FINANCIAL CRIMES ENFORCEMENT NETWORK

Financial Trend Analysis

Identity-Related Suspicious Activity: 2021 Threats and Trends

January 2024

Identity-Related Suspicious Activity: 2021 Threats and Trends

This Financial Trend Analysis (FTA) focuses on pattern and trend information identified in Bank Secrecy Act (BSA) data linked to identity-related suspicious activity reported in 2021. FinCEN is issuing this report pursuant to Section 6206 of the Anti-Money Laundering Act of 2020 that requires periodic publication of BSA-derived threat pattern and trend information.[1] *FinCEN has determined that identity-related suspicious activity is a cybercrime concern, has highlighted the importance of customer identity in achieving its mission, and has included cybercrime and fraud as government-wide priorities in the June 2021 Anti-Money Laundering/ Combatting the Financing of Terrorism (AML/CFT) policy. This FTA intends to use BSA data to quantify and feed back to industry how bad actors exploit identity-related processes during account opening, access, and transactions ("identity processes") to perpetrate crimes. The information is relevant to the public, particularly financial institutions and entities involved in identity processes and mitigating crimes. This report highlights the value of BSA information filed by regulated financial institutions.*

Executive Summary: This FTA provides threat pattern and trend information on identity-related suspicious activity, or suspicious activity tied to the exploitation of one or more steps of identity processes, including those within financial institutions, based on Bank Secrecy Act (BSA) data filed with FinCEN from January to December 2021 (the Review Period).[2] [3] During the Review Period, approximately 1.6 million, or 42% of around 3.8 million total BSA reports, equivalent to $212 billion in suspicious activity, related to identity.

Note Regarding Terminology in this Report: This FTA intends to quantify how bad actors exploit identity processes to perpetrate crimes. These exploitations include "impersonation", "circumvention", and "compromise." These occur, respectively, in three identity processes: validation, verification, and authentication. FinCEN's identity process definitions closely align with the National Institute of Standards and Technology (NIST) definitions, including for "verification" that distinguishes between verification and validation. (See Scope and Methodology box for further information.) FinCEN recognizes that this FTA's use of the term "verification" may differ from how the term is used under its Customer Identification Program (CIP) and Customer Due Diligence (CDD) Rules, among other BSA obligations. T**his FTA does not intend to, nor does it impose, any additional regulatory obligations or supervisory expectations, or alter any existing regulatory obligations or expectations on financial institutions, including those with CIP and CDD obligations.**

Overview of Key Findings: During the Review Period, perpetrators of identity-related suspicious activity (also referred herein to as "attackers") have used at least 14 typologies to exploit the three identity processes (see figure 1). According to FinCEN's analysis:

- *Most attackers have impersonated others to defraud victims:* Sixty-nine percent of identity-related BSA reports (approximately 1.7 million filings) indicate that attackers impersonated others as part of efforts to defraud victims. Eighteen percent of identity-related BSA reports

(approximately 446,000 filings) describe attackers using compromised credentials to gain unauthorized access to legitimate customers' accounts. Thirteen percent of identity-related BSA reports (approximately 323,000 filings) report attackers exploiting insufficient verification processes to advance their schemes (see figure 3).

- *Depository institutions have filed the greatest number of identity-related BSA reports:* 54% of identity-related BSA reports (approximately 1.3 million filings) were filed by depository institutions, reporting $201 billion in suspicious activity. Money services businesses (MSBs) are the next largest category of filer, filing 21% of identity-related BSA reports (see figure 4).[4]
- *Fraud was the most reported typology:* Of 14 commonly reported typologies, the most reported were general fraud (approximately 1.2 million), false records (approximately 423,000), identity theft (approximately 222,000), third-party money laundering (approximately 154,000), and circumventing standards (approximately 110,000) (see figure 2 and appendix 1).
- *The impact of identity-related exploitations by BSA report volumes and cited U.S. dollar values are significant and vary by type:* Attackers most frequently use impersonation tactics, followed by compromise during authentication, and finally, circumventing verification to evade detection. In contrast, compromise has a disproportionally large monetary impact compared to impersonation and circumvention.

Throughout this analytic effort, FinCEN has leveraged its interagency and public-private partnerships to share information and explore best practices for mitigating the threats financial institutions face from gaps and vulnerabilities in identity processes, particularly with respect to fraud and cybercrime.

Scope and Methodology: FinCEN examined approximately 3.8 million BSA reports filed during the Review Period, identifying $566 billion in suspicious activity, to detect identity-related suspicious activity patterns and trends.[5] FinCEN has used a combination of automated and manual review of suspicious activity checkboxes and thousands of free-text entries, including addressing errors, to find "identity-related suspicious activity" — BSA reports that denote suspicious activity tied to the exploitation of one or more steps of "identity processes," as described below, including those steps that occur within financial institutions.[6]

Based on this review, FinCEN has clustered the suspicious activities in identity-related BSA reports into 14 core typologies and confirmed them through a manual review of narratives. Identity processes generally include three steps: validation, verification, and authentication. For the purposes of this report, FinCEN based these identity processes on the NIST Special Publication 800-63A Digital Identity Guidelines.[7] FinCEN has generalized these steps broadly to adequately capture a wide range of unforeseen use cases, implementations, and relationships among verifiers, authorizers, and those being verified. Additionally, the identity processes steps may occur both within and outside financial institutions and their customers, including customers' customers, and their counterparties when operationally accessing authorized

privileges and services. At financial institutions, identity processes are generally conducted during customer account creation, accessing of customer accounts, and when making and processing transactions.

For the purposes of this report, the "Validation" step combines NIST's "Resolution" of an individual as unique, and related processes such as presentation and validation of their attributes, evidence, credentials, etc. The "Verification" step includes the processes used to tie validated attributes and evidence to the correct individual, matching, and related activities. The "Authentication" step includes the authentication process, factors, authorization, access to privileges and services, and similar activities performed by a credential service provider or authorizer such as a financial institution.

Based on these steps, FinCEN has identified three common exploitations of the identity processes (together, identity-related exploitations). Attackers: (i) impersonate others to evade validation; (ii) circumvent or exploit insufficient verification processes; and (iii) use compromised credentials to gain unauthorized access during authentication. FinCEN then mapped the 14 typologies to the relevant identity-related exploitations based on an analysis of the underlying activity. For the purposes of this analysis, FinCEN has only used the *primary* identity-related exploitation to generate results. Although FinCEN has observed some overlap of activities in the data, a primary mode of exploit could be identified for each BSA filing. FinCEN has observed that a successful exploitation of any step of the identity processes weakens the overall integrity of the process and the identity, allowing attackers to gain additional access and to advance schemes.

For the purposes of this analysis, FinCEN divided BSA data gathered into two datasets. The first to calculate the number of BSA reports for each typology, and the second to calculate the identity-related volume of filings and dollar-amounts of suspicious activity, respectively: the aggregate and discrete datasets.

Aggregate Data on Typologies: The aggregate dataset consists of BSA reports focused on 14 core typologies, resulting in a dataset of approximately 2.4 million identity-related BSA reports, reporting $351 billion in suspicious activity, filed during the Review Period. This dataset includes duplicate filings as typologies are not mutually exclusive, and BSA reports may be included in several typologies based on checkboxes, free-text entries, and narrative information provided by filers.[8] [9] [10] This dataset is used throughout the report for statistics tied to criminal typologies, allowing them to be compared to each other by relative impact as measured by the aggregate suspicious activity tied to each typology. This aggregate data was then sorted by the primary identity-related exploitation and filing institution to generate results. All figures in this report reflect comparative analysis based on this aggregate data.

Discrete Volume of BSA Reports and Value of Suspicious Activity: The discrete dataset consists of BSA reports in the aggregate dataset where redundant duplicate data is removed (i.e., de-duplicated), resulting in a dataset of approximately 1.6 million identity-related BSA

reports, reporting $212 billion in suspicious activity, filed during the Review Period. The identity-related BSA reports represent 42% of a total 3.8 million reports filed in 2021. This data set is only used to identify the overall discrete number of reports tied to identity-related suspicious activity volumes and suspicious activity U.S. dollar amounts.

To account for typos and errors, and to reduce outliers, FinCEN has excluded suspicious amounts over $100 million, which constituted less than 1% of the data. Amounts associated with these BSA reports may include attempted transactions and payments that were unpaid. This figure also includes BSA reports that describe continuing suspicious activity or amend earlier reporting, as well as reports that cover expanded networks involved in potential illicit activity. These suspicious amounts may include duplicates, counting of both inbound and outbound transactions, fund transfers between accounts, typos, and errors as submitted by filers. An assessment of the modes of attestation, authentication channels, types of presenters, credentials, and financial instruments were not included and are beyond the scope of this report.

Identity Processes in Financial Institutions

FinCEN regulates a broad range of financial institution types with varying regulatory requirements. In this report, FinCEN has attempted to create a systemic framework to feed back to industry their financial intelligence in an aggregated manner to help mitigate identity-related suspicious activity or identity processes exploitation. At account opening, an identity process is necessary to verify customer identity, establish that a customer is who they claim to be, and enable the financial institution to form a reasonable belief that it knows the true identity of each customer, based on the bank's assessment of the relevant risks and information provided by the customer. Financial institutions may also rely on identity processes as part of authorizing account access by existing customers and when those customers are making transactions with counterparties.

For the purposes of this report, FinCEN has used identity processes drawn generally from definitions detailed in NIST's *Digital Identity Guidelines* (Special Publication 800-63-4 ipd) when relevant to financial institutions' BSA activities. NIST, a congressionally mandated agency of the U.S. Department of Commerce, promotes American innovation and competitiveness by advancing measurement science, standards, and technology. FinCEN recognizes that NIST's guidelines do not address all financial institutions' BSA-related activities, including transaction monitoring among others. Additionally, private sector compliance with NIST standards is voluntary.

NIST's identity processes generally include three steps: validation, verification, and authentication.[11] These steps involve the following:

- **Validation:** The validation stage begins when a customer presents identity attributes and supporting evidence (e.g., birth certificate, passport, driver's license, etc.) — in person or remotely — for review by a financial institution.[12] The financial institution then attempts to

determine: (i) whether the presented identity "exists" (i.e., whether it is tied to a real-life identity); (ii) whether the presented identity is "unique" (i.e., whether it is claimed by only one entity); and (iii) whether the presented information and evidence are authentic and accurate. The financial institution makes these determinations by comparing the presented information and evidence against authoritative government data, such as public records and Social Security Administration data, or third-party data sources, such as credit reporting agency, utility, and employer data (i.e., independent and reliable data sources).[13] [14]

- **Verification:** In the verification stage, the financial institution confirms that the previously validated identity evidence belongs to the customer. The financial institution may, for example, match the customer's appearance in person or virtually via photo or video to a photo on the customer's driver's license, passport, or other photo identification. Verification tools and techniques can rely on humans or be entirely automated. These tools may also use biometrics like facial recognition and liveness detection or verify documents and attributes to determine a match. A variety of other technical and risk data from third parties may also be used in this process.
- **Authentication:** In the authentication stage, a financial institution attempts to assess whether the customer is who they purport to be based on the customer's possession and control of valid authenticators.[15] Financial institutions may engage in other activities around transactions as well, such as verifying counterparties and other transaction monitoring. Authentication provides risk-based assurance that the customer is the same customer whose identity was validated and verified during previous steps of the identity process.[16] The authentication process can occur in person or remotely, be manual or digital, rely on humans or machines, and is considered more robust when it relies on multiple authentication factors (i.e., multi-factor authentication). Common authentication factors include: "Ownership" of something the customer has (e.g., a badge, phone, or cryptographic key); "Knowledge" of something the customer knows (e.g., a password, passphrase, or PIN); and "Inherent" or something the customer is (e.g., a fingerprint or other biometric data).[17]

The proliferation of data breaches compromising personally identifiable information (PII), synthetic identities, and the rapid evolution of Artificial Intelligence (AI) may further enable bad actors to exploit identity processes more easily, quickly, and inexpensively to drive money laundering, fraud, and other cybercrime.

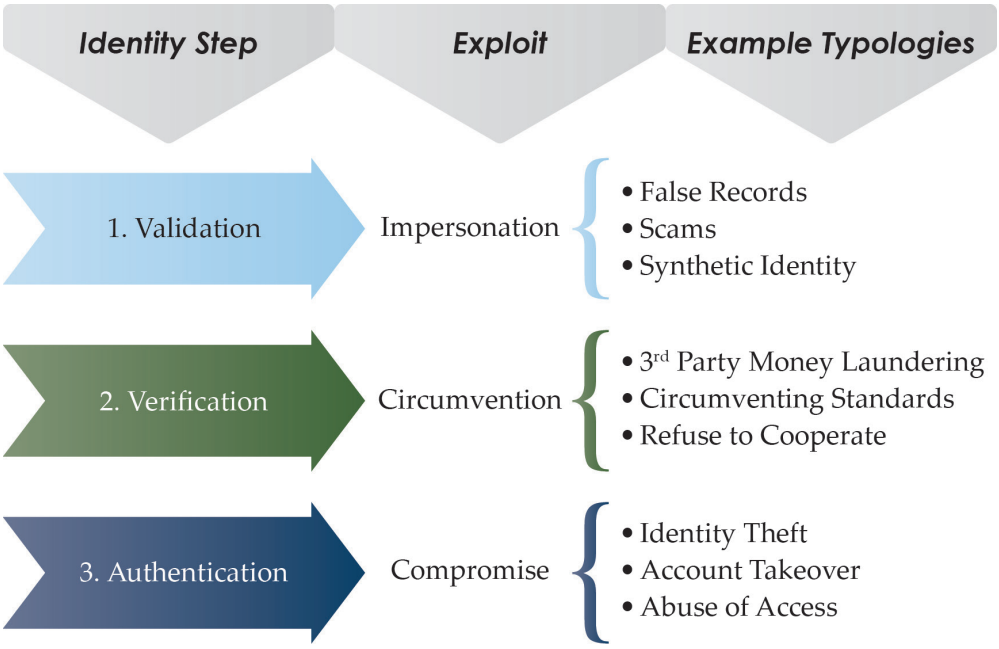
FinCEN Identified Three Identity-Related Exploitations

FinCEN has identified three identity-related exploitations that align to the three steps of the identity process. According to identity-related BSA reports, attackers: (i) impersonate others to evade validation; (ii) circumvent or exploit insufficient verification processes; and (iii) use compromised credentials to gain unauthorized access during authentication.

A successful exploitation of any step of the identity process weakens the overall integrity of the process. Attackers leverage data breaches that expose identity information and credentials, as well as technologies, such as automated password cracking tools. Additionally, the significant shift toward

remote financial services may present additional openings for attackers to exploit breakdowns in identity processes.[18] Attackers target vulnerabilities in virtual and physical environments to steal sensitive information, compromise financial activity, and disrupt business operations.

Figure 1. Identity-Related Exploitations and Typologies Attackers use to Undermine Identity Processes[19]



For example, in the first identity step, validation, perpetrators of "False Records" exploit the validation step by altering, counterfeiting, or forging documentation, records, or forms of payment. Similarly, perpetrators of "Synthetic Identity" use a combination of real and fake PII to fabricate a person or entity to pass validation processes. During the second identity step, verification, bad actors attempt to circumvent verification by using the legitimate credentials of third-parties as straw men in "Third Party Money Laundering" or by using third-parties with lax standards ("Circumventing Standards") or refusing to provide requested information ("Refuse to Cooperate"). During the authentication step, bad actors engage in an "Account Takeover" using stolen authenticators and credentials to gain full access to victim financial accounts. Bad actors who compromise the full PII details of victims ("Identity Theft") create new account relationships such as loans or new accounts to defraud victims. Finally, trusted providers of goods and services misuse their authorized access ("Abuse of Access") to data, information, or systems for financial gain (e.g., insider abuse, corruption, and embezzlement) thereby compromising the authentication step.

Attackers Impersonate Others to Defraud Victims

Attackers impersonate others by providing false identifying information, claiming to be other entities, and otherwise misrepresenting identity information to evade validation. Financial institutions and other victims appeared to have more difficulty identifying impersonation when they lack an

authoritative source to compare identity documentation and evidence. Examples of authoritative sources include records and credentials issued by government sources. Successful impersonation starts in the validation stage and continues throughout identity processes. For example:

- Attackers provide false or inconsistent PII, employment, and payment records to open accounts, receive COVID-19 and other government benefits, and apply for lines of credit, according to identity-related BSA reports.
- Attackers deposit counterfeit checks with forged signatures and other edited payment information.[20]
- As part of various scams, attackers claim to be businesses, charities, financial institutions, government entities, and other individuals to manipulate victims into providing funds, PII, or account or system access. Examples of these scams include romance scams,[21] person-in-need scams,[22] tech and customer support scams,[23] employment scams,[24] and financial institution and government imposter scams.[25]

Attackers Exploit and Circumvent Verification

Attackers circumvent verification to obfuscate the sources and movement of funds. Attackers use third-party transactors to mask the true transactors or refuse to cooperate and provide photo identification or supporting identity documentation. These suspicious activities limit financial institutions' ability to fully identify their customers, their customers' transactions, and their customers' counterparties. For example:

- Attackers build upon successfully passing the validation stage by presenting fake or stolen photo identification usually during online interactions. This overcomes verification, which may be weak or insufficient, allowing attackers to successfully open accounts and lines of credit before scam victims, other intermediaries, and financial institutions performing additional due diligence discover the fraud.
- To obfuscate the true party or parties behind transactions, attackers use money mules, straw buyers, and other third-party transactors, or act as unlicensed or unregistered MSBs to move funds on behalf of others.[26] [27]
- Attackers also fail to provide additional photo identification, proof of funds, and other supporting identity documentation when requested by financial institutions. This inhibits financial institutions' ability to perform additional verification on customers, their customers' transactions, and their customers' counterparties.

Attackers Compromise Authentication and Misuse Credentials to Gain Access

Attackers compromise victims' credentials to gain unauthorized access to data, funds, information, locations, services, and systems. Attackers target victims, their credentials, and their funds directly through account takeovers, business email compromises, brute-force login attacks, data

breaches, identity theft, and other cyber events such as phishing, ransomware, and other endpoint compromises.[28] [29] [30] [31] Attackers then generate illicit proceeds from the sale of stolen credentials or use stolen credentials to open accounts, apply for lines of credit, and conduct transactions. Attackers also use the compromised credentials to access accounts, information, and systems for their own financial gain. For example:

- Attackers use social engineering, computer intrusions, and compromised email accounts to manipulate victims into thinking a trusted person or entity was directing them to make payments. This misleads financial institutions and their customers into conducting fund transfers to attacker-controlled accounts or allows attackers to directly gain unauthorized access to victims' accounts and execute unauthorized peer-to-peer or wire transfers.[32] [33] [34]
- Additionally, attackers misuse their position as authenticators or their insider access to identity processes for their own financial gain. For example, compromised powers of attorney exploit elders and move funds from victims' accounts to their own; corrupt individuals abuse their authority or position for personal gain; and bad actors access confidential, proprietary, or non-public information and use that information to engage in insider trading and market manipulation.

Fraud Most Frequently Reported Illicit Finance Typology

As previously noted, FinCEN has identified over 14 typologies commonly reported in identity-related BSA reports. The most frequently reported typologies are fraud, false records, identity theft, third-party money laundering, and circumventing standards (see figure 2). The top five typologies account for 88% of the identity-related BSA reports and 74% of the total identity-related suspicious activity amount during the Review Period.[35] Some of these typologies may be considered types of fraud but are separated for the purposes of this report to account for differences in how fraud perpetration methods exploit identity processes.

Figure 2. Top Typologies Reported, January to December 2021[36]

Typology	Number of BSA reports	Total Suspicious Amounts
General Fraud	1.2 million	$149 billion
False Records	~423,000	$45 billion
Identity Theft	~222,000	$36 billion
Third-Party Money Laundering	~154,000	$18 billion
Circumventing Standards	~110,000	$12 billion
Total	**2.1 million**	**$260 billion**

General Fraud

General fraud is by far the most frequently reported suspicious activity by both number of BSA reports and total suspicious activity amount. This is consistent with the National Money Laundering Risk Assessment that found that fraud continues to be the largest driver of money laundering activity

in terms of scope and magnitude of illicit proceeds.[37] Fraud is also considered one of the eight national AML/CFT priorities.[38] Filers report fraud in 1.2 million identity-related BSA reports with $149 billion in suspicious activity. Filers report many types of fraud, including bust out schemes (where attackers open credit card accounts with false information and then max out the cards), check fraud, credit and debit card fraud, and many types of COVID-19 fraud.[39] Attackers also commit several types of check fraud. They deposit counterfeit checks with edited payment information and forged signatures, and then exploit check settlement times between financial institutions by accessing funds before financial institutions process the checks and discover insufficient funds (i.e., check kiting). Attackers also obtain compromised credit and debit card numbers and conduct unauthorized transactions. As part of this analysis, FinCEN has separated several typologies that are generally considered subtypes of fraud, such as account takeover, business email compromise, identity theft, check kiting, and synthetic identities (see appendix 1).

False Records

The second most frequently reported typology is false records, with approximately 423,000 identity-related BSA reports and $45 billion in suspicious activity.[40] Attackers provide false identification, documentation, payments, and records in interactions with financial institutions. For example, attackers provide fake Social Security numbers, inconsistent identifying information, false income and employment documents, false invoices, forged signatures, and counterfeit money when opening accounts, applying for lines of credit, or conducting transactions. Some financial institutions successfully identify false records during customer onboarding or during transactions and deny attackers' attempts. Others only identify concerns after opening accounts, accepting funds, or funding loans. Some false records are not discovered until another financial institution or an additional party, sometimes victims, reviews the activity.

Identity Theft

More than 222,000 identity-related BSA reports documented identity theft. These identity-related BSA reports have found $36 billion in suspicious activity and describe attackers' attempts to use compromised identifying information belonging to a real individual or entity to open accounts and apply for lines of credit.[41] This typology heavily overlaps with false records, as attackers present false information, documentation, and signatures to carry out identity theft. Financial institutions often identify the activity after discovering false records, additional fraud, or determining the victim is deceased, incapacitated, incarcerated, or otherwise unable to apply at the time of application. In some cases, other financial institutions involved in the lending process discover identity inconsistencies and report these to the filer, or victims report the fraud themselves.

Third-Party Money Laundering

FinCEN has identified approximately 154,000 identity-related BSA reports reporting $18 billion in suspected third-party money laundering activity.[42] Individuals act as straw buyers and money mules to conduct transactions and move funds on behalf of others. Straw buyers apply for vehicle

and mortgage loans on behalf of another person and conceal the identity of the true purchaser.[43] Similarly, money mules receive and transfer funds on behalf of others. Money mules are often recruited online through scams and may be witting or unwitting participants in laundering fraud proceeds while also concealing the identity of the true transactor, thereby circumventing verification.

Circumventing Standard Processes

FinCEN has identified approximately 110,000 identity-related BSA reports, reporting $12 billion in suspicious activity, in which filers have reported entities engaged in transactions on behalf of others that are not applying standard processes, such as proper recordkeeping or registration, that enable financial institutions to verify customers and counterparties. The majority of these identity-related BSA reports find that entities not registered with FinCEN appear to receive and send funds on behalf of others in what appear to be informal value transfer systems or unlicensed MSB activity, often using peer-to-peer money transfer applications.[44] Filers reportedly analyze and identify these transactions based on the volume, dollar amounts, payment comments, and number of counterparties, and described the activity as inconsistent with typical usage of the accounts. Some of these BSA reports may be the result of entities not knowing or understanding acceptable practices and regulatory requirements while others appeared to be attempts to advance fraud, cybercrime, or other types of identity-related suspicious activity.

Significant Volume and Value Impact of Identity-Related Exploitations

Attackers most frequently use impersonation tactics to exploit identity processes, followed by leveraging compromised credentials for unauthorized access during authentication, and finally, evading detection by circumventing verification (see figure 3)—according to analysis of 2.4 million identity-related BSA reports.

- 69%, or 1.7 million identity-related BSA reports, report that attackers impersonated businesses, charities, financial institutions, government entities, and other individuals to defraud victims and financial institutions.
- 18%, or approximately 446,000 identity-related BSA reports, report that attackers used compromised credentials to gain unauthorized access or misused their authorized access to generate illicit proceeds. Compromises are disproportionally costly as they accounted for 32% of the total suspicious activity amount or $112 billion.
- 13%, or approximately 323,000 identity-related BSA reports, report that attackers either exploit weak or insufficient verification, or circumvent verification altogether.

Figure 3. Exploitations Reported in Identity-Related BSA Reports, January to December 2021

Identity Exploitation	Number of BSA Reports	Percent of BSA Reports	Total Suspicious Amounts	Percent of Suspicious Amount
Impersonation	1.7 million	69%	$200 billion	57%
Compromise	~446,000	18%	$112 billion	32%
Circumvention	~323,000	13%	$39 billion	11%
Total	**2.4 million**	**100%**	**$351 billion**	**100%**

Identity-Related BSA Reports Vary by Financial Institution Type

While identity-related suspicious activity impacts all types of financial institutions reporting under the BSA, depository institutions file the most identity-related BSA reports (see figure 4). Additionally, while most financial institutions report impersonation as their top identity exploitation, MSBs most often report circumvention of verification (see figure 5). Casinos and card clubs report an equal amount of impersonation and circumvention of verification exploitations.

Figure 4. Filing of Identity-Related BSA Reports: Categorized by Financial Institution Type, January to December 2021[45] [46] [47]

Financial Institution Type	Number of BSA Reports	Percent of BSA Reports	Total Suspicious Amounts	Percent of Suspicious Amount
Depository Institution	1.3 million	54%	$201 billion	57%
Money Services Business	~501,000	21%	$31 billion	9%
Other	~429,000	18%	$75 billion	21%
Securities/Futures	~103,000	4%	$33 billion	9%
Loan or Finance Company	~51,000	2%	$7 billion	2%
Casino/Card Club	~14,000	1%	$438 million	<1%
Housing GSE	~9,000	<1%	$4 billion	1%
Insurance Company	~3,000	<1%	$761 million	<1%
Total	**2.4 million**	**100%**	**$351 billion**	**100%**

Figure 5. Reported Identity-Related Exploitations: Categorized by Financial Institution Type, January to December 2021

Financial Institution Type	Impersonation	Compromise	Circumvention	Total
Depository Institution	1 million	~279,000	~40,000	1.3 million
Money Services Business	~190,000	~46,000	~265,000	~501,000
Other	~342,000	~77,000	~10,000	~429,000
Securities/Futures	~62,000	~40,000	~1,000	~103,000
Loan or Finance Company	~49,000	~2,000	~300	~51,000
Casino/Card Club	~6,500	~1,000	~6,500	~14,000
Housing GSE	~8,500	~100	~50	~9,000
Insurance Company	~2,000	~1,000	~200	~3,000
Total	**1.7 million**	**~446,000**	**~323,000**	**2.4 million**

Opportunities for Public-Private Partnership and Application of Emerging Technologies

In accordance with the AML Act of 2020, FinCEN has engaged with the private and public sectors to assess opportunities to explore the risks and challenges emerging technologies present to financial institutions for preventing and detecting identity compromise. This FTA helps establish a framework to better identify and diagnose where identity processes are failing across the financial ecosystem, assess the impact of such failings, and inform policy making. FinCEN has collaborated with other government agencies to share respective approaches and efforts to develop frameworks and models that may inform best practices. Emerging technologies such as digital identity, AI, and Privacy-Enhancing Technologies (PET) may help mitigate customer identity process exploitations and combat a wide variety of illicit finance typologies.[48] FinCEN continues to engage with partners and explore the utility of available and developing identity solutions to enable stronger identity processes and counter the underlying drivers of identity-related crime.

Appendix 1: Assessed Typology Results

Typology	Definition	Primary Exploitation	Number of BSA reports	Suspicious Amounts
General Fraud	Wrongful or criminal deception intended to result in financial or personal gain.[49]	Impersonation	1.2 million	$149 billion
False Records	Altering, counterfeiting, or forging documentation, records, or forms of payment.	Impersonation	~423,000	$45 billion
Identity Theft	Using identifying information unique to the rightful owner without the rightful owner's permission.	Compromise	~222,000	$36 billion
Third-Party Money Laundering	Laundering of illicit proceeds by a person who was not involved in the commission of the predicate offense.[50]	Circumvention	~154,000	$18 billion
Circumventing Standards	Lack of adherence to standards or acceptable practices, knowingly or unknowingly.	Circumvention	~110,000	$12 billion
Account Takeover	Deliberate compromise of a victim's account to remove, steal, procure, or otherwise affect the victim's funds.[51]	Compromise	~80,000	$9 billion
Abuse of Access	Misuse of authorized access to data, information, or systems for financial gain, (e.g. insider abuse, corruption, and embezzlement).[52]	Compromise	~76,000	$48 billion
Refusal to Cooperate	Refusal of requests to follow procedures or provide information.	Circumvention	~59,000	$8 billion
Cyber Incident	Attempt to compromise or gain unauthorized access to electronic systems, services, resources, or information.[53]	Compromise	~47,000	$11 billion
Scam	Schemes designed to manipulate someone into giving something away, especially money.[54]	Impersonation	~28,000	$6 billion

Typology	Definition	Primary Exploitation	Number of BSA reports	Suspicious Amounts
Business Email Compromise	Schemes where criminals compromise the email accounts of victims.[55]	Compromise	~20,000	$8 billion
False Claims	Knowing submission of an untrue claim of fraud, identity theft, or unauthorized transactions.	Impersonation	~6,000	$164 million
Synthetic Identity	The use of a combination of real and fake PII to fabricate a person or entity.[56]	Impersonation	~3,000	$182 million
Kiting	The fraudulent use of financial instruments, usually checks, between two or more bank accounts to cover insufficient funds.[57]	Impersonation	~2,000	$362 million
Total			**2.4 million**	**$351 billion**

Endnotes

1 Congress enacted the Anti-Money Laundering Act as Division F, §§ 6001-6511, of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283 (2021).

2 The data relied upon in this FTA consists of information filed with FinCEN pursuant to the BSA, herein referred to as "BSA data," and is not a complete representation of all identity-related suspicious activity during the Review Period. Trends represented in this report illustrate identification and reporting of identity-related suspicious activity and may not reflect the dates actually associated with incidents.

3 This report is not intended to provide additional guidance or establish new requirements for financial institution customer identification programs.

4 "Other" is selected by the filer when none of the additional types of financial institutions apply (i.e., depository institution, securities/futures, et al). The "Other" filer type may include BSA reports filed by holding companies or dealer in precious metals, stones or jewels. For more information, see "SAR Filing by Industry," Financial Crimes Enforcement Network, https://www.fincen.gov/reports/sar-stats/sar-filings-industry.

5 Total figures reported in this FTA may differ from total figures reported elsewhere as FinCEN examined all BSA reports filed in 2021 including initial filings and updates to develop this identity framework.

6 FinCEN reviewed 247 checkboxes and identified 135 relevant to this study. FinCEN reviewed 15,996 unique "Other" free text fields and identified 2,326 terms describing identity-related suspicious activity that was further sorted into 238 groups of activity.

7 For more information, see "NIST Special Publication 800-63-4 (Initial Public Draft)." National Institute of Science and Technology, NIST SP 800-63-4 ipd (initial public draft), Digital Identity Guidelines.

8 Filers have the ability to select multiple suspicious activities (as applicable) on the reports they submit, and many BSA reports reflect more than one type of activity. All options checked in fixed-fields 29(a) through 38(z), within Part II (Suspicious Activity Information) of FinCEN Form 111, are individually counted and then aggregated for that type of suspicious activity. For example, an institution electronically files two SARs, one citing Check Fraud (31c) as the suspicious activity and the other listing Check Fraud (31c) and Identity Theft (35g). These would be tabulated as two (2) instances of Check Fraud and one (1) instance of Identity Theft. Moreover, as multiple activities may be reported by a filer, the total number of overall suspicious activities is greater than the total number of filings received.

9 FinCEN assessed BSA data filed between 1 January and 31 December 2021 for accuracy, duplication, and false positives based on checkboxes, free-text entries, and narrative information provided by filers.

10 For more information, see Appendix 1.

11 For the purposes of this report, FinCEN based these identity process steps on the NIST Special Publication 800-63-4 ipd *Digital Identity Guidelines* identity proofing and enrollment process and authentication and lifecycle management process.

12 For more information, see "Guidance on Digital Identity," Financial Action Task Force (FATF), March 2020, https://www.fatf-gafi.org/publications/financialinclusionandnpoissues/documents/digital-identity-guidance.html.

13 For more information, see the Social Security Administration's electronic Consent Based Social Security Number Verification Service https://www.ssa.gov/dataexchange/eCBSV/ and "Catalog of Technical Standards for Digital Identification Systems," World Bank Group, September 2018, https://documents.worldbank.org/en/publication/documents-reports/documentdetail/707151536126464867/catalog-of-technical-standards-for-digital-identification-systems.

14 For the purposes of this report, identity processes may include but are not limited to the processes referenced by the Customer Identification Program or CIP. However, the definition of "verification" in this report more closely aligns with the NIST definition that distinguishes between verification and validation steps versus the CIP definition of "verification."

15 For more information, see "NIST Special Publication 800-63-4 (Initial Public Draft)," National Institute of Science and Technology, NIST SP 800-63-4 ipd (initial public draft), Digital Identity Guidelines.

16 For more information, see "Authentication and Access to Financial Institution Services and Systems," Federal Financial Institutions Examination Council, FFIEC Guidance, 11 August 2021, https://www.ffiec.gov/guidance/Authentication-and-Access-to-Financial-Institution-Services-and-Systems.pdf.

17 For more information, see "Guidance on Digital Identity," Financial Action Task Force (FATF), March 2020, https://www.fatf-gafi.org/publications/financialinclusionandnpoissues/documents/digital-identity-guidance.html.

18 For more information, see "Authentication and Access to Financial Institution Services and Systems," Federal

Financial Institutions Examination Council, FFIEC Guidance, 11 August 2021, https://www.ffiec.gov/guidance/Authentication-and-Access-to-Financial-Institution-Services-and-Systems.pdf.

19 As noted above, FinCEN mapped the 14 typologies to the relevant identity-related exploitations based on an analysis of the underlying activity. For the purpose of this analysis, only the primary identity-related exploitation was used to generate results.

20 For more information, see "FinCEN Alert on Nationwide Surge in Mail Theft-Related Check Fraud Schemes Targeting the U.S. Mail," Financial Crimes Enforcement Network, FinCEN Alert #FIN-2023-Alert003, 27 February 2023, https://www.fincen.gov/sites/default/files/shared/FinCEN%20Alert%20Mail%20Theft-Related%20Check%20Fraud%20FINAL%20508.pdf.

21 Romance scams (also referred to as "online dating," "confidence," or "sweetheart" scams) involve attackers creating a fictitious profile on an online dating app or website to establish a close or romantic relationship, typically with older adults, to exploit their confidence and trust. For more information, see "Advisory on Elder Financial Exploitation," Financial Crimes Enforcement Network, FinCEN Advisory #FIN-2022-A002, 15 June 2022, https://www.fincen.gov/sites/default/files/advisory/2022-06-15/FinCEN%20Advisory%20Elder%20Financial%20Exploitation%20FINAL%20508.pdf.

22 FinCEN observed attackers impersonating relatives, charities, and other persons-in-need before requesting victims send funds immediately to resolve the situation. For more information, see "Advisory on Elder Financial Exploitation," Financial Crimes Enforcement Network, FinCEN Advisory #FIN-2022-A002, 15 June 2022, https://www.fincen.gov/sites/default/files/advisory/2022-06-15/FinCEN%20Advisory%20Elder%20Financial%20Exploitation%20FINAL%20508.pdf.

23 In tech and customer support scams, attackers impersonated technology companies or other service providers, and contacted victims stating they needed access to their computers to provide a refund, and then claimed to "overpay" the victim while actually moving the victims' funds between their own accounts without their knowledge. Attackers often demanded that victims repay the difference with either wire transfers or gift cards. For more information, see "Advisory on Elder Financial Exploitation," Financial Crimes Enforcement Network, FinCEN Advisory #FIN-2022-A002, 15 June 2022, https://www.fincen.gov/sites/default/files/advisory/2022-06-15/FinCEN%20Advisory%20Elder%20Financial%20Exploitation%20FINAL%20508.pdf.

24 In employment scams, attackers acted as potential employers and either requested that victims pay a fee before starting work or made victims into witting or unwitting money mules to move illicit funds. For more information, see "Advisory on Imposter Scams and Money Mule Schemes Related to Coronavirus Disease 2019 (COVID 19)," Financial Crimes Enforcement Network, FinCEN Advisory #FIN-2020-A003, 7 July 2020, https://www.fincen.gov/sites/default/files/advisory/2020-07-07/Advisory_%20Imposter_and_Money_Mule_COVID_19_508_FINAL.pdf.

25 In financial institution and government imposter scams, attackers impersonated financial institutions or government entities and claimed victims needed to provide PII or pay for outstanding balances and legal infractions. For more information, see "Advisory on Elder Financial Exploitation," Financial Crimes Enforcement Network, FinCEN Advisory #FIN-2022-A002, 15 June 2022, https://www.fincen.gov/sites/default/files/advisory/2022-06-15/FinCEN%20Advisory%20Elder%20Financial%20Exploitation%20FINAL%20508.pdf.

26 Money mules are individuals who transfer money on behalf of others. These individuals may be witting or unwitting participants in laundering illicit proceeds. Money mules are often recruited online through other scams. For more information, see "Advisory on Imposter Scams and Money Mule Schemes Related to Coronavirus Disease 2019 (COVID 19)," Financial Crimes Enforcement Network, FinCEN Advisory #FIN-2020-A003, 7 July 2020, https://www.fincen.gov/sites/default/files/advisory/2020-07-07/Advisory_%20Imposter_and_Money_Mule_COVID_19_508_FINAL.pdf.

27 Straw buyers are entities who allow their name, identifiers, and credit rating to be used to secure lines of credit. In real estate transactions, the straw buyer generally understands they will neither occupy the property nor make payments on the loan. The straw buyer is generally paid a fee by the entity who either intends to flip the property or use the loan to launder illicit funds. For more information, see "Suspected Money Laundering in the Residential Real Estate Industry," Financial Crimes Enforcement Network, April 2008, https://www.fincen.gov/sites/default/files/shared/MLR_Real_Estate_Industry_SAR_web.pdf.

28 For more information, see "Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime," Financial Crimes Enforcement Network, FinCEN Advisory #FIN-2016-A005, 25 October 2016, https://www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508_2.pdf.

29 For more information, see "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments," Financial Crimes Enforcement Network, FinCEN Advisory #FIN-2021-A004, 8 November 2021, https://www.fincen.gov/sites/default/files/advisory/2021-11-08/FinCEN%20Ransomware%20Advisory_FINAL_508_.pdf.

30 For more information, see "Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021," Financial Crimes Enforcement Network, FinCEN Financial Trend Analysis, 15 October 2021, https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf, and "Ransomware Trends in Bank Secrecy Act Data between July 2021 and December 2021: Russia-Related Malware Dominates Ransomware Landscape," Financial Crimes Enforcement Network, FinCEN Financial Trend Analysis, 1 November 2022, https://www.fincen.gov/sites/default/files/2022-11/Financial%20Trend%20Analysis_Ransomware%20FTA%202_508%20FINAL.pdf.

31 Endpoints are devices such as mobile phones, computers, servers, and other devices that are connected to networks.

32 For more information, see "Account Takeover Activity," Financial Crimes Enforcement Network, FinCEN Advisory #FIN-2011-A016, 19 December 2011, https://www.fincen.gov/sites/default/files/advisory/FIN-2011-A016.pdf.

33 For more information, see "Advisory to Financial Institutions on Email Compromise Fraud Schemes," Financial Crimes Enforcement Network, FinCEN Advisory #FIN-2016-A003, 6 September 2016, https://www.fincen.gov/sites/ default/files/advisory/2016-09-09/FIN-2016-A003.pdf.

34 For more information, see "Business Email Compromise in the Real Estate Sector: Threat Pattern and Trend Information, January 2020 to December 2021," Financial Crimes Enforcement Network, FinCEN Financial Trend Analysis, 30 March 2023, https://www.fincen.gov/sites/default/files/shared/Financial_Trend_Analysis_BEC_FINAL.pdf.

35 For the full list of assessed typologies, see Appendix 1. FinCEN reviewed and excluded SARs reporting other identity-related typologies due to insufficient detail for thorough analysis.

36 These typologies are not mutually exclusive, and BSA reports may be included in several typologies based on checkboxes, free-text entries, and narrative information provided by filers.

37 For more information, see "National Money Laundering Risk Assessment," U.S. Department of Treasury, February 2022, https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment.pdf.

38 For more information, see "Anti-Money Laundering and Countering the Financing of Terrorism National Priorities," Financial Crimes Enforcement Network, 30 June 2021, https://www.fincen.gov/sites/default/files/shared/AML_CFT Priorities (June 30%2C 2021).pdf.

39 For more information, see "Fraud FAQs – What is Fraud Waste and Abuse," Pandemic Oversight, General & Fraud FAQs, https://www.pandemicoversight.gov/faq-resources/general-and-fraud.

40 False records are altered, counterfeit, or forged documentation, records, or forms of payment.

41 Identity theft is using identifying information unique to the rightful owner without the rightful owner's permission. For more information, see "Identity Theft: Trends, Patterns, and Typologies Reported in Suspicious Activity Reports," Financial Crimes Enforcement Network, October 2010, https://www.fincen.gov/sites/default/files/shared/ID%20Theft%2011_508%20FINAL.pdf.

42 The Financial Action Task Force (FATF) defines third-party money laundering as the laundering of proceeds by a person who was not involved in the commission of the predicate offence. For more information, see "Professional Money Laundering," Financial Action Task Force, 2018, https://www.fatf-gafi.org/media/fatf/documents/Professional-Money-Laundering.pdf.

43 For more information, see "Mortgage Loan Fraud," Financial Crimes Enforcement Network, An Industry Assessment based upon Suspicious Activity Report Analysis, November 2006, https://www.fincen.gov/mortgage-loan-fraud.

44 Informal value transfer systems are a type of MSB that may legally operate in the United States, so long as they abide by applicate and federal laws, including registering with FinCEN and complying with AML/CFT provisions of the BSA. For more information, see "Information Value Transfer Systems," Financial Crimes Enforcement Network, FinCEN Advisory #FIN-2010-A011, 1 September 2010 / Updated 5 July 2022, https://www.fincen.gov/sites/default/files/advisory/2022-07-05/FIN-2010-A11-updated_508.pdf.

45 These figures are based on identity-related BSA reports and their typologies. If filers reported multiple typologies, filer type may apply to all reported.

46 "Other" is selected by the filer when none of the additional types of financial institutions apply (i.e., depository institution, securities/futures, et al). The "Other" filer type may include BSA reports filed by holding companies or dealer in precious metals, stones or jewels. For more information, see "SAR Filing by Industry," Financial Crimes

Enforcement Network, https://www.fincen.gov/reports/sar-stats/sar-filings-industry.

47 Percentages reflect comparisons to the aggregate data set.

48 A digital identity solution (otherwise known as a digital identity system or digital identity service) is a set of processes that use digital technologies to assert and prove remotely and/or in-person the official identity of natural persons, organizations, or machines.

49 For more information, see "Fraud FAQs – What is Fraud Waste and Abuse," Pandemic Oversight, General & Fraud FAQs, https://www.pandemicoversight.gov/faq-resources/general-and-fraud.

50 For more information, see "Professional Money Laundering," Financial Action Task Force, 2018, https://www.fatf-gafi.org/media/fatf/documents/Professional-Money-Laundering.pdf.

51 For more information, see "Identifying Account Takeover Activity," Financial Crimes Enforcement Network, FinCEN Advisory #FIN-2011-A016, 19 December 2011, https://www.fincen.gov/sites/default/files/advisory/FIN-2011-A016.pdf.

52 For more information, see "The SAR Activity Review – Trends, Tips, and Issues," Financial Crimes Enforcement Network, Issue 20, October 2011, https://www.fincen.gov/sites/default/files/shared/sar_tti_20.pdf, and "Advisory on Kleptocracy and Foreign Public Corruption," Financial Crimes Enforcement Network, FinCEN Advisory #FIN-2022-A001, 14 April 2022, https://www.fincen.gov/sites/default/files/advisory/2022-04-14/FinCEN%20Advisory%20Corruption%20FINAL%20508.pdf.

53 For more information, see "Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime," Financial Crimes Enforcement Network, FinCEN Advisory #FIN-2016-A005, 25 October 2016,https://www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508_2.pdf.

54 For more information, see "Scams," Federal Trade Commission, https://consumer.ftc.gov/scams, and "What are Some Common Types of Scams?" Consumer Financial Protection Bureau, 26 April 2023, https://www.consumerfinance.gov/ask-cfpb/what-are-some-common-types-of-scams-en-2092/.

55 For more information, see "Updated Advisory on Email Compromise Fraud Schemes Targeting Vulnerable Business Processes," Financial Crimes Enforcement Network, FinCEN Advisory #FIN-2019-A005, 16 July 2019, https://www.fincen.gov/sites/default/files/advisory/2019-07-16/Updated%20BEC%20Advisory%20FINAL%20508.pdf.

56 For more information, see "Synthetic Identity Fraud Defined," The Federal Reserve, FedPayments Improvement, (n.d.), https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/synthetic-identity-payments-fraud/syntheticidentity-fraud-defined/.

57 For more information, see "The SAR Activity Review – Trends, Tips, and Issues," Financial Crimes Enforcement Network, Issue 20, October 2011, https://www.fincen.gov/sites/default/files/shared/sar_tti_20.pdf.