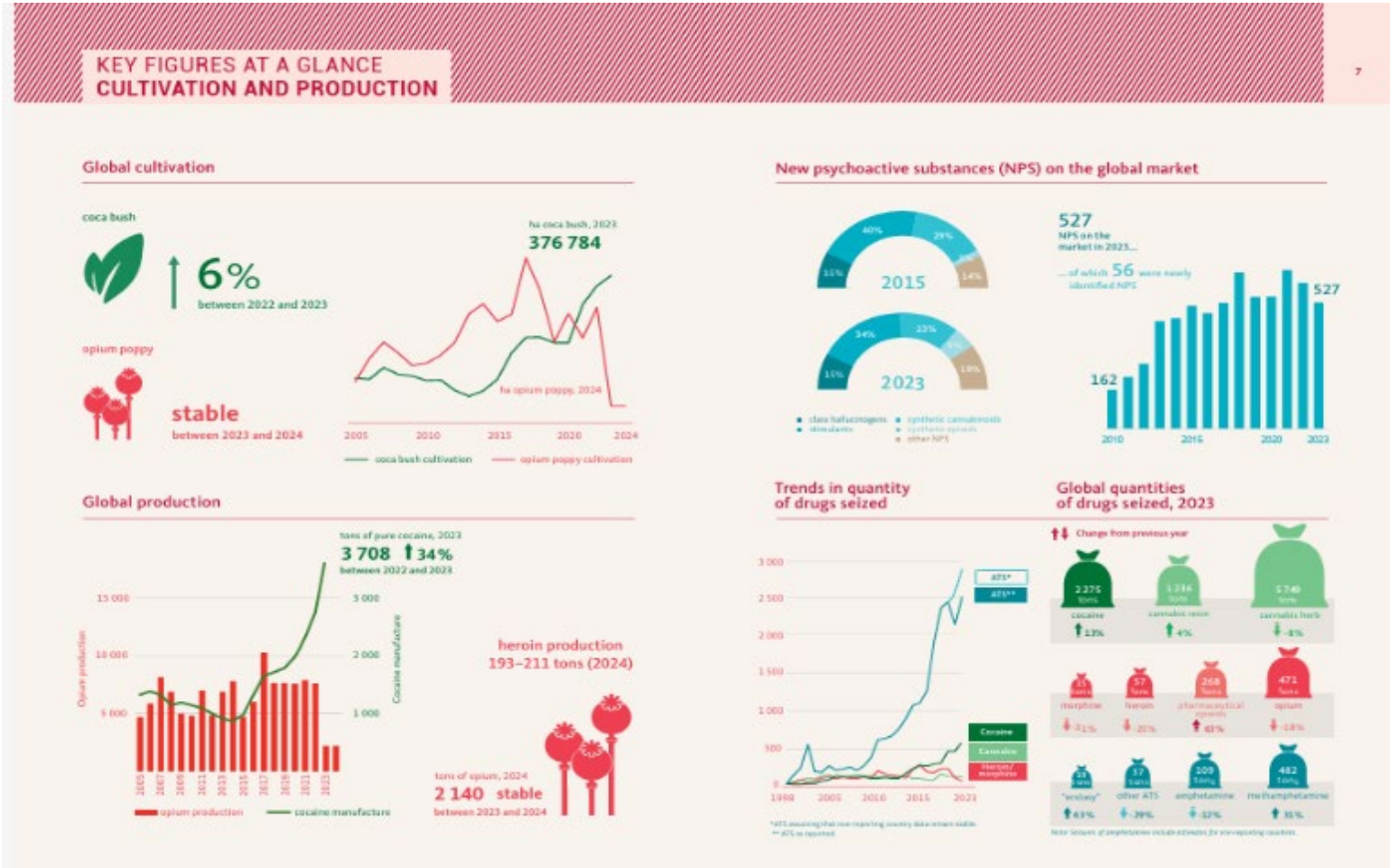
Compliance Conversations
AML/CFT (BSA) & Fraud

2025 World Drug Report (cont.)



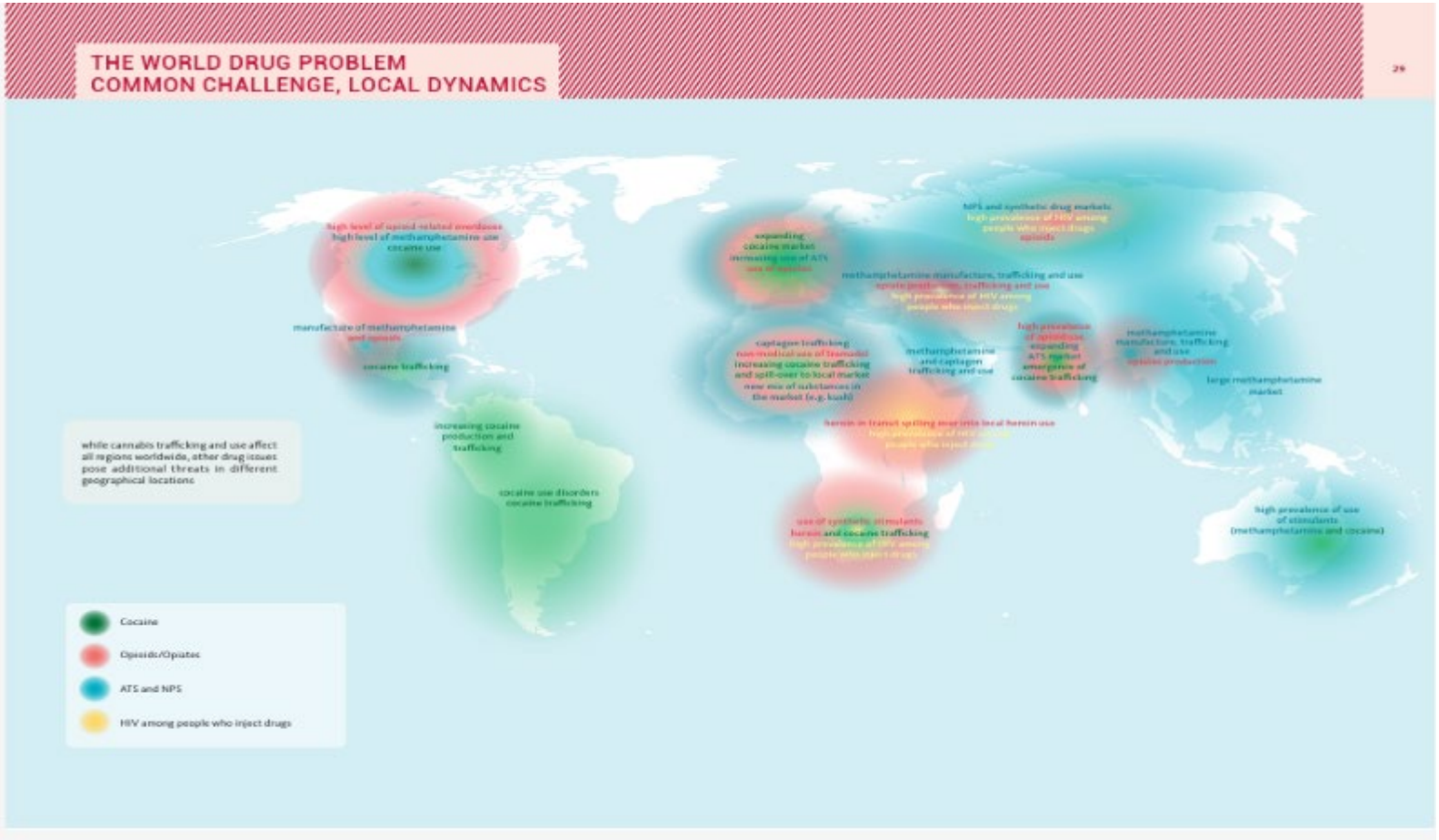
Compliance Conversations
AML/CFT (BSA) & Fraud

2025 World Drug Report (cont.)



Compliance Conversations
AML/CFT (BSA) & Fraud

2025 World Drug Report (cont.)



Compliance Conversations
AML/CFT (BSA) & Fraud

Latest FinCEN Advisories

FinCEN ADVISORY

FIN-2025-A002 June 6, 2025

FinCEN Advisory on the Iranian Regime's Illicit Oil Smuggling Activities, Shadow Banking Networks, and Weapons Procurement Efforts

Suspicious Activity Report (SAR) Filing Request: FinCEN requests that financial institutions reference this Advisory in SAR field 2 ("Filing Institution Note to FinCEN") and the narrative by including the key term "**IRAN-2025-A002.**"

Introduction

The U.S. Department of the Treasury's (Treasury) Financial Crimes Enforcement Network (FinCEN) is issuing this Advisory to assist U.S. financial institutions in identifying and reporting potential sanctions evasion and other suspicious activity related to the Islamic Republic of Iran (Iran). On February 4, 2025, President Trump issued National Security Presidential Memorandum (NSPM-2) announcing a maximum pressure campaign against Iran with the goals of denying Iran nuclear weapons and intercontinental ballistic missiles (ICBMs); countering its development of other weapons capabilities; neutralizing Iran's network and campaign of regional aggression; and disrupting, degrading, and denying Iran, including the Islamic Revolutionary Guard Corps (IRGC),[1] and its terrorist proxies, access to the resources that sustain their destabilizing activities.[2]

Compliance Conversations
AML/CFT (BSA) & Fraud

Latest FinCEN Advisories (cont.)

FinCEN ALERT

FIN-2025-Alert002 May 1, 2025

FinCEN Alert on Oil Smuggling Schemes on the U.S. Southwest Border Associated with Mexico-Based Cartels

Suspicious Activity Report (SAR) Filing Request:

FinCEN requests that financial institutions reference this Alert by including the key term "**FIN-2025-OILSMUGGLING**" 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), in coordination with Treasury's Office of Foreign Assets Control (OFAC) and the U.S. Drug Enforcement Administration (DEA), Federal Bureau of Investigation (FBI), and Homeland Security Investigations (HSI), is issuing this Alert to urge financial institutions[1] to be vigilant in detecting, identifying, and reporting suspicious activity connected to the smuggling of stolen crude oil from Mexico across the U.S. southwest border into the United States by the Jalisco New Generation Cartel (CJNG), Sinaloa Cartel, Gulf Cartel, and other Mexico-based transnational criminal organizations (TCOs) — frequently known as the "Cartels." In recent years, fuel theft in Mexico, including crude oil smuggling, has become the most significant non-drug illicit revenue source for the Cartels and enables them to sustain their global criminal enterprises and drug trafficking operations into the United States. This Alert is being issued in coordination with an OFAC sanctions action.[2]

According to U.S. law enforcement authorities, the Cartels are using complicit Mexican brokers in the oil and natural gas industry to smuggle and sell crude oil stolen from Mexico's state-owned energy company, Petróleos Mexicanos (Pemex),[3] to complicit, small U.S.-based oil and natural gas companies (hereafter "U.S. importers") operating near the U.S. southwest border. Through these schemes, the Cartels are stealing billions of dollars of crude oil from Pemex, fueling rampant violence and corruption across Mexico, and undercutting legitimate oil and natural gas companies in the United States.[4]

Compliance Conversations
AML/CFT (BSA) & Fraud

Latest FinCEN Advisories (cont.)

FinCEN ADVISORY

FIN-2025-A001 April 1, 2025

FinCEN Advisory on the Financing of the Islamic State of Iraq and Syria (ISIS) and its Global Affiliates

Suspicious Activity Report (SAR) Filing Request:

FinCEN requests that financial institutions reference this Advisory by including the key term "**ISIS-2025-A001**" in SAR field 2 (Filing Institution Note to FinCEN) and the narrative and select SAR field 33(a) (Terrorist Financing-Known or suspected terrorist/terrorist organization) and include the term

The Financial Crimes Enforcement Network (FinCEN) is issuing this Advisory to assist financial institutions in identifying and reporting suspicious activity related to the financing of the Islamic State of Iraq and Syria (ISIS).[1] ISIS is a Sunni terrorist organization that has conducted and inspired terrorist attacks worldwide for more than a decade, killing or injuring thousands of people.[2] The U.S. Department of the Treasury's (Treasury) 2024 National Terrorist Financing Risk Assessment notes that ISIS, which separated from al-Qa'ida (AQ) and declared itself a caliphate in 2014, remains a regional and global threat.[3]

Latest FinCEN Advisories (cont.)

Homegrown Violent Extremism Inspired by ISIS

ISIS advocates through videos and other English language propaganda for supporters to conduct attacks in the United States and Western countries and has specifically advocated for attacks against civilians, the military, law enforcement, and intelligence community personnel.[77] Actors who carry out these attacks are referred to as HVEs and are defined as individuals who live and operate in the United States and who advocate, are engaged in, or are preparing to engage in ideologically motivated terrorist activities inspired by foreign terrorist organizations (FTOs) like ISIS or their ideologies but who act independently of direction by an FTO.[78] Furthermore, according to DHS, ISIS online media groups have used the Israel-Hamas conflict to encourage attacks against the West and Jewish and Christian communities. ISIS media outlets have also capitalized on recent attacks in Europe in attempts to inspire more violent action.[79]

Since 2015, HVEs have shown an interest in a wide range of targets, including law enforcement, U.S. military, and civilian targets. HVEs are most likely to use easy-to-acquire weapons such as firearms and edged weapons and will also occasionally use vehicles.[80] According to the FBI, attackers inspired by FTOs who have conducted vehicle attacks in the United States and abroad have used rented, stolen, and personally owned vehicles.[81]

Latest FinCEN Advisories (cont.)

FinCEN ALERT

FIN-2025-Alert001 March 31, 2025

FinCEN Alert on Bulk Cash Smuggling and Repatriation by Mexico-Based Transnational Criminal Organizations

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-2025-BULKCASH**" and select SAR field 36(z) (Money Laundering – Other) and include the term "**BULKCASH**" in the text box.

The U.S. Department of the Treasury's (Treasury) Financial Crimes Enforcement Network (FinCEN) is issuing this Alert to financial institutions,[1] urging them to be vigilant in identifying and reporting transactions potentially related to the cross-border smuggling of bulk cash[2] from the United States into Mexico and the repatriation of bulk cash into the U.S. and Mexican financial systems by Mexico-based transnational criminal organizations (TCOs). This Alert highlights one of several typologies that TCOs use to launder illicit proceeds generated in the United States through the cross-border movement of cash.[3]

Compliance Conversations
Bank Secrecy Act & Fraud

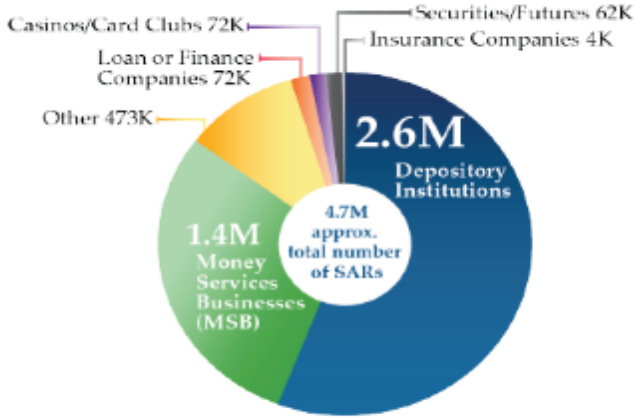
2024 FinCEN Year-In-Review

Reports Pursuant to the BSA

FinCEN receives reports from approximately 324,000 registered financial institutions and other e-filers in support of criminal justice and national security objectives.[2]

Forms	FY 2022	FY 2023	FY 2024	Average Daily Filings FY24
Suspicious Activity Reports (SARs)	4.3M	4.6M	4.7M	12,870
Currency Transaction Reports (CTRs)	20.6M	20.8M	20.5M	56,160
Currency and Other Monetary Instrument Reports (CMIRs)	128,100	143,200	152,100	417
Reports of Cash Payments >$10K Received in a Trade or Business (Form 8300)	431,800	421,500	470,400	1,290
Foreign Bank and Financial Accounts (FBARs)	1.5M	1.6M	1.7M	4,660

FY24 SARs by Type of Financial Institution[3]



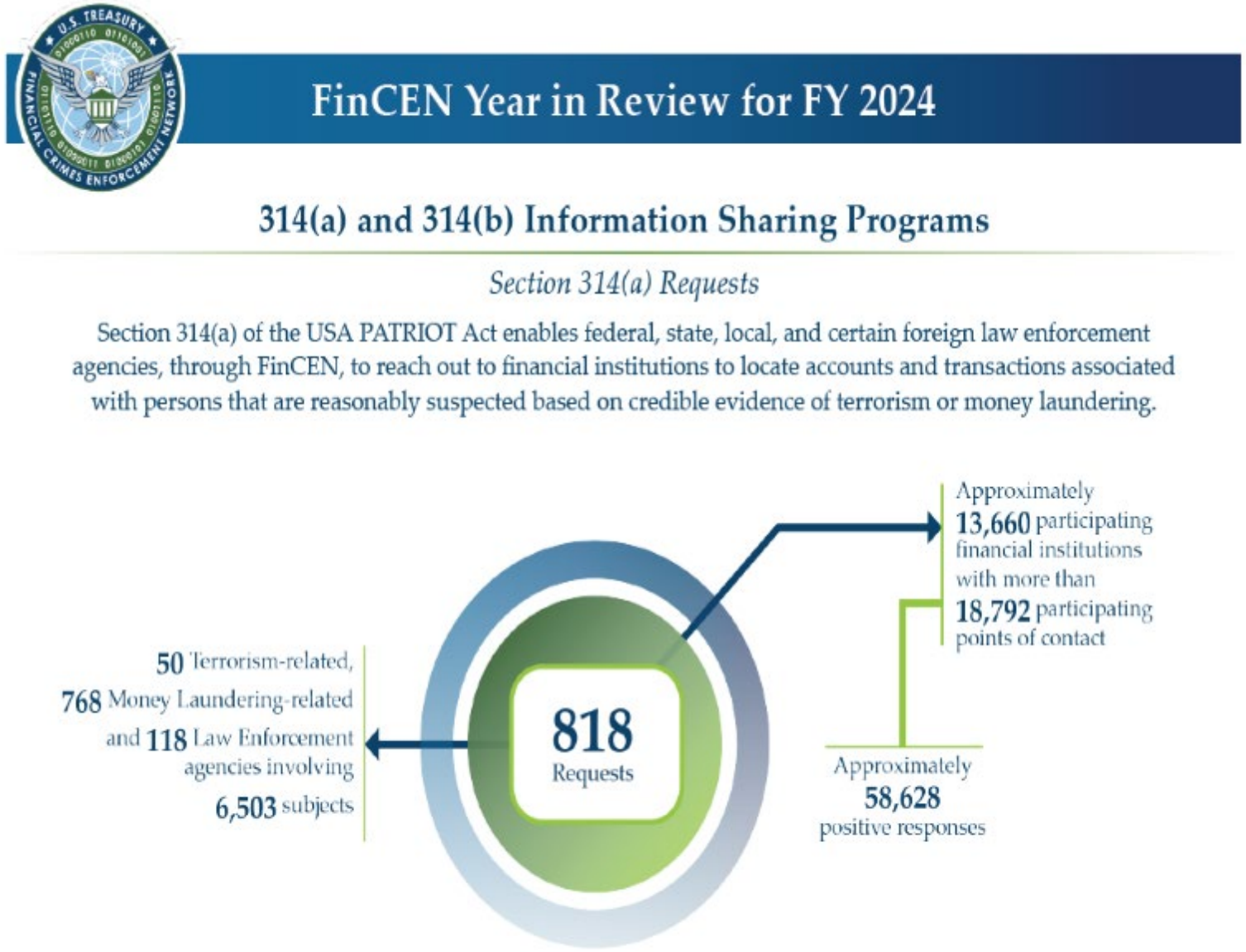
FY24 SAR Activity Type[4]

SARs: The top 10 filers of SARs filed approximately **45%** of all FY24 SARs.

2 M = Million
3 The "other" category includes filings by depository institution holding companies; dealers in precious metals, precious stones, or jewels; operators of credit card systems; and housing government sponsored enterprises.
4 An individual SAR may have more than one SAR activity type, and therefore the sum total of the corresponding graph exceeds the total number of SAR filings.

Compliance Conversations
Bank Secrecy Act & Fraud

2024 FinCEN Year-In-Review (cont.)



Compliance Conversations
Bank Secrecy Act & Fraud

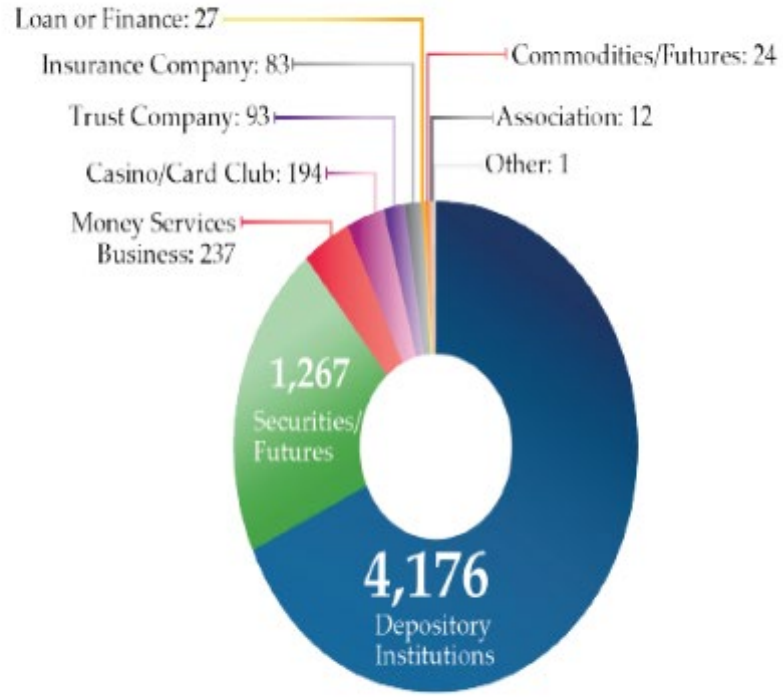
2024 FinCEN Year-In-Review (cont.)

Section 314(b)

Section 314(b) of the USA PATRIOT Act permits registered financial institutions to share information with one another in order to identify money laundering or terrorist activity, and to report any identified suspicious activity to FinCEN.

Section 314(b) in FY24	
6,100+	314(b) registered financial institutions
1,693	Financial institutions referenced 314(b) in SAR narratives
48,223	SARs that referenced 314(b)
62	Terrorism-related SARs referenced 314(b)

The number of 314(b) registered financial institutions



Compliance Conversations
Bank Secrecy Act & Fraud

Fedwire Conversion – ISO 20022 Format ?

ACH Operations Bulletin # 1-2025

Nacha

ACH Operations Bulletin #1-2025

Same-Day Processing of ACH Returns by RDFIs

June 3, 2025

Summary

A Nacha Request for Information in 2024 asked, "As an RDFI, do you currently return any entries using the same-day windows?" Only 59% of respondents said they use Same Day ACH processing windows to send any returns. Of those that do, 45% use same-day processing for less than half of their returns. The responses suggest that many RDFIs are foregoing the benefits of sending returns in a same-day window. *Nacha recommends faster returns as a best practice that benefits RDFIs, including the use of same-day processing windows for the return of forward entries that were not Same Day ACH Entries.*

forvis mazars

ACH Operations Bulletin # 1-2025 (cont.)

Nacha Encourages the Use of Same-Day Processing Windows for Returns

Nacha strongly encourages faster returns using same-day processing windows for the reasons stated in this bulletin. Nacha also encourages any RDFI whose vendor or processor does not support the use of same-day processing windows for returns to ask its processor to enable the capability. RDFIs can experience a liquidity benefit and a reduction in operational risk from the faster return of ACH debits, while ODFIs and their Originators can benefit from receiving any ACH return as soon as possible in order to take appropriate actions. Faster returns, therefore, bestow a network benefit.

Compliance Conversations
AML/CFT (BSA) & Fraud

Reputational Risk “Removal”

Press Release

June 23, 2025

Federal Reserve Board announces that reputational risk will no longer be a component of examination programs in its supervision of banks

For release at 2:00 p.m. EDT

Share

The Federal Reserve Board on Monday announced that reputational risk will no longer be a component of examination programs in its supervision of banks.

The Board has started the process of reviewing and removing references to reputation and reputational risk from its supervisory materials, including examination manuals, and, where appropriate, replacing those references with more specific discussions of financial risk. The Board will train examiners to help ensure this change is implemented consistently across Board-supervised banks and will work with the other federal bank regulatory agencies to promote consistent practices, as necessary.

This change does not alter the Board's expectation that banks maintain strong risk management to ensure safety and soundness and compliance with law and regulation nor is it intended to impact whether and how Board-supervised banks use the concept of reputational risk in their own risk management practices.

For media inquiries, please email media@frb.gov or call 202-452-2955.

Compliance Conversations
AML/CFT (BSA) & Fraud

Reputational Risk “Removal” (cont.)

BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM
WASHINGTON, D.C. 20551

DIVISION OF SUPERVISION
AND REGULATION

SR 95-51 (SUP)
November 14, 1995
Revised June 23, 2025

Revision history:

On June 23, 2025: This letter’s attachment, Federal Reserve Guidelines for Rating Risk Management at State Member Banks and Bank Holding Companies, was revised to remove references to reputational risk.

Clarification on the Responsibilities of the Board of Directors February 26, 2021: As described in SR letter 21-4/ CA letter 21-2, “Inactive or Revised SR Letters Related to Federal Reserve Expectations for Boards of Directors,” this SR letter was revised as of February 26, 2021 to better reflect the Federal Reserve’s guidance for boards of directors in SR letter 21-3 / CA letter 21-1 “Supervisory Guidance on Board of Directors’ Effectiveness,” and SR letter 16-11, “Supervisory Guidance for Assessing Risk Management at Supervised Institutions with Total Consolidated Assets Less than $100 Billion.” No other material changes were made to this letter.

On February 17, 2021: This guidance remains applicable to state member banks and bank holding companies with $100 billion or more in total assets until superseding guidance is issued for these institutions. See SR letter 16-11 for supervisory guidance on assessing risk management practices at state member banks, bank holding companies, and savings and loan holding companies (including insurance and commercial savings and loan holding companies) with less than $100 billion in total consolidated assets, and foreign banking organizations with consolidated U.S. assets of less than $100 billion. These applicability modifications align with the Board’s tailoring rules. See 84 Fed. Reg. 59032 (November 1, 2019) for more information.

Thank you for participating in our discussion today!

Questions?

Compliance Conversations Can Continue
Upcoming Events

September 8–12, 2025 / 2025 Regulatory Compliance Conference

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 & include compliance seminars, webinars, & 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, & 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 & engaging webinars in a format that is right for you & your employees, including Live & 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 & current issues, & provides helpful compliance & management tips.

Compliance Schools & Conferences

ProBank Education Services personnel routinely serve as instructors at banking schools & 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, & independent banker associations, credit union leagues & other industry groups on specific areas of interest, such as compliance, deposits, lending, AML/BSA, fair lending, CRA, compliance risk management & 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, & conventions across the United States. Our well-received presentations rely on the depth of experience of our team & are designed to help sharpen attendees’ regulatory compliance acumen & 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 & 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.

bankED Online Compliance Training

Developed by former federal examiners, compliance trainers, attorneys, & bankers, bankED is an easy-to-use, broad online platform offering courses reflective of today’s financial industry compliance issues & gives the user the ability to work through annual regulatory & policy-driven compliance training requirements at their own pace.

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

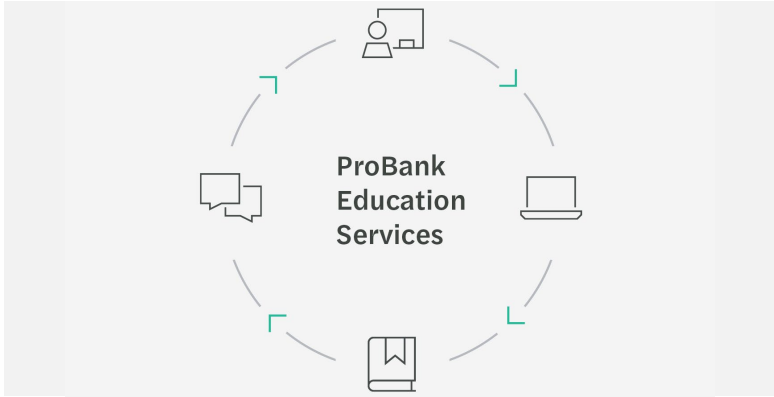
ProBank Advisor®
Take Control of Your Compliance

Compliance Help, Anytime

- Ask Compliance Questions
- Get Ads, Policies, & Disclosures reviewed
- Empower your team to seek answers

Regulations, Simplified

- Access a library of helpful compliance resources like policy guidance, manuals, calculators, & more.
- Stay up-to-date with our regulatory tracking tool!



Transformative Training

- Receive exclusive discounts for your entire institution on ProBank Education Services:
  - Seminars
  - Webinars
  - Conference Events

Learn More & Request A Demo - www.forvismazars.us/probank-advisor

Contact

Forvis Mazars

ProBank Education Services | probank.com | 800.523.4778 |
registrareducationservices@gmail.com