Thomson Reuters Institute

Suspicious Activity Reports Surge: 2023 Filings Expected to Set Another Record

A deeper dive into the data

THOMSON REUTERS®

Contents

Introduction

Financial institutions in the United States have reported soaring volumes of suspicious financial activity to U.S. anti-money laundering (AML) authorities over the past three years.

Disruptions from the global pandemic created unique opportunities for financial crime, particularly fraud schemes involving checks, government benefit payments, and investment accounts. Vulnerable populations have grown in both size and susceptibility, especially among migrants and the elderly, forming a target-rich environment for threat actors.

In 2022, Financial institutions submitted more than 3.6 million Suspicious Activity Reports (SARs) to the U.S. Treasury's Financial Crimes Enforcement Network (FinCEN). SAR filings in March 2023 set a monthly record, with more than 351,000 reports.

Based on data from the first quarter of 2023, this year is likely to set additional records.

Since suspicious activity reporting became fully electronic in 2012, total SAR volumes had increased modestly but steadily until approximately 2019, before spiking dramatically in 2020, 2021, and 2022.

Potential non-criminal drivers

Accelerated SAR filings may not necessarily correlate to symmetrical increases in actual illicit activity. Rather, as the name implies, suspicious activity reports indicate that a financial firm detected and alerted authorities to customer activities known to suggest links to crime. A rapid SAR-filing tempo may be driven by a variety of potential factors.

Several causes likely explain the surge in SAR filings, including heightened regulatory pressure, enhanced threat awareness or detections by firms, and pandemic-related changes such as proliferation of government programs and the rapid, widespread adoption of mobile banking.

'Defensive' SAR filing

Additionally, the spike in reporting could be attributed to defensive filing, a widely recognized practice in which firms apply overly broad detection criteria to minimize their own risk. While aiming to preempt regulatory scrutiny, however, defensive filing produces a higher proportion of SAR filings that unhelpfully point to legitimate activity.

Firms see a clear cost-benefit equation here: Submitting a thinly substantiated SAR carries no regulatory risk – whereas failing to report suspicious activity can attract significant enforcement action and painful penalties.

Key trends

While the sharp rise in SAR filings spanned virtually all categories of illegal activity, this special report highlights key trends, which are supported with additional data.

Growth in suspected fraud linked to government programs likely stemmed from the extensive, documented abuse of pandemic relief programs. Increases in suspected human exploitation appear to reflect heightened awareness by financial institutions, owing to recent alerts from the U.S. Treasury Department and outreach from non-governmental organizations. Additionally, elder financial abuse figured prominently in SARs data, also likely reflecting pandemic-era societal shifts that exposed seniors to new threats.

Correlation to crime

Considerable evidence, backed by expert consensus, indicates that elevated suspicious activity reporting does reflect a genuine increase in certain types of criminal activity. Technological developments and documented increases in certain crime categories, including identity theft and online fraud, are also likely contributors.

SARs related to check fraud have soared over the past three years, FinCEN data shows. Contemporaneous statistics from the Federal Bureau of Investigation (FBI) demonstrate a similar increase in reported fraud cases, particularly in the online domain, which suggests that fraud is rising at an alarming rate.

The following report provides a user-friendly analysis of SAR-filing trends in critically important areas, such as check fraud, human exploitation, and elder abuse. Data is presented showing important annual and monthly trends.

SAR program background

Between 2000 and 2013, FinCEN published semi-annual SARs activity reviews, each containing a detailed analysis of suspicious activity patterns and other financial intelligence insights, including from investigations by federal, state, and local law enforcement agencies. Those reviews ended in 2013. Since 2017, FinCEN has maintained a comprehensive SAR database on its public website[1] , which is updated monthly and includes tools for data interrogation.

[1] FinCEN's SARs Database is available at https://www.fincen.gov/reports/sar-stats.

SAR filing requirements became even more granular when Congress passed the Anti-Money Laundering Act of 2020, requiring firms to report emergent threat typologies, such as money laundering and terrorism financing patterns and trends.

In January 2021, FinCEN began publishing Semi-Annual Trend Analyses, five of which have been issued to date[2]. Each analysis covers a single issue in detail, unlike the 2000-2013 SAR Activity Reviews, which covered multiple issues in less detail. The new trend reports examine unique threats such as ransomware, wildlife trafficking, Russian oligarchs, and business e-mail compromise.

Methodology

This report relies on data from January 2014 through March 2023, obtained from FinCEN's online SAR stats database. All suspicious activity categories were included in our analysis, as were all products, relationships, and specific regulators. To assess the broadest possible dataset, no categories were omitted.

Monthly and annual SAR data was filtered by industry, suspicious activity designation, and filing volume for specific periods.

To simplify data presentation and enhance relevancy, this report aggregates depository institutions, money service businesses, and loan/finance companies into a single "financial institutions" group. Firms in the securities and futures sector, however, were segregated into a separate group, because their regulatory regimes are sufficiently unique to justify their own category.

Additionally, all four gambling-related categories were combined into a generic "casino industry" group. SARs originating from FinCEN's "other" industry category were included in the aggregate data but were not subject to additional analysis.

With regards to the total number of SARs filed, it should be noted that an individual SAR may describe multiple, separate suspicious activities. This report examines those underlying designations to maximize granularity and context.Additionally, this document includes information on threat indicators (or "red flags") derived from official alerts and warnings. Red flags help firms better identify and report suspicious transactions.

The data and findings presented throughout this report can be used for budgeting and planning purposes. For example, monthly data reveals seasonal filing trends. Such information is a valuable resource for corporate compliance, risk, and legal departments. It may also be useful for AML, sanctions, and financial crime units within financial firms, particularly for comparison purposes and presentations to senior management or boards of directors.

[2] FinCEN's Financial Trend Analysis is available at https://www.fincen.gov/resources/financial-trend-analyses.

Background: SARs and FinCEN

SARs filed with FinCEN are important tools to help monitor financial activity that is unusual, may reflect a precursor or derivative of illegal activity, or might threaten public safety.

FinCEN collects and analyzes information about financial transactions to combat domestic and international money laundering, terrorism financing, and other financial crimes. It is the single filing point for SARs and is responsible for distributing that information within the government. FinCEN is also responsible for analyzing this information and producing intelligence products useful to investigators, regulators, and the banking industry.

> ***Failure to detect and report suspicious financial activity can result in significant enforcement action and penalties***

The suspicious activity reporting system was established to help authorities and financial institutions fight financial crime by producing a continuous flow of data about potentially serious activity between depository institutions and federal financial supervisory agencies, such as the Federal Reserve Board, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, National Credit Union Administration, FinCEN, and law enforcement agencies throughout the United States.

Financial institutions are obligated to file a SAR when they detect a suspicious transaction or activity by an identifiable, individual involving at least $5,000, and lacking an apparent lawful purpose, or when there is reason to suspect the funds were derived from illegal activities.

SARs are a tool provided under the Bank Secrecy Act (BSA) of 1970. Originally called a "criminal referral form," SARs became the standard vehicle for reporting suspicious activity in 1996. The USA PATRIOT Act of 2001 expanded SAR-filing requirements to help combat domestic and global terrorism.

Failure to detect and report suspicious financial activity can result in significant enforcement action and penalties.

The flow of such information can have life-and-death implications. SARs enable law enforcement agencies to uncover and prosecute significant money laundering, fraud, terrorism, and other illegal operations.

When are SARs required?

Most commonly, FinCEN requires firms to file a SAR within 30 days of detecting customer transactions featuring details that indicate potential money laundering, terrorism financing, or violations of the BSA. If more evidence is needed – such as the identities of transacting parties – an extension not exceeding 60 days is available. Firms must retain SARs for five years after the date of filing.

What institutions must file SARs?

Many types of financial firms are subject to SAR-filing requirements, including banks and credit unions, stock and mutual fund brokers, and various money service businesses, such as check-cashing companies and money-order providers. However, casinos, dealers of precious metals and gems, insurance companies, and mortgage businesses are also subject to the BSA, and thus are required to file SARs.

Confidentiality is key

The effectiveness of reporting suspicious activity relies in part on confidentiality. At no time may a person under investigation be notified about a SAR filing. Additionally, it is a federal criminal offense to disclose SAR contents to outside parties, such as news organizations.

When a bank or financial institution reports suspicious activity, they are required to ensure the information provided is reviewed at multiple stages by internal investigators, company management, and legal counsel before finalizing the SAR. Special privileges protect those who submit SARs, whether on a company's behalf or as a private individual. The submitting party is not required to disclose their identity, and they are immune to legal discovery processes.

All reporting entities receive immunity for statements made in the SAR.

How are SARs Filed?

Figure 1: SAR Filings Must include Five Sections of information:

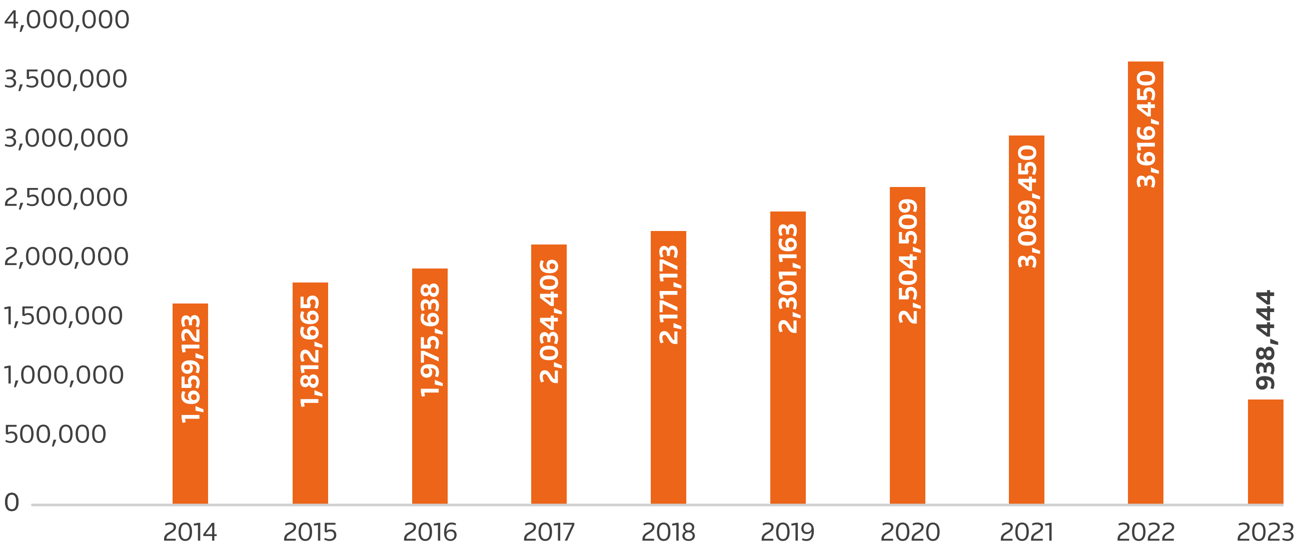
- **Identifying information:** Names, addresses, social security numbers, birth dates, driver license or passport numbers, occupations, and phone numbers of all parties involved.
- **Incident data:** Dates and suspicious activity codes.
- **Institution name:** The firm where the suspicious activity occurred.
- **Institution contact:** Contact details for the reporting firm.
- **Incident narrative:** A written description of the suspicious activity, providing a narrative to the data.

SARs are submitted through FinCEN's electronic filing portal. The digital system facilitates data standardization and increased efficiency which are critical in situations involving public safety concerns.

High-level Findings and Trends

FinCEN received reports from more than 260,000 registered financial institutions and other e-filers in 2022, according to its latest annual review[3]. The review provides valuable insight into the data cited in this report, and it should be noted that apparent differences between this report and FinCEN's annual publication stem from our consolidation of filing entities by industry, as well as our disaggregation of suspicious activity designations in SARs containing multiple entries.

Figure 2: **Total SARs Filed (all industries)**



** 2023 Stats include Jan-March filings*

We have attempted to present the data in a reader-friendly manner. In most cases, the infographics tell much of the story, but in some areas, we have included additional analysis and context.

FinCEN's Year in Review for 2022 revealed some astonishing statistics, which we have highlighted below. Note that FinCEN's statistics differ slightly from ours, due to FinCEN operating on a governmental fiscal-year basis rather than our calendar-year methodology.

[3] Financial Crimes Enforcement Network (FinCEN) Year in Review for FY 2022; April 2023. Available at https://www.fincen.gov/sites/default/files/shared/FinCEN_Infographic_Public_2023_April_21_FINAL.pdf

Figure 3: Notable SAR stats:

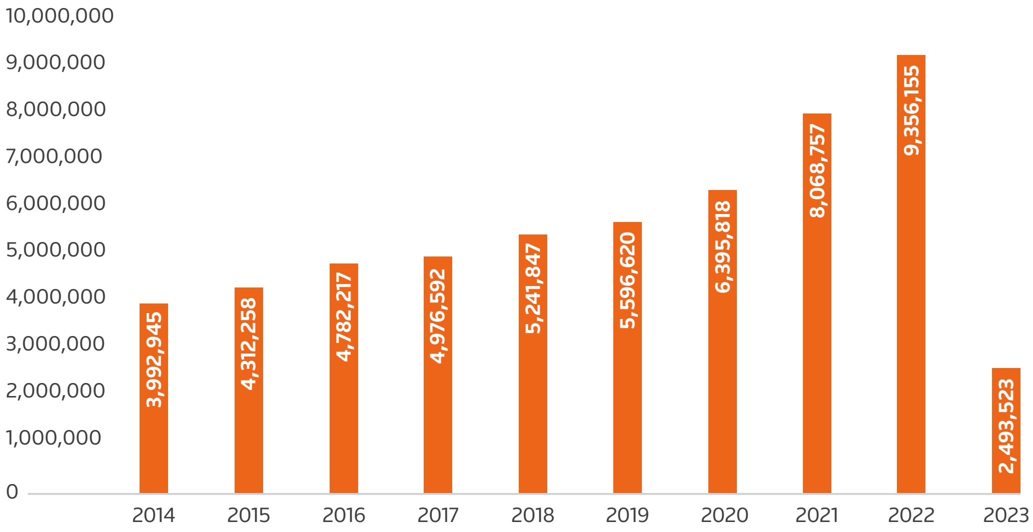
- Approximately **3.6 million SAR forms were submitted in 2022**, or almost 10,000 reports per day
- The **top-10 SAR filers submitted approximately 52% of all SARs in fiscal 2022**
- **Depository institutions and money services businesses (MSBs)** filed the **vast majority (85%)** of all SARs
- **Law Enforcement** and other authorized users **conducted more than 2.3 million queries of FinCEN data in 2022**
- More than **14,800 financial institutions shared data** with law enforcement agencies
- **More than 7,600 financial institutions participate in 314(b) information sharing** (bank to bank)

Growing volume of SARs

More than 3.6 million SARs were filed in 2022, an 18% increase over 2021. The 3.1 million SARs filed in 2021 represented a 22.5% increase over 2020.

The graph below, Figure 4, below shows the total annual volume of suspicious activity designations, or "flags," reported across all filings. For those unfamiliar with the SAR form, numerous check-box options are available when describing the suspicious activity being reported. It is widespread practice to select multiple suspicion flags because some activities straddle multiple categories.

Figure 4: **Total Suspicious Activity Designations (all industries)**



** 2023 Stats include Jan-March filings*

Both datasets – i.e., total SARs and total suspicious activity designations – are important. Aggregated annual filing data provides a broad, holistic view and is valuable for forecasting. The designation-specific data provides granular visibility of specific threat vectors, such as fraud or money laundering, targeted by illicit actors.

In general, since data became available in 2014, there has been steady growth in reported suspicious activity. This is partly due to increasing sophistication in corporate anti-money laundering and anti-fraud programs, as well as advances in detection technology, evolving regulatory priorities, and enhanced scrutiny by enforcement bodies.

However, the notable surge in SAR volumes between 2020 and 2023, where the number of suspicion designations grew from 6.3 million to 9.3 million, represents an increase of 46%.

Figure 5: Top 10 Suspicious Activity Flags (Overall)

Suspicious Activity	2019	2020	2021	2022	2023
Transaction with no apparent economic, business, or lawful purpose	313,124	430,669	686,481	780,057	213,281
Check	285,716	284,888	350,372	683,541	185,584
Suspicion concerning the source of funds	391,650	445,874	594,713	608,043	173,618
Transaction(s) below currency reporting threshold	306,324	426,664	552,640	573,057	139,429
Suspicious use of multiple transaction locations	401,922	429,501	480,224	521,028	141,559
Transaction(s) below BSA recordkeeping threshold	479,496	494,076	564,264	493,287	119,608
Other suspicious activities	262,987	277,074	346,811	477,336	110,027
Two or more individuals working together	244,922	287,023	355,253	467,448	130,493
Suspicious electronic transfers	244,814	356,958	467,053	450,754	112,662
Transaction out of pattern for customer(s)	231,967	307,971	402,180	420,854	107,817

** 2023 Stats include Jan-March filings*

Pandemic response-related fraud

Since 2020, all industries have seen significant growth in fraud of all types, from simple check fraud and scam activity to business email compromises and electronic intrusions resulting in financial losses. We investigate the pandemic's role in fraud growth later in this report.

Digital-first banking

With digital-first banking, customer interactions occur primarily through digital channels, such as websites and mobile device applications. Adopting this approach has been a priority for national and regional banks for several years, as it allows them to reach more customers outside traditional community branches by offering around-the-clock access to bank accounts and services. That flexibility became a crucial selling feature when pandemic mitigation measures disrupted daily life in 2020.

Pivoting to the digital-first paradigm required financial firms to balance the competing priorities of maximizing security while minimizing customer friction. Fraudsters took advantage of the built-in incentives driving banks to streamline customer-facing processes, and the result was fraud on a massive scale

Regulatory pressure

FinCEN has issued dozens of advisories, alerts, and notices since July 2020[4], highlighting its focus on emergent AML concerns ranging from cryptocurrency abuse to human trafficking, elder financial exploitation, ransomware, sanctions evasions, mail-theft-related check fraud, and illicit real estate activity.

Regulators have consistently reminded financial institutions of their suspicious-activity reporting obligations, while providing additional direction on how to make SARs more informative and actionable for authorities. FinCEN also compiles and shares threat typologies and red-flag indicators to help financial institutions detect and report suspicious activity. We have reiterated many of these red flags throughout the report.

Defensive filings

While most individual SAR filings never lead to criminal convictions, the cumulative flow of data is of immense value to financial intelligence and law enforcement agencies. Regulators are therefore unlikely to ever discourage firms from reporting grey-area transactions that, while appearing unusual, do not meet the technical criteria for raising suspicion.

Suspected money laundering and general suspicious activity account for most SARs filings, followed closely by fraud. The data also shows many firms consider incomplete customer information as sufficient grounds to report a money laundering concern.

Three of the 10 most reported suspicious activities relate to information gaps about a customer or out-of-pattern transactions that raised red flags. Many SARs are filed when analysts and investigators cannot determine funding sources, cannot find legitimate reasons for unusually large deposits or withdrawals, or cannot identify relationships between parties that could explain out-of-pattern activity.

Figure 6: Designations Commonly Used in Defensive SAR Filings

Suspicious Activity	2019	2020	2021	2022	2023
Transaction with No Apparent Economic, Business, or Lawful Purpose	313,124	430,669	686,481	780,057	213,281
Suspicion Concerning the Source of Funds	391,650	445,874	594,713	608,043	173,618
Transaction Out of Pattern for Customer(s)	231,967	307,971	402,180	420,854	107,817
Total:	936,741	1,184,514	1,683,374	1,808,954	301,675

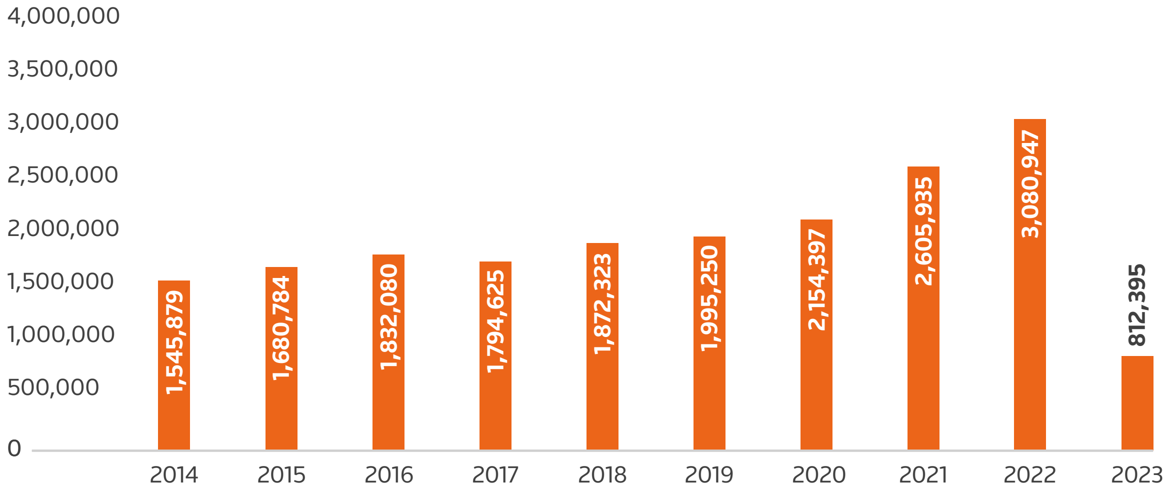
** 2023 Stats include Jan-March filings*

[4] FinCEN Alerts/Advisories/Notices/Bulletins/Fact Sheets, available at https://www.fincen.gov/resources/advisoriesbulletinsfact-sheets.

If AML analysts and investigators as a group had sufficient time, resources, and data, they likely could remediate or avoid a statistically significant portion of the suspicious transactions listed in the chart below. These grey-area reports account for approximately 20% of all SAR filings.

Indeed, with the right combination of public records, transactional insights, and relevant input from customers, financial institutions can significantly reduce the volume of extraneous SAR filings.

Figure 7: **Year-Over-Year SAR Filings by Financial Institutions**



** 2023 Stats include Jan-March filings*

The financial institution group consists of depository institutions, money service businesses (MSBs), and loan or finance companies. This industry category files more than 85% of all SARs. According to FinCEN, the 10 most prolific SAR filers in fiscal 2022 produced 52% of all reports.

Seasonality

Monthly SAR Filings - All Industries

	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
January	130,342	167,693	151,620	166,854	177,537	182,655	189,304	207,953	293,320	295,760
February	122,452	130,716	145,716	144,296	160,132	176,363	190,438	211,130	271,374	291,595
March	126,754	150,211	163,943	186,042	192,786	196,876	199,904	246,411	325,378	351,089
April	145,226	152,984	163,668	156,667	179,171	183,080	202,120	256,745	292,621	
May	140,813	141,306	157,010	177,677	188,204	209,066	166,229	258,017	286,702	
June	143,585	152,593	191,516	177,625	181,926	184,782	183,527	277,334	309,408	
July	142,908	155,932	164,103	157,952	174,018	196,480	223,788	263,780	291,870	
August	134,718	140,574	171,970	187,391	209,468	198,579	220,348	264,122	330,581	
September	144,651	157,882	177,329	175,763	167,193	187,609	238,884	268,224	312,379	
October	150,304	147,031	153,958	168,882	186,616	210,507	225,608	268,224	286,721	
November	138,539	157,894	164,246	168,116	182,276	190,188	223,849	267,052	310,487	
December	138,831	157,849	170,559	167,141	171,846	184,978	240,510	280,458	305,609	
Monthly Average	138,260	151,055	164,637	169,534	180,931	191,764	208,709	255,788	301,371	312,815

** 2023 Stats include Jan-March filings*

Key: ○ <Average 🟠 >Average 🔴 > 1 σ

Monthly SAR loads tend to vary year to year, as economic and societal factors likely play a role in periods featuring high reporting volumes. Pre-pandemic, anti-fraud and AML specialists typically observed a spike in filings during the spring and tax-return season, as well as the end-of-summer and back-to-school period. The monthly SAR chart highlights in red any month where SAR filings exceeded that year's average by at least one standard deviation. Orange highlights indicate filing volumes that were above the annual average but still typically within range. White months had average or below-average volumes.

The monthly SARs chart confirms that for the last nine years, January and February typically showed below-average SAR volumes, while late spring and late summer were often particularly busy. These findings align tightly with observations by AML experts.

Figure 8: Takeaways from Monthly SAR Volumes Include:

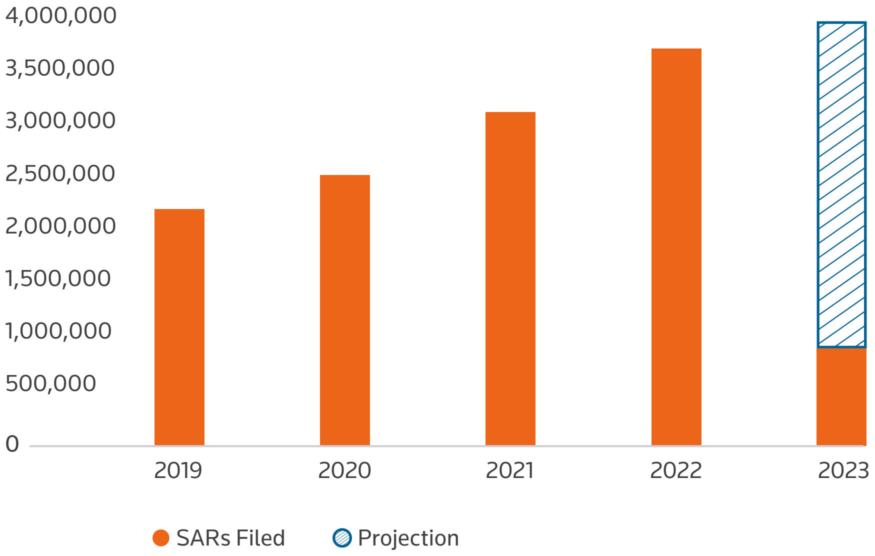
- 2022 saw exceptionally high SAR volumes in March and August, with moderately above-average levels in June, September, November and December
- Every month in 2022 showed more SAR-filing activity than corresponding months in 2021
- 2020-2021 saw heightened caseloads during the back-to-school and winter-holiday shopping seasons.
- 2017-2019 saw below-average caseloads between November and February.
- Consistently lower caseloads between January and April of each year.

> ***January and February typically showed below-average SAR volumes, while late spring and late summer were often particularly busy.***

2023 SAR Prediction: A Record Year in Volume

Based on monthly data, we can project that approximately 3.75 million SARs will be filed in 2023, representing another record year in volume. This projection also considers current regulatory trends, which suggest that SAR-filing requirements will only increase in the near- to medium-term. Additionally, data from the first quarter of 2023 is consistent with the overall growth trend in SARs filings.

Figure 9: **2023 End-Of-Year Projected SAR Filings**



** 2023 Stats include Jan-March filings*
*** Projections subject to change based on overall market*

Financial institutions filed an average of 312,815 SARs per month in the first quarter of 2023, reflecting a 4% increase from the previous year's first-quarter monthly average. That increase was slightly less than in 2019. In 2018 and 2019, however, monthly average SAR growth in the first quarter roughly matched the average rate of increase for the entire year, so we have chosen to incorporate that pattern into our projection for 2023.

Risk leaders should plan for a normal busy season at the beginning and end of summer.

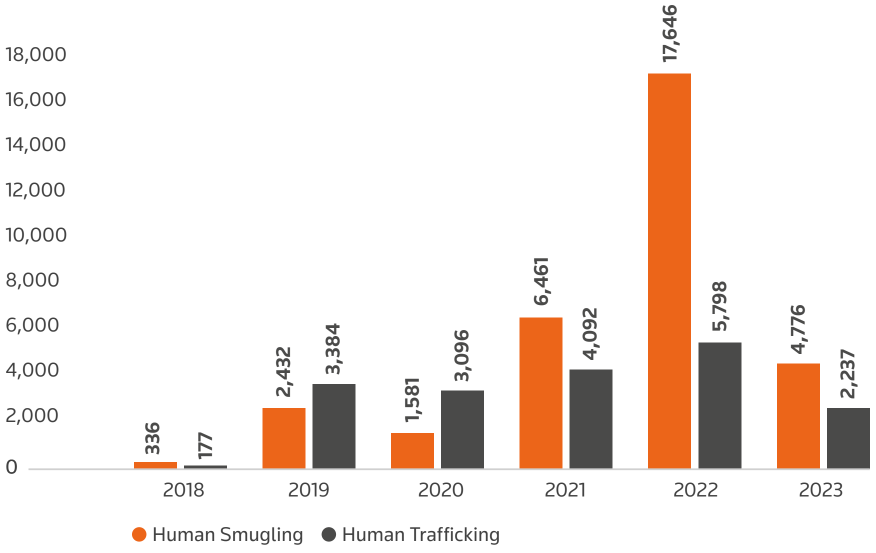
It should be noted that annual SAR volumes are largely driven by a combination of factors, including consumer spending velocity, regulatory guidance, and technological or process innovations.

Human Exploitation

FinCEN data showed a 373% increase in human smuggling related SAR filings from 2020 to 2021, followed by a subsequent 173% increase from 2021 to 2022. In the first quarter of 2023, FinCEN received 4,776 human-smuggling SARs, compared to 6,461 such reports for all of 2021.

SARs related to human trafficking increased by 32% from 2020 to 2021, followed by a further 42% increase from 2021 to 2022. The first quarter of 2023 saw 2,237 human-trafficking SARs filed.

Figure 10: **Human Exploitation SAR Filings**



** 2023 Stats include Jan-March filings*

FinCEN distinguishes between two types of human exploitation – smuggling and trafficking – according to the following criteria:

- **Human smuggling:** Facilitation, transportation, or attempted transportation of persons across national borders, in violation of immigration laws. Smuggling is typically conducted for profit, with the individuals being smuggled often voluntarily paying smugglers to help them enter another country illegally. Subjects of human smuggling can often become victims of human trafficking.
- **Human trafficking:** Modern-day slavery, involving the use of force, fraud, or coercion to exploit individuals for labor or commercial sex purposes. Trafficking in people often involves physical violence, psychological manipulation, or debt bondage. Victims can include men, women, and children. Victims can be trafficked across local, state, and national borders.

FinCEN issued an alert in January 2023[5] addressing human-trafficking trends, typologies, and red flags to help financial institutions better identify and report suspicious transactions related to the multi-billion dollar criminal enterprise.

“Illicit actors, including transnational criminal organizations, engage in human smuggling activity at the U.S. southwest border to reap illicit financial gains, and they do so without regard for the well-being or physical safety of those involved,” said FinCEN Acting Director Himamauli Das. “Financial institutions need to know that their vigilance and prompt Bank Secrecy Act reporting matters – it aids investigations tied to human smuggling and transnational organized crime and can ultimately save lives.”

Human trafficking is one of FinCEN’s eight national priorities related to anti-money laundering and countering the financing of terrorism, as mandated by the Anti-Money Laundering Act of 2020.

Human smugglers operating across the southwest border of the United States have exploited a period of surging migration to generate an estimated $2 billion to $6 billion in yearly organized crime revenue, according to the U.S. Department of Homeland Security. These networks are often associated with transnational criminal organizations, including drug cartels, which control the territories through which smuggling operations take place.

> ***“Recent events involving the death of migrants attempting to cross into the United States illustrate the dangers associated with human smuggling and how smuggling networks exploit human beings for profit,” FinCEN stated.***

The increase in SAR filings has been largely driven by renewed FinCEN guidance on identifying and reporting human trafficking activity in October 2020[6]. In response, organisations started awareness and education efforts, as well as making more filings. Government programs and organizations such as The Knoble[7] have also driven reporting and law enforcement action.

[5] FinCEN Alert on Human Smuggling along the Southwest Border of the United States; (FIN-2023-Alert001) January 13, 2023; available at https://www.fincen.gov/sites/default/files/shared/FinCEN%20Alert%20Human%20Smuggling%20FINAL_508.pdf.

[6] https://www.fincen.gov/sites/default/files/advisory/2020-10-15/Advisory%20Human%20Trafficking%20508%20FINAL_0.pdf

[7] See The Knoble, at https://www.theknoble.com/.

Laundering the proceeds of human exploitation

Human smuggling is often tied to larger criminal groups whose money laundering methods overlap significantly with those of drug cartels and similar organizations.

Smuggling fees are often paid by migrants' U.S.-based family members using transfers disguised as common remittances. Funds are sent to "funnel accounts" at financial institutions with branches along both sides of the southwest border where they are subsequently withdrawn as cash to pay smugglers. Migrants primarily pay smugglers in cash which requires the criminals to move cash in bulk and use it to purchase high-value assets such as real estate and businesses.

Human smugglers also use mobile payment applications and other peer-to-peer networks to transfer funds, albeit less frequently.

Bank Secrecy Act obligations

FinCEN's human exploitation alert advised firms that SARs related to human smuggling should be included in the narrative the key term, "FIN-2023- HUMANSMUGGLING" in SAR field 2 (Filing Institution Note to FinCEN), as well as in the narrative, and be selecting SAR field 38(g) (human smuggling).

FinCEN noted that potential victims of human trafficking should not be reported as the subject of a SAR. "Rather, all available information on the victim should be included in the narrative portion of the SAR." FinCEN further requests that financial institutions reference the advisory by including the key term: "HUMAN TRAFFICKING FIN-2020-A008" in SAR field 2 (Filing Institution Note to FinCEN) to indicate a connection between the suspicious activity being reported and the activities highlighted in the advisory. Additional information to report includes behavioral indicators, email addresses, phone numbers, and IP addresses, when possible, to aid law enforcement investigations.

> ***Smuggling fees are often paid by migrants' U.S.-based family members using transfers disguised as common remittances.***

Figure 11: Important FinCEN Trafficking and Smuggling Red Flags

Indicators of human trafficking

- Customers frequently appear to move through, and transact from, different geographic locations in the United States. These transactions can be combined with travel in foreign countries known to be significant conduits for human trafficking.
- Transactions are inconsistent with a customer's expected activity or line of business and reflect an apparent effort to cover trafficking victims' living costs including housing, transportation, medical expenses, pharmacies, clothing, grocery stores, and restaurants.
- Transactional activity that occurs largely outside of normal business hours (e.g., a business that operates during the day but conducts many transactions at night), almost always in cash, with deposits that are larger than expected for the business.
- An individual frequently purchases and uses prepaid access cards.
- A customer's account shares common identifiers such as a telephone number, email, social media handle, or address associated with escort agencies and commercial sex advertisements.
- Frequent transactions with online classified sites based in foreign jurisdictions.
- A customer frequently sends or receives funds via cryptocurrency to or from dark net markets or services with known links to illicit activity. This may include services that host advertising content for illicit services, sell illicit content, or financial institutions that allow prepaid cards to pay for cryptocurrencies without appropriate risk mitigation controls.
- Frequent transactions using third-party payment processors that conceal transaction originators or beneficiaries.
- A customer avoids transactions that require identification documents or that trigger reporting requirements.

Indicators of human smuggling

- Transactions involving multiple wire transfers, cash deposits, or peer-to-peer payments from multiple originators in different locations either across the United States, or Mexico and Central America, to one beneficiary located on or near the southwest border, with no apparent business purpose.
- Deposits by multiple individuals from multiple locations into a single account. The depositors are not affiliated with the account holder's work or area of residence, and the transfers lack an apparent economic purpose.
- Unexplained currency deposits into U.S. accounts, followed by rapid wire transfers to countries with high migrant flows, such as Mexico and Central America. The transfers are inconsistent with expected customer activity.
- Frequent conversion of small-denomination bills to larger denominations by customers outside cash-intensive industries.
- Multiple customers sending wire transfers to a single beneficiary, where the senders are not relatives but may be located in the sender's home country. The transfers are inconsistent with the recipient customer's usual account activity and reported occupation.
- A customer depositing significantly larger amounts than expected of peers in similar professions or lines of business.
- A customer making cash deposits that are inconsistent with the customer's line of business.
- Extensive use of cash to conduct transactions and purchase assets such as real estate.

Source: www.fincen.gov/sites/default/files/advisory/2020-10-15/Advisory%20Human%20Trafficking%20508%20FINAL_0.pdf

Online Child Exploitation

FinCEN issued a notice in September 2021 alerting firms to increasing rates of online child sexual exploitation[8]. It gave financial institutions specific SAR-filing instructions and highlighted related financial trends. Unfortunately, the SARs data for children is not separated into its own category.

The FinCEN alert provided direction for financial institutions and their handling of online child sexual exploitation (OCSE). The notice provided SAR filing instructions requesting that financial institutions reference the notice in SAR field 2 (Filing Institution Note to FinCEN) using the keyword "OCSE-FIN-2021-NTC3." Financial institutions were also instructed to select SAR Field 38(z) (Other) as the associated suspicious activity type. If human trafficking or human smuggling are suspected in addition to OCSE activity, financial institutions were instructed to also select the respective categories.

> ***Reports of suspected child exploitation rose 35% in 2021, compared to the previous year, according to the National Center for Missing and Exploited Children.***

International standard-setters have also launched initiatives targeting online child exploitation. The United Nations partnered with the Association of Certified Anti-Money Laundering Specialists (ACAMS) in March 2023 to create a no-cost certification program to help AML professionals and law enforcement authorities better detect financial transactions linked to child sexual abuse. The move followed growing concern about the online sale of visually recorded abuse material.

The ACAMS training program – Preventing Online Child Exploitation with Financial Intelligence – teaches the use of cryptocurrency blockchain analytics and compliance data to identify and track the billions of dollars in illicit proceeds generated by online child sexual abuse materials (CSAM). It is supported by the Finance Against Slavery & Trafficking (FAST) initiative from the U.N. University Centre for Policy Research.

'The extent of organized, for-profit child abuse is only getting worse', FAST Project Director Daniel Thelesklaf said, echoing senior officials at ACAMS who designed the program.

Global events have exacerbated the threat. The COVID-19 pandemic forced at-risk children to isolate at home with their abusers, and Russia's February 2022 invasion of Ukraine displaced millions of people, including thousands of Ukrainian children forcibly relocated to Russian territory.

[8] https://www.fincen.gov/sites/default/files/shared/FinCEN%20OCSE%20Notice%20508C.pdf.

Fraud

Fraud rates in general have exploded over recent years, targeting both public and private sectors. As with other threats, the COVID-19 pandemic accelerated the proliferation of fraudulent activity, as criminals leveraged lockdowns, technological shifts, and demographic changes.

American consumers reported an average of 2.6 million fraud cases annually during the pandemic's three-year emergency phase (2020-2022), according to Federal Trade Commission data. While fraud reporting volumes were relatively stable during that period, total reported annual fraud losses increased dramatically.

Overall, financial institutions and other entities have reported significant year-over-year increases across nine of the 10 most-reported fraud categories.

Figure 12: **FBI Internet Crime Reporting by the Numbers**

$10.3 Billion
Victim losses in 2022

2,175+
Average complaints recieved daily

651,800+
Average complaints recieved per year (last 5 years)

Over 7.3 Million
Complaints reported since inception

Figure 13: Top 10 Federal Trade Commission (FTC) Fraud Report Categories

Rank	Category	# of Reports	% Reporting $ Loss	Total $ Loss	Median $ Loss
1	Imposter Scams	761,600	21%	$2,731.5M	$1,000
3	Online Shopping and Negative Reviews	359,706	43%	$358.7M	$179
3	Prizes, Sweepstakes and Lotteries	148,161	12%	$308.6M	$950
4	Internet Services	113,548	4%	$28.5M	$300
5	Investment Related	107,205	74%	$3,907.6M	$5,000
6	Business and Job Opportunities	94,129	32%	$373.5M	$2,000
7	Telephone and Mobile Services	91,220	9%	$20.9M	$200
8	Health Care	74,031	6%	$16.7M	$260
9	Travel, Vacations and Timeshare Plans	65,135	16%	$105.1M	$1,266
10	Foreign Money Offers and Fake Check Scams	41,159	32%	$123.8M	$2,000

Source: https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudLosses

Filtering FinCEN's suspicious activity data by fraud type (as coded in SAR forms) reveals sharp increases in particular categories between 2019 and 2022, including a 140% increase in reported check fraud, an 84% increase in credit/debit card fraud, and a 142% increase in counterfeit currency.

Check fraud, analyzed in more detail below, was by far the most prevalent fraud type reported in 2022, with over 680,000 SAR filings. It was the second largest of all SAR categories that year. While firms have responded by reinforcing their anti-fraud organizations overall, they have focused particular attention on check fraud. While firms have responded by reinforcing their anti-fraud organizations overall, they have focused particular attention on check fraud.

Figue 14: Identity Theft Types

Rank	Theft Type	# of Reports
1	Credit Card Fraud	440,631
3	Other Identity Theft	326,468
3	Bank Fraud	156,116
4	Loan or Lease Fraud	153,569
5	Employment or Tax-Rlated Fraud	103,409
6	Phone or Utilities Fraud	77,308
7	Government Documents or Benefits Fraud	57,898

Source: https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudLosses

Figue 15: Top 10 SAR Fraud Flags

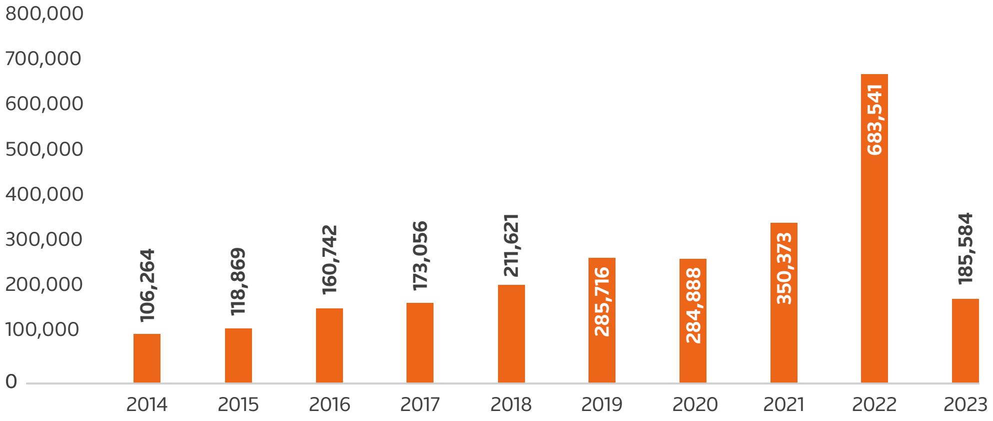
Suspicious Activity	2019	2020	2021	2022	2023
Check	285,716	284,888	350,372	683,541	185,584
Other Fraud (Type)	201,222	262,530	382,037	390,238	110,702
Credit/Debit Card	214,682	189,470	220,586	349,439	100,369
Counterfeit Instrument	129,972	135,432	159,475	327,413	89,128
ACH	121,290	203,635	276,093	291,583	80,942
Wire	123,664	120,025	122,562	136,695	41,153
Consumer Loan (see instructions)	98,209	80,009	76,438	106,966	27,351
Mass-Marketing	13,462	20,996	22,229	33,225	12,707
Business Loan	3,440	16,386	49,008	29,417	9,899
Application Fraud	12,683	16,357	18,875	22,088	5,264

Source: https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudLosses

Check Fraud

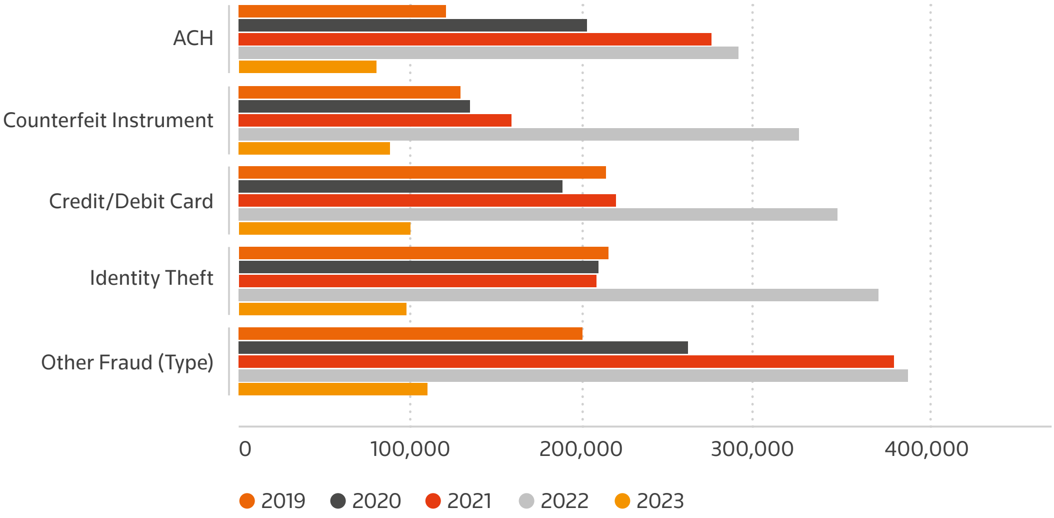
Suspicious activity reporting about check fraud nearly doubled in 2022. Financial institutions filed over 680,000 check fraud SARs last year, a 95% increase over the 350,000 filed in 2021.

Figure 16: **Check Fraud (All Industry)**



** 2023 Stats include Jan-March filings*

Figure 17: **Fraud SAR Filing Trends**



** 2023 Stats include Jan-March filings*

A previous alert from 2021 warned firms that fraud, including check fraud, was "the largest source of illicit proceeds in the United States" and was among the country's top anti-money laundering priorities.

FinCEN warned financial institutions in February 2023 of a nationwide surge in check fraud schemes targeting the U.S. Postal Service[10].

Criminals increasingly targeted U.S. mail carriers during the COVID-19 pandemic, regulators said. This type of crime typically involves stealing personal checks, business checks, tax refund checks, and checks related to government assistance such as Social Security and unemployment benefits.

Figure18: Check Fraud Indicators Include:

- Uncharacteristically large withdrawals from a customer's account via check to a new payee.
- Customer complaints about checks stolen from the mail and deposited into unknown accounts.
- Complaints about mailed checks never reaching intended recipients.
- Checks used to withdraw funds appear to be made of a noticeably different paper stock than that used by the issuing bank or other stock used for known, legitimate transactions.
- Existing customer with no history of check deposits has new, sudden check deposits and withdrawals or transfers.
- Non-characteristic, sudden, abnormal deposit of checks, often electronically, followed by rapid withdrawal or transfer.
- Examination of suspect checks reveals faded handwriting underneath darker handwriting, suggesting that the original handwriting was overwritten.
- Suspect accounts may exhibit indicators of other suspicious activity, such as pandemic-related fraud.
- New customer opens an account that is seemingly used only for the deposit of checks followed by frequent withdrawals and transfers.
- A non-customer who attempts to cash a large check or multiple large checks in person and, when questioned by the financial institution, provides an explanation that is suspicious or potentially indicative of money mule activity.

Source: https://www.fincen.gov/sites/default/files/shared/FinCEN%20Alert%20Mail%20Theft-Related%20Check%20Fraud%20FINAL%20508.pdf

[10] https://www.fincen.gov/sites/default/files/shared/FinCEN%20Alert%20Mail%20Theft-Related%20Check%20Fraud%20FINAL%20508.pdf

Fraudsters and organized criminal groups may alter or wash stolen checks, substituting legitimate payee information with new personal or business accounts controlled by the criminals, FinCEN said. In addition to check washers, the alert outlined the role of so-called money mules, which it described as people who transfer or move illicit funds at the direction of others.

FinCEN requested that financial institutions indicate a connection between the suspicious activity being reported and the activities highlighted in its alert by including the term "FIN-2023-MAILTHEFT" in SAR field 2, as well as in the narrative and by selecting SAR Field 34(d) (check fraud).

Indicators of Check fraud

FinCEN advised financial institutions to consider the surrounding facts and circumstances before escalating suspicion, such as whether transactions are consistent with prevailing business practices and whether a customer raises multiple red flags.

> ***Financial institutions are obligated to file a SAR when they detect a suspicious transaction or activity by a identifiable, individual involving at least $5,000, and lacking an apparent lawful purpose, or when there is reason to suspect the funds were derived from illegal activities.***

Supporting Criminal Data

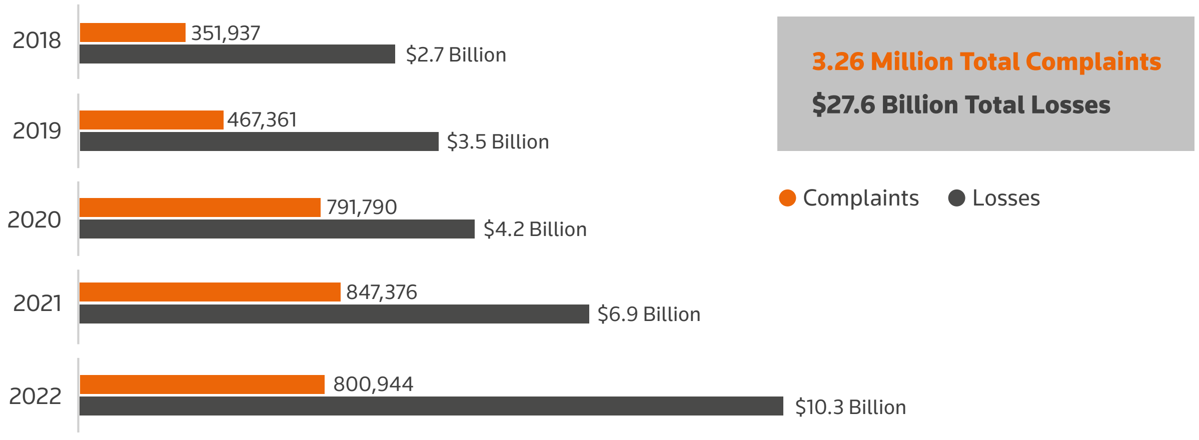
SAR and FBI Data Paint Bleak Picture

Data from the U.S. Federal Bureau of Investigations (FBI) validates the rising fraud trend apparent in FinCEN's SAR database.

FBI Internet Crime Complaint Center (IC3) data for 2022 showed:

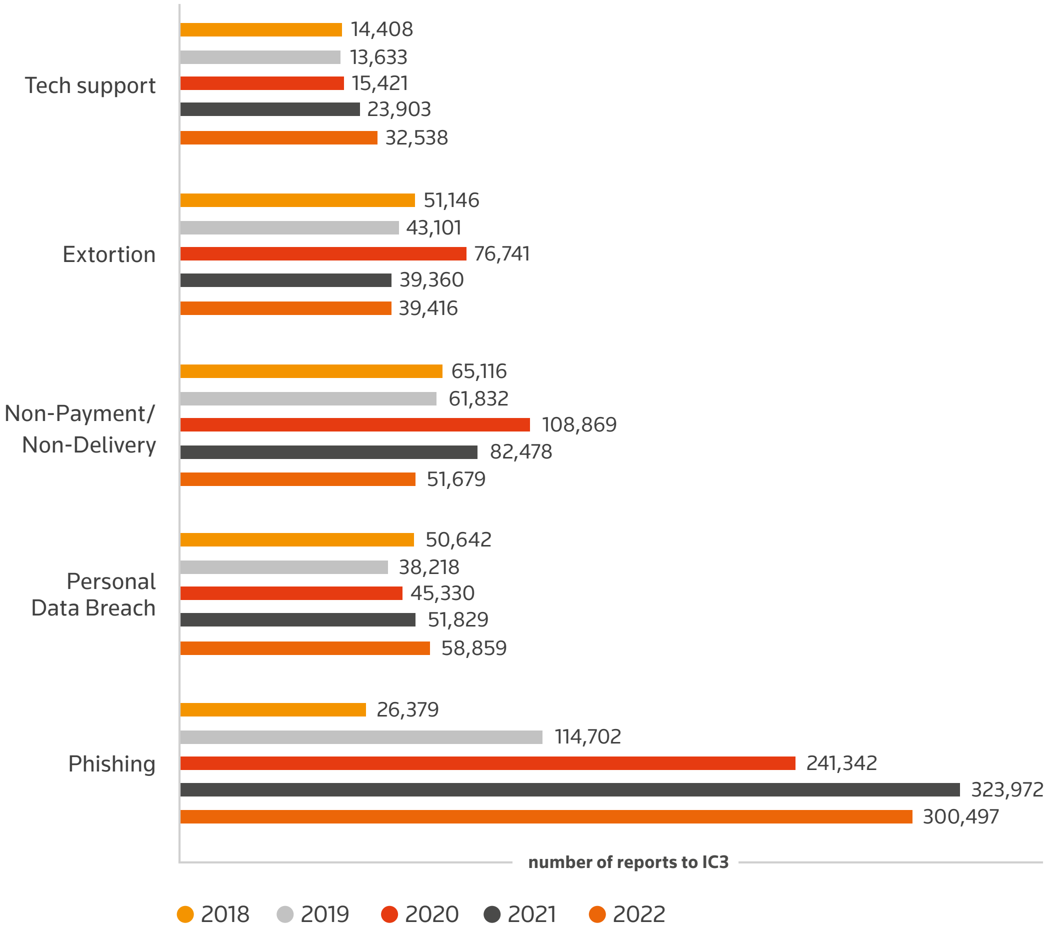
- 127% increase in reported investment fraud, amounting to $3.3 billion in reported losses.
- Call center fraud affected more than 44,000 victims, accounting for over $1 billion in losses.
- 2,385 complaints of ransomware targeting critical infrastructure, with reported losses totaling over $34 million.

Figure 19: **Complaints and Losses over the Last Five Years**



Source: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf (FBI's IC3 Annual Report for 2022)

Figure 20: **FBI IC3's Top Five Internet Crime Types**



Source: IC3 FBI's IC3 Annual Report for 2022

FBI Internet Crime Complaint Center (IC3) Supporting Data

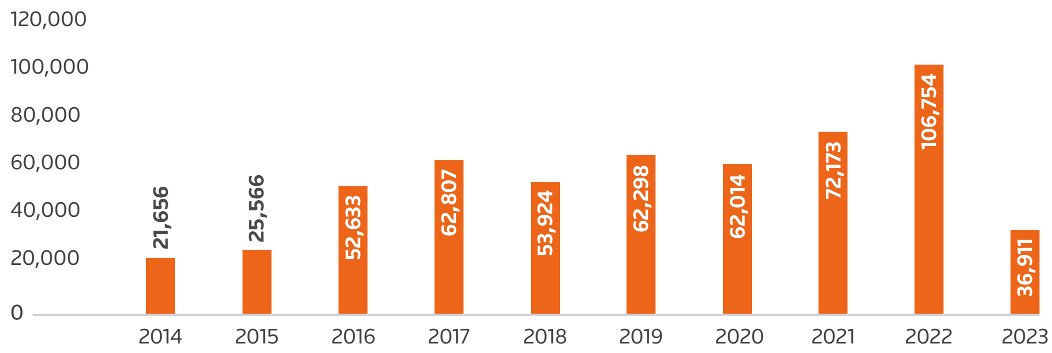
Takeaways:

- Exponential growth in victims and financial losses.
- Exacerbated by the pandemic.
- Domestic and international organized crime as well as state-sponsored criminal enterprises are all active in financial crimes.
- Fraudulent events create devastating losses to victims.
- Major business opportunities for scam perpetrators.
- Significant amounts of elder fraud go un-reported due to embarrassment, financial problems, and familial abuse.

Elder Financial Exploitation

SAR data shows a dramatic increase in suspected elder financial abuse. FinCEN recorded nearly 107,000 SARs related to elder abuse in 2022. That figure's correlation to incidents of crime is supported by the FBI's Internet Crime Complaint Center (IC3), which recorded 88,000 cases of online fraud targeting seniors. Losses by elder victims increased by 84% in 2022, FBI data showed.

Figure 20: **Elder Financial Exploitation SAR Filings**



** 2023 Stats include Jan-March filings*

Figure 21: **IC3 Victims Over 60 by the numbers**

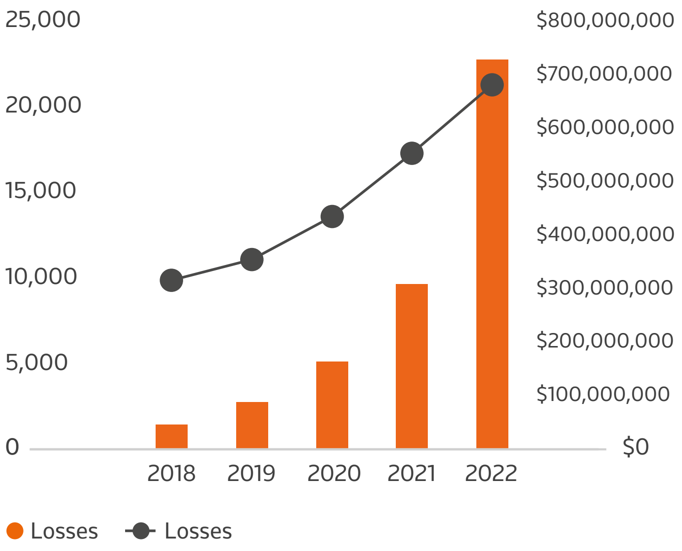
88,262	Total Victims Over 60
$3.1 Billion	Total Losses
84%	Increase in losses from 2021
$35,101	Average Losses Per Victim
5,465	Victims losing more then $100K

Sourced (FBI's IC3 Annual Report for 2022)

Senior vulnerability to online fraud was exacerbated by the COVID-19 pandemic which forced many seniors to transition from in-branch service to mobile banking. Instances of phishing, identity theft, and other cybercrime targeting the elderly population became much more prevalent.

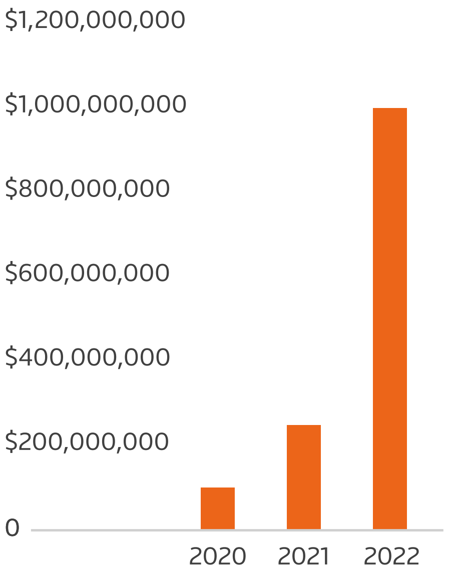
Such scams are often perpetrated through popular online services, such as the practice of "catfishing," in which fraudsters use fictitious social-media profiles to ensnare seniors in false romantic relationships resulting in financial abuse. Another tactic involves SMS-phishing – or smishing – whereby scammers send text messages purporting to be from reputable companies in order to manipulate targets into revealing personal information including passwords or credit card numbers.

Figure 22: Call Center Frauds - Victims Over 60



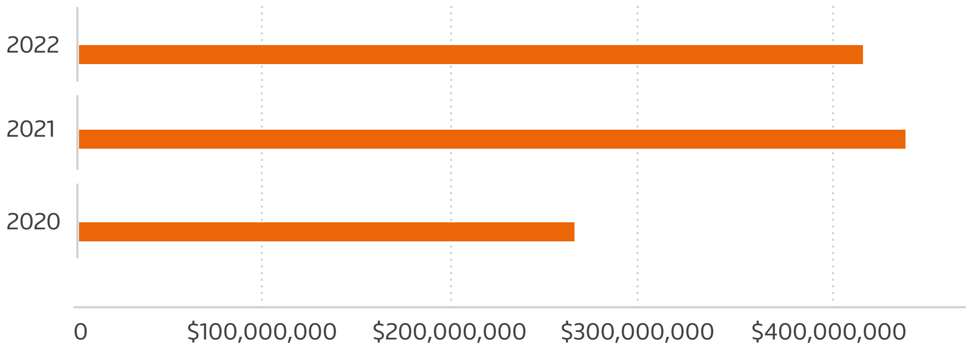
Source: FBI Elder Fraud Report 2022 (https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3ElderFraudReport.pdf)

Figure 23: Investment Scam Losses by Victims Over 60



Source: FBI Elder Fraud Report 2022 (https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3ElderFraudReport.pdf)

Figure 24: **Confidence/Romance Scam Losses by Victims Over 60**



Source: FBI Elder Fraud Report 2022 (https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3ElderFraudReport.pdf)

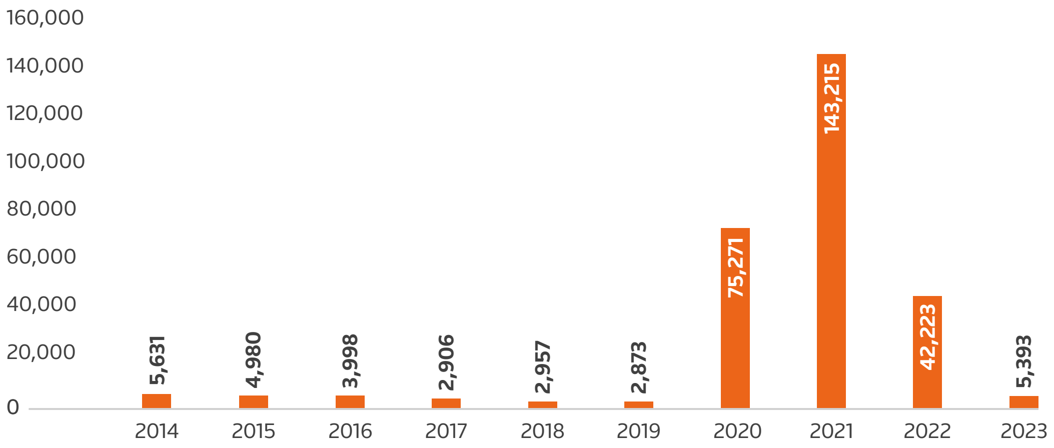
A 2022 FinCEN alert about elder abuse included both behavioral and financial red flags indicating suspicious activity[9].

FinCEN requested that financial institutions filing SARs on such activity mark the check box for Elder Financial Exploitation and include the key term "EFE FIN-2022-A002" in SAR field 2 and to ensure the narrative section describes a connection between the reported suspicious activity and the specific indicators highlighted in the advisory.

[9] https://www.fincen.gov/sites/default/files/advisory/2022-06-15/FinCEN%20Advisory%20Elder%20Financial%20Exploitation%20FINAL%20508.pdf.

Pandemic-related Fraud and Suspicious Receipt of Government Payments

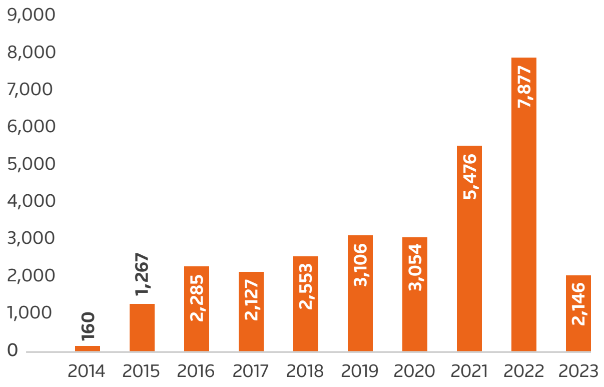
Figure 25: **Suspicious Receipt of Government Payments/Benefits**



** 2023 Stats include Jan-March filings*

The chart above shows a dramatic spike in SAR filings related to public support programs in 2020 and 2021, almost certainly driven by pandemic-related U.S. government spending through the Paycheck Protection Program (PPP), Economic Injury Disaster Loans (EIDL), and other state and federal unemployment benefits.

Figure 26: **Housing Government Sponsored Enterprises**



** 2023 Stats include Jan-March filings*

Unemployment insurance fraud reached $60 billion during the pandemic; the U.S. General Accounting Office estimated in a February 2023 report[14]. Investigations by the Department of Labor's inspector general, opened at a rate of 100 per week, resulted in 1,200 indictments or initial charges from April 2020 through January 2023.

Like other financial institutions and government agencies, federal housing programs have seen a surge in SAR filings.

Government-sponsored enterprises (GSEs), which bring capital to the housing market, include Fannie Mae, Freddie Mac, and the Federal Home Loan Banks.

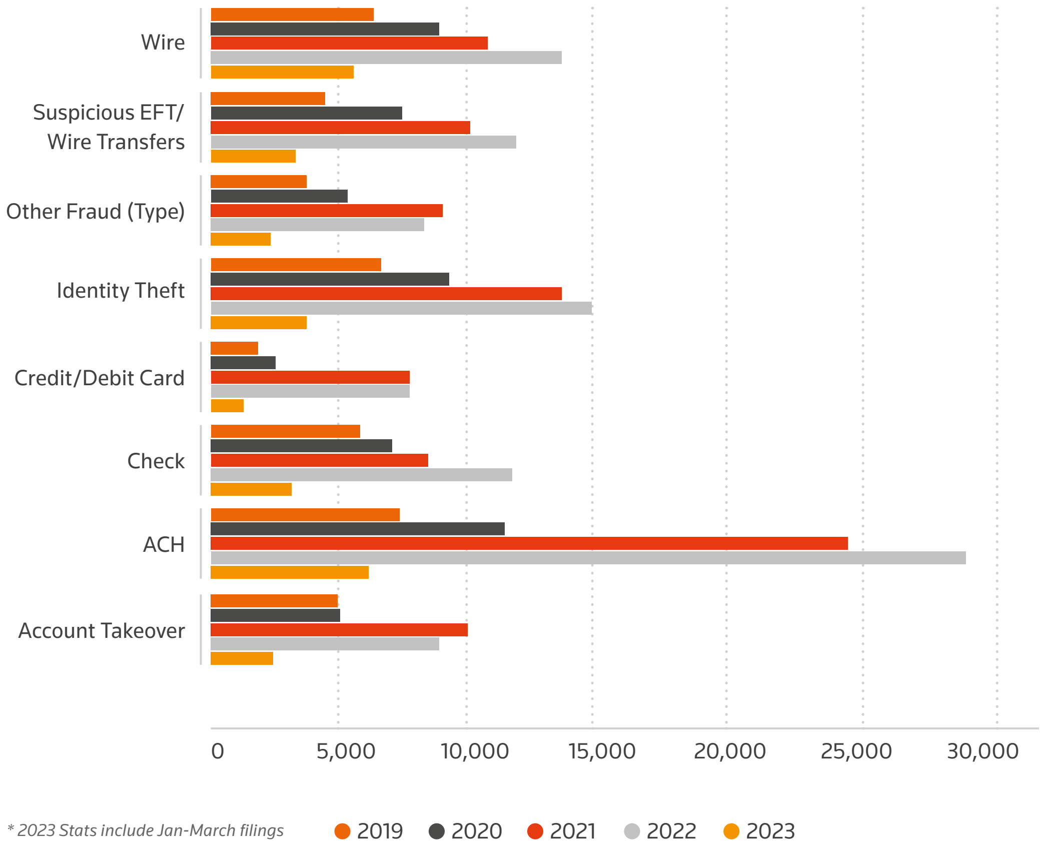
[14] https://www.gao.gov/assets/gao-23-106586.pdf

Specific Industries and Terror Financing

Financial Institutions: Securities/Futures

Financial markets are also experiencing a sharp uptick in suspicious activity filings that often overlap with other crime trends such as elder financial exploitation. Although check, credit card, and wire frauds occur at traditional financial service firms such as banks, more advanced frauds occur in the securities and futures markets.

Figure 27: **Securities/Futures Industry SAR Filings - Steady Fraud Uptick**



Sophisticated criminals have been raiding brokerage accounts by fraudulently transferring assets through the Automated Customer Account Transfer Service (ACATS). ACATS frauds could likely fall under several of the threat designations covered in this report.

The Financial Industry Regulatory Authority (FINRA) issued Regulatory Notice 23-06[10] in March 2023, highlighting effective practices for mitigating the risk of criminal actors abusing ACATS. FINRA's warning followed Regulatory Notice 22-21[11], published in October 2022, which highlighted a rising trend of fraud perpetrated through ACATS. It also outlined relevant regulatory obligations and provided information for reporting fraud.

ACATS enables eligible participants to enter, review, and settle the transfer of customer accounts. It facilitates the transfers of many different asset types, including equities, corporate and municipal bonds, unit investment trusts, mutual funds, options, annuities, and cash.

Criminal actors abuse the system by opening an online brokerage account using the stolen personally identifiable information of a legitimate client from another member firm.

"The bad actor may then engage receiving and/or carrying members to conduct a transfer of the account of the legitimate customer at the carrying member into the new brokerage account at the receiving member," FINRA said.

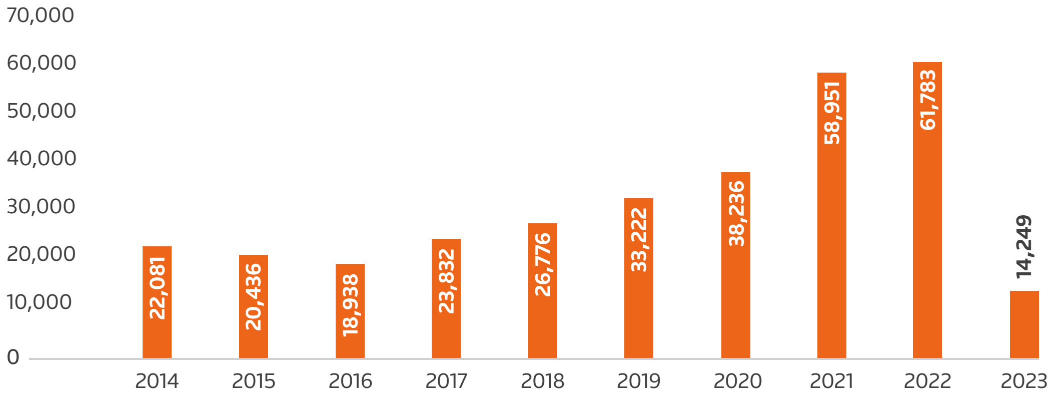
"When that transfer is complete, the bad actor may then proceed with moving the ill-gotten assets out of the newly established brokerage account to another external account or financial institution."

Some of the safeguards firms employ resemble those for preventing identity theft and phishing attacks. Firms should be on the lookout for grammatical and spelling errors, as well as writing that changes in style from previous email communications. Additionally, some of the practices are consistent with precautions outlined in Regulatory Notice 21-18[12] on preventing online account takeovers and Regulatory Notice 20-13[13], which warned firms about fraud risk during the COVID-19 pandemic.

FINRA urged firms to evaluate their supervisory systems related to ACATS transfers and fraud mitigation.

[10] https://www.finra.org/rules-guidance/notices/23-06.
[11] https://www.finra.org/rules-guidance/notices/22-21.
[12] https://www.finra.org/rules-guidance/notices/21-18.
[13] https://www.finra.org/rules-guidance/notices/20-13.

Figure 28: **Securities Industry SAR Filings**



** 2023 Stats include Jan-March filings*

Figure 29: Indicators of ACATS Fraud:

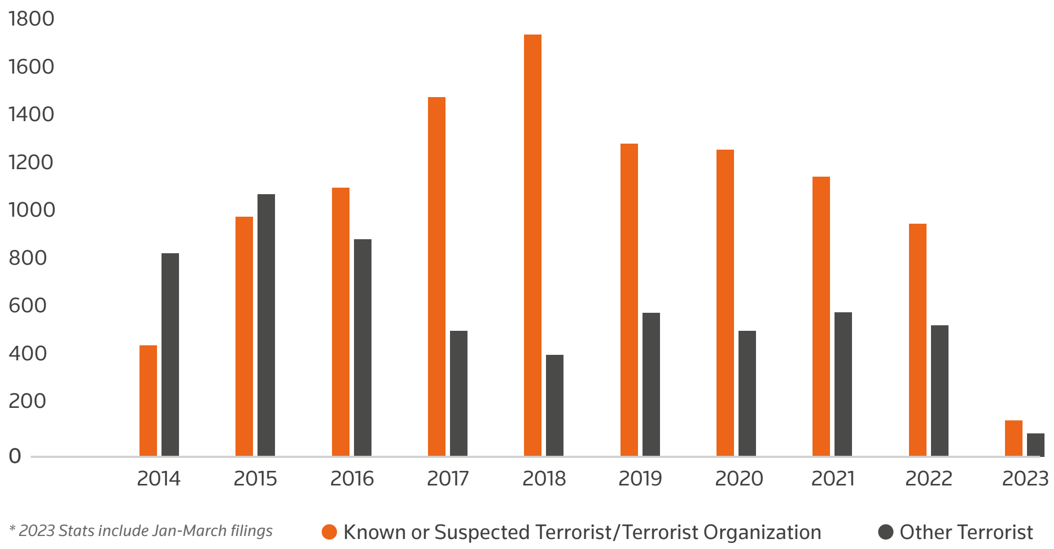
- Repeated transfer rejections due to incomplete or inaccurate information. Errors might relate to account type or other basic information, including a carrying member's rejection of a receiving member's account transfer request for the same customer on multiple occasions.
- Rapid asset transfers following account creation. Soon after assets have been moved into a new brokerage account, a bad actor sends instructions to quickly move those assets to another external account or financial institution.
- Changes in communication patterns. Customers who usually communicate by telephone may suddenly prefer to communicating only by email, and when the firm contacts the customer by usual means, the customer confirms that the email communication did not come from the customer.

Source: https://www.fincen.gov/sites/default/files/advisory/2022-06-15/FinCEN%20Advisory%20Elder%20Financial%20Exploitation%20FINAL%20508.pdf

Terror Financing

Suspicious transaction reporting related to terrorism financing has declined in recent years, a deviation from overall increases in other financial crimes. The aggregate volume of terrorism related SAR filings has, however, always been relatively low in absolute terms, an ironic twist considering the landmark USA PATRIOT Act of 2001 created a host of new AML/CFT obligations following the September 11 terrorist attacks in New York City and Washington, D.C.

Figure 30: **Terrorism Financing Related SARs**



In addition to funding from wealthy sympathizers and rogue nations, terrorist organizations rely on a variety of criminal activities to finance their operations, including fraud and drug trafficking. As a result, financial institutions may identify a suspicious transaction but lack sufficient awareness to ascertain its indirect connection to terrorism, unless the named originator or beneficiary was officially sanctioned as a designated terrorist.

Firms may therefore file a fraud SAR, including the names of involved parties, and leave it to law enforcement authorities with specialized intelligence to determine whether the activity is linked to terrorism.

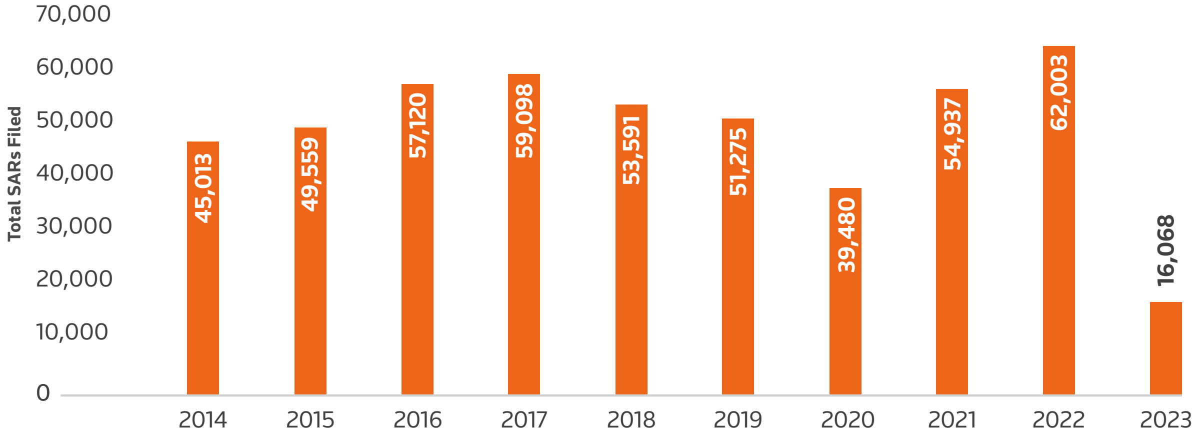
Furthermore, there has been some criticism of FinCEN over its apparent lack of focus on alerts and advisories providing updated guidance and red flags with regards to terror finance. Some experts believe a lack of recent, major terrorist attacks has allowed regulatory focus to shift.

Casino Industry

Casino-relate suspicious activity reporting saw a notable decline in 2020, due to pandemic measures that closed many casinos, followed by a significant drop in attendance after gradual reopening.

The casino sector has, however, faced increasing regulatory pressure over money-laundering concerns.

Figure 31: **Casino Industry SARs**



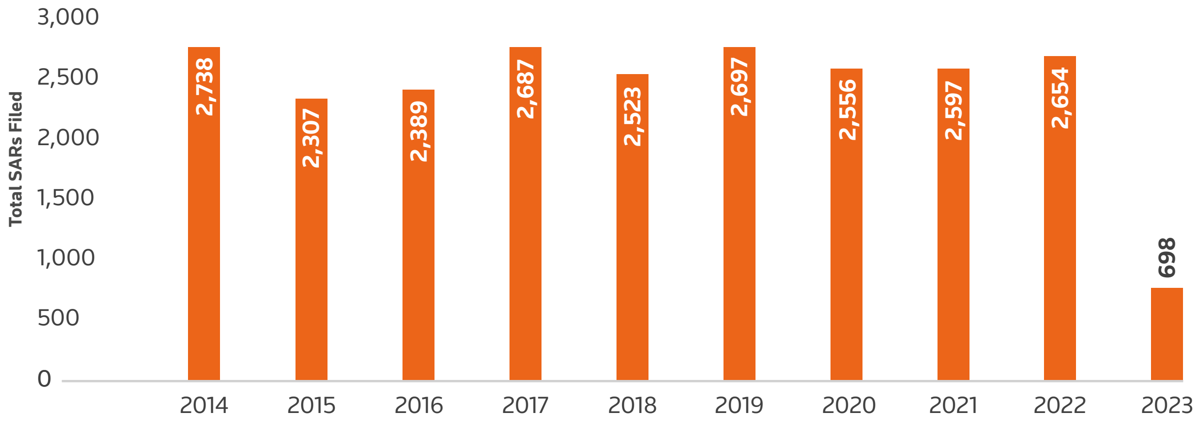
* 2023 Stats include Q1 filings
**Casino Industry consists of: Casino/Card Club – Other, Casino/Card Club, Casino/Card Club - State Licensed Casino and Casino/Card Club - Tribal Authorized Casino

Healthcare and Insurance Industry

The U.S. Department of Justice (DOJ) announced criminal charges in April 2023 against 18 defendants for their alleged role in healthcare fraud schemes that exploited the COVID-19 pandemic, resulting in over $490 million in false billings to federal programs and theft from publicly funded pandemic programs.

Monitoring medical providers and other recipients of government health insurance payments for fraudulent activity has always been difficult because it depends on an institution's ability to segment its clients. That challenge has escalated with the surge in COVID-related programs such as the Health Resources and Services Administration's program to help the uninsured.

Figure 32: **Insurance Industry SARs**

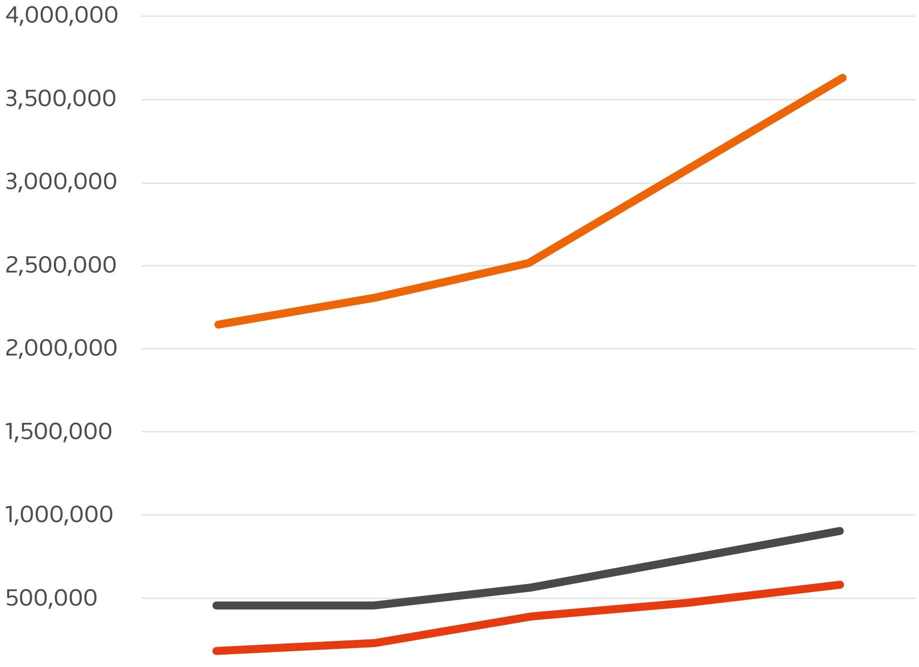


** 2023 Stats include Jan-March filings*

International Comparisons

The quantity of SAR filings – called suspicious transaction reports internationally – varies widely between countries, owing to differences in economic size and intensity. Their purpose, however, remains the same: to detect and prevent illegal activity. These statistics reflect significant annual growth in suspicious transaction filings internationally.

Fig 33: **International SAR Filing Comparison**



Country	2018	2019	2020	2021	2022
USA ▬	2,171,173	2,301,163	2,504,509	3,069,450	3,616,450
United Kingdom ▬	463,938	478,437	573,085	742,317	901,255
Canada ▬	179,172	235,661	386,102	468,079	585,853

Source: United Kingdom Financial Intelligence Unit Annual Report:
https://nationalcrimeagency.gov.uk/who-we-are/publications/632-2022-sars-annual-report-1/file

Source: Canada Data: FINTRAC ANNUAL REPORT - https://fintrac-canafe.canada.ca/publications/ar/2022/1-eng

Closing Thoughts: Increasing Fraudulent Activity, Increasing Surveillance Tools

The data presented in this report highlights significant trends and changes in SAR filings. Disruptions inherent to the COVID-19 pandemic created new opportunities for criminal abuse, reflected in broad reporting surges in nearly all types of financial crime. Additionally, increased regulatory pressure, warnings, and defensive filing practices have provided a steady and growing momentum to filing volumes. Fraud has increased to unprecedented levels as validated by data from the FBI and Federal Trade Commission.

Suspicious Activity Reports are an essential tool in law enforcement's effort to fight crime. They have also become a critical challenge for corporate compliance, anti-fraud, and risk departments across virtually all financial services firms.

Risk, BSA, compliance, and anti-fraud leaders should continuously monitor this data as it provides insight into developments affecting industry peers.

Organizations should contrast the granular, publicly available data with their own internal sources to benchmark themselves against the broader market. Bank leaders can use such comparisons to identify strengths and weaknesses in their compliance programs and find potential blind-spots for illegal activity within their customer base. By taking the most recent SAR statistics into account, financial institutions and other businesses should reasonably be able to identify the most prevalent fraud and money laundering threats.

Law enforcement agencies and professionals have repeatedly voiced concern over increases in defensive filings, while urging firms to include more specific information in SAR filings.

Institutions should also be working to reduce unproductive alerts and working to leverage technology to combat fraud proactively. Additionally, there is a growing need for qualified subject-matter experts to examine trending fraud practices.

About the authors

JACOB DENMAN

With more than a decade of experience in financial crime investigations, financial crime leadership roles, and law enforcement, Jacob has a wealth of knowledge and expertise in risk, financial crime, and fraud. As a Risk, Fraud & Compliance Manager at Thomson Reuters, Jacob is responsible for developing and executing creative strategies to grow the risk and fraud product lines by driving customer engagement and adoption of our products. He collaborates closely with sales, product management, and other key business stakeholders to ensure Thomson Reuters products are aligned with customer needs. Prior to joining Thomson Reuters, Jacob was a lead investigator in financial crimes at Wells Fargo, and TCF Bank. Jacob also has more than seven years of experience in law enforcement.

BRETT WOLF

Brett Wolf is a Senior Anti-Money Laundering Correspondent for Thomson Reuters. For more than two decades, Brett has been on the AML beat, producing daily regulatory intelligence news and analysis to aid AML and sanctions compliance professionals. A proven investigative journalist for Thomson Reuters, Brett also has experience reporting on Justice Department efforts to combat money laundering, terrorist financing, corruption, and offshore tax evasion and non-compliance with the Bank Secrecy Act (BSA).

TODD EHRET

Todd Ehret is a Senior Regulatory Intelligence Expert for Thomson Reuters Regulatory Intelligence. At Thomson Reuters he has authored numerous articles and white-papers, and frequently presents at industry conferences, events, and seminars on a myriad of financial regulatory topics including fintech and crypto-assets. Todd has an enormous breadth of experience gained from more than 25 years on Wall Street at financial services firms dealing with both institutional and retail clients. Before joining Thomson Reuters, he served as a Chief Compliance Officer and Chief Operating Officer at a registered investment adviser/ hedge fund for nearly a decade.

Contributors

Rabihah Butler — Enterprise Content Manager – Thomson Reuters Institute

Alex Robson — Managing Editor - Thomson Reuters Regulatory Intelligence

Daniel Seleanu — Commissioning Editor - Thomson Reuters Regulatory Intelligence

Gregg Wirth — Content Manager - Thomson Reuters Institute

Thomson Reuters

Thomson Reuters is a leading provider of business information services. Our products include highly specialized information-enabled software and tools for legal, tax, accounting and compliance professionals combined with the world's most global news service – Reuters. For more information on Thomson Reuters, visit tr.com and for the latest world news, reuters.com.

Thomson Reuters Regulatory Intelligence

Thomson Reuters® Regulatory Intelligence is a market leading solution that empowers you to make well-informed decisions to confidently manage regulatory risk, while providing the tools to make proactive decisions and action change within your organization. It has been developed with a full understanding of your compliance needs – locally and globally, today and in the future.

Thomson Reuters Institute

The Thomson Reuters Institute brings together people from across the legal, corporate, tax & accounting and government communities to ignite conversation and debate, make sense of the latest events and trends and provide essential guidance on the opportunities and challenges facing their world today. As the dedicated thought leadership arm of Thomson Reuters, our content spans blog commentaries, industry-leading data sets, informed analyses, interviews with industry leaders, videos, podcasts and world-class events that deliver keen insight into a dynamic business landscape.

Visit **thomsonreuters.com/institue** for more details.

THOMSON REUTERS®