Financial Crimes Enforcement Network
U.S. Department of the Treasury

Washington, D.C. 20220

ANDREA GACKI
DIRECTOR, FINCEN

PREPARED REMARKS
IDENTITY PROJECT COLLOQUIUM
WASHINGTON, DC

Introduction

Good afternoon. My name is Andrea Gacki, and I'm the Director of the Financial Crimes Enforcement Network (FinCEN).

I'd like to conclude today's meeting by talking about a recent achievement and follow-on news that is relevant to this group—which is, the ongoing work related to our Identity Project.

This work is important and timely. Understanding who is truly behind illicit transactions is at the heart of FinCEN's work, and we need to monitor and stay ahead of related vulnerabilities to improve our anti-money laundering and countering the financing of terrorism (AML/CFT) regime.

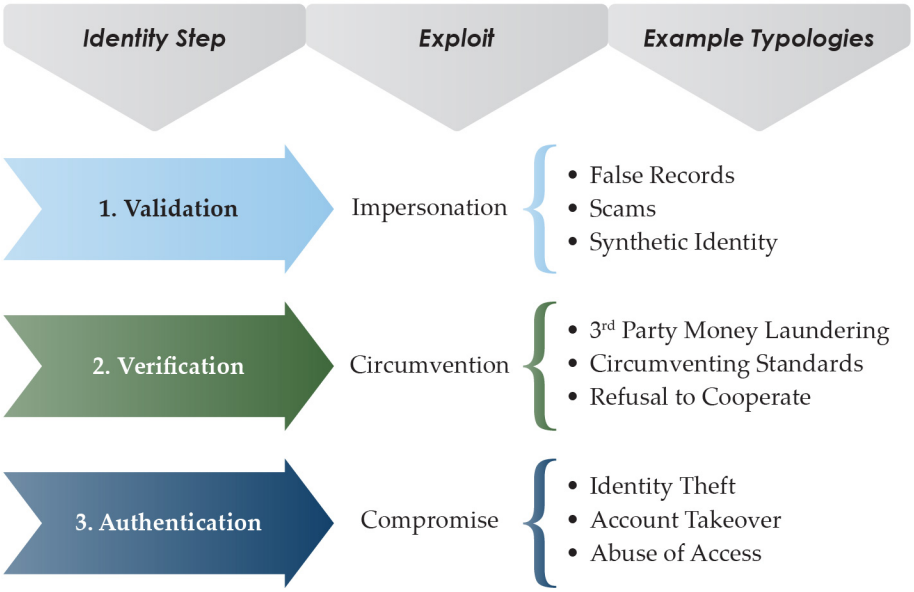
Identity Project Framework

At FinCEN, we are hard at work using our resources to help financial institutions navigate the challenges around identity.

Robust customer identity processes are the foundation of a secure and trusted U.S. financial system and are fundamental to the effectiveness of every financial institution's AML/CFT program.

In January of this year, in a Financial Trend Analysis addressing identity-related suspicious activity, we published our Identity Project framework (*See figure below*) and applied it to Bank Secrecy Act reports filed with FinCEN in 2021.

FinCEN Identity Project Framework



Source: FinCEN Identity Financial Trend Analysis, January 9, 2024. Figure 1. Identity-Related Exploitations and Typologies Attackers use to Undermine Identity Processes.

The Financial Trend Analysis outlines a framework to categorize and quantify how bad actors exploit identity-related processes at account opening, or when accessing accounts or conducting transactions, to perpetrate crimes.

A real-life example of the three Identity Project framework steps is when you open a bank account for the first time.

You probably went to your local bank branch and sat down with a customer representative who asked for your license and other documents.

- During that experience, the representative likely examined the license to ensure that it had the properties of a real license—this is called Validation.
- The representative likely looked at the image and at your face to make sure that the image on the license matched your face—this is called Verification.
- Then you were likely given a card and chose a username and password, or authenticators, that allowed you to access your account in the future—this is called Authentication.

Exploitations are possible at all steps of those identity processes. For example:

- During Validation, an attacker could present a counterfeit license or altered documents.
- During Verification, an attacker could present real documents that belong to someone else, thereby circumventing verification.
- During Authentication, an attacker could use a stolen username and password—which is compromised—in order to access an account.

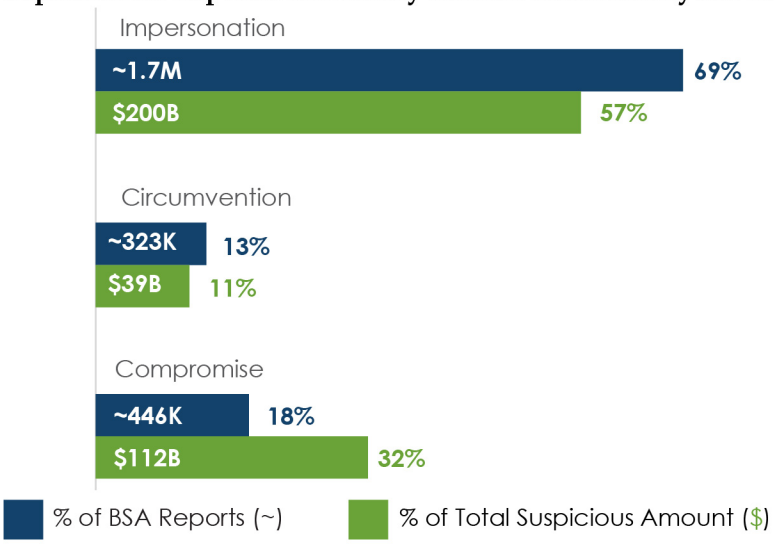
Identity Project 2021 Results

In the January Identity Financial Trend Analysis, we applied the framework and fed back to industry the 2021 Bank Secrecy Act data.

This report reveals the existence of significant identity-related exploitations, through a large variety of schemes.

And the report highlights the value of Bank Secrecy Act information filed by regulated financial institutions and other members of the public.

Exploitations Reported in Identity-Related Bank Secrecy Act Reports



Source: FinCEN Identity Financial Trend Analysis, January 9, 2024.
Figure 3. January to December 2021.

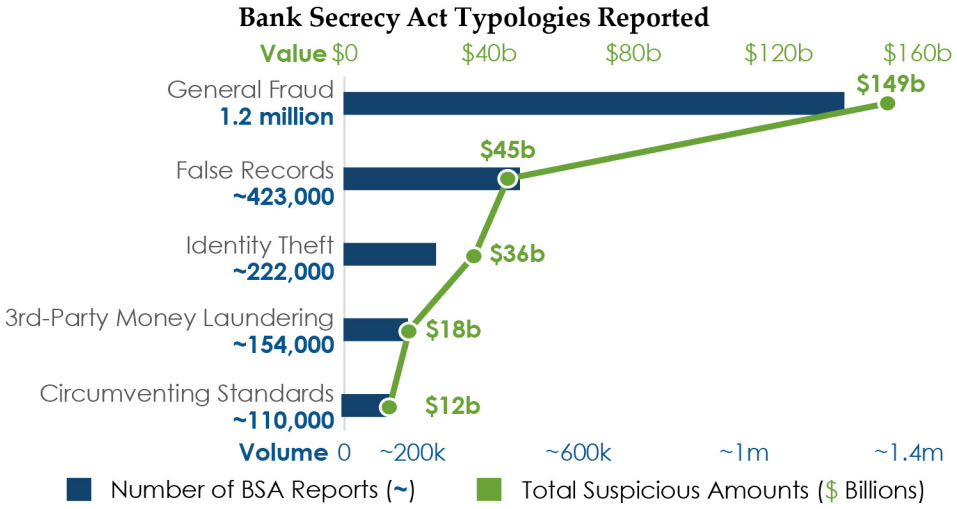
Of note, 69% of the reports and 57% of the value cited in reports, equivalent to $200 billion (*See figure above*), relate to impersonation challenges involving the validation of a unique, real human and identity evidence.

On a related note, we recognize that innovations in digital identity, like emerging state mobile driver's licenses, have the potential to address impersonation exploitations, as well as strengthen AML/CFT compliance.

Digital identity solutions can also help banks and other financial institutions more effectively and efficiently identify and report illicit financial activity after account opening.

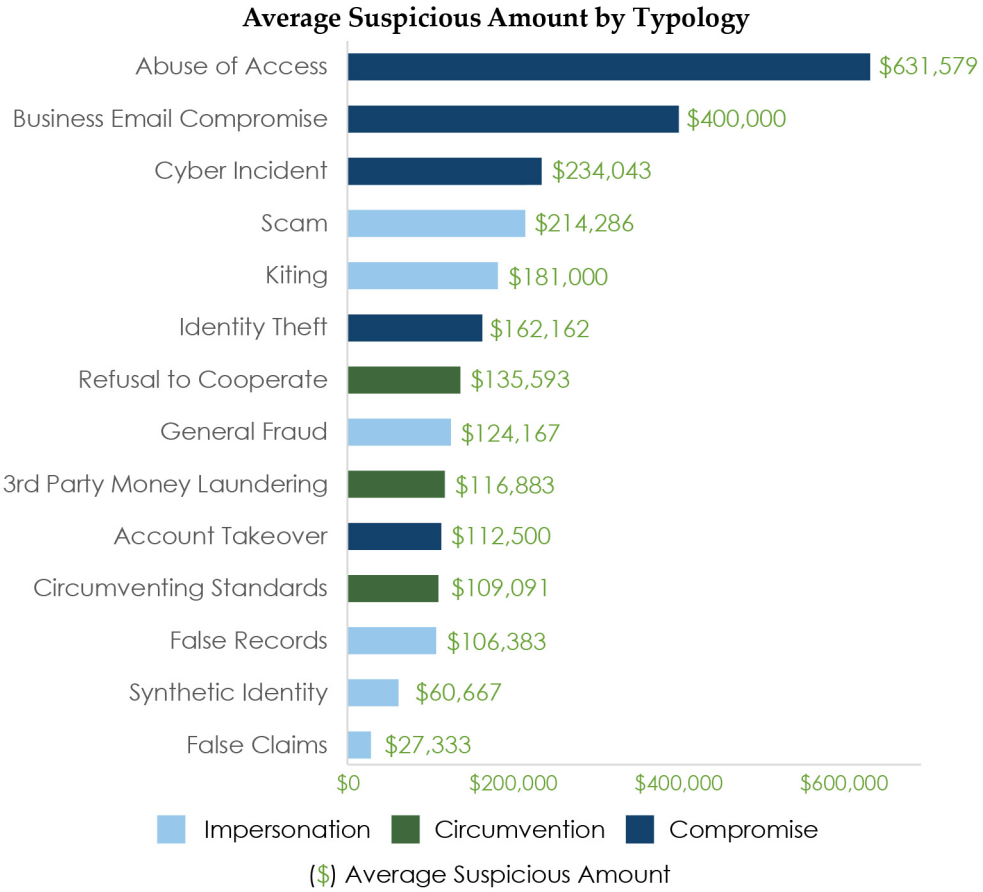
This is important because the use of compromised credentials has a disproportionately higher monetary impact—around 18% of reports, but 32% of total transaction value—than impersonation and circumvention of verification exploitations.

Underscoring my earlier point about the overlap between fraud and AML/CFT, we saw that general fraud was almost a third of records included in the 2021 Identity Financial Trend Analysis and close to $150 billion in transaction value (*See figure below*).



Source: FinCEN Identity Financial Trend Analysis, January 9, 2024.
Figure 2. January to December 2021.

Understanding that cybercrime—like abuse of access, business email compromise, and cyber incidents—has the highest per report monetary impact *(see figure below)*, when announcing the Financial Trend Analysis on identity, I encouraged financial institutions to work across their internal departments to address these identity-related schemes.



Source: FinCEN Identity Financial Trend Analysis, January 9, 2024. Appendix 1. January to December 2021.
Note: Average Suspicious Amount is calculated by dividing Total Suspicious Amount Cited in Bank Secrecy Act (BSA) Reports Categorized by Type by Total BSA Reports Categorized by Report Type.

We hope that our simplified language around exploitations—impersonation and circumvention of verification at account opening and use of compromised credentials during account access and when transacting—will help financial institutions consider how to prevent exploitations that enable fraudsters to harm customers and launder ill-gotten gains, regardless of whether the issue is related to fraud, cybercrime, or AML/CFT.

We believe that all three areas—fraud, cybercrime, or AML/CFT—face the same challenge of determining "who is behind the keyboard."

With AI-related threats rising, we believe that the Identity Project framework will help financial institutions identify at which stage exploitations are occurring.

You will note these new visuals are the tables in the Identity Financial Trend Analysis. We have created them and added average suspicious amounts by Bank Secrecy

Act Report type following private sector feedback. Our goal is to help financial institutions understand the results and consider the monetary impact of different exploitations as they attempt to mitigate illicit finance.

Identity Project 2022-2023 Results Preview

I would like to preview a couple of highlights from the team's work on the 2022 and 2023 Identity Project data sets.

The volume of total Bank Secrecy Act filings has grown, from 3.8 million reports in 2021 to 4.7 million in 2023. Transaction value has grown at a slower pace.

The percentage of volume and value attributable to identity-related SARs has also grown since 2021. Based on initial indications, by 2023, identity-related SARs accounted for around half of value and almost three quarters of volume.

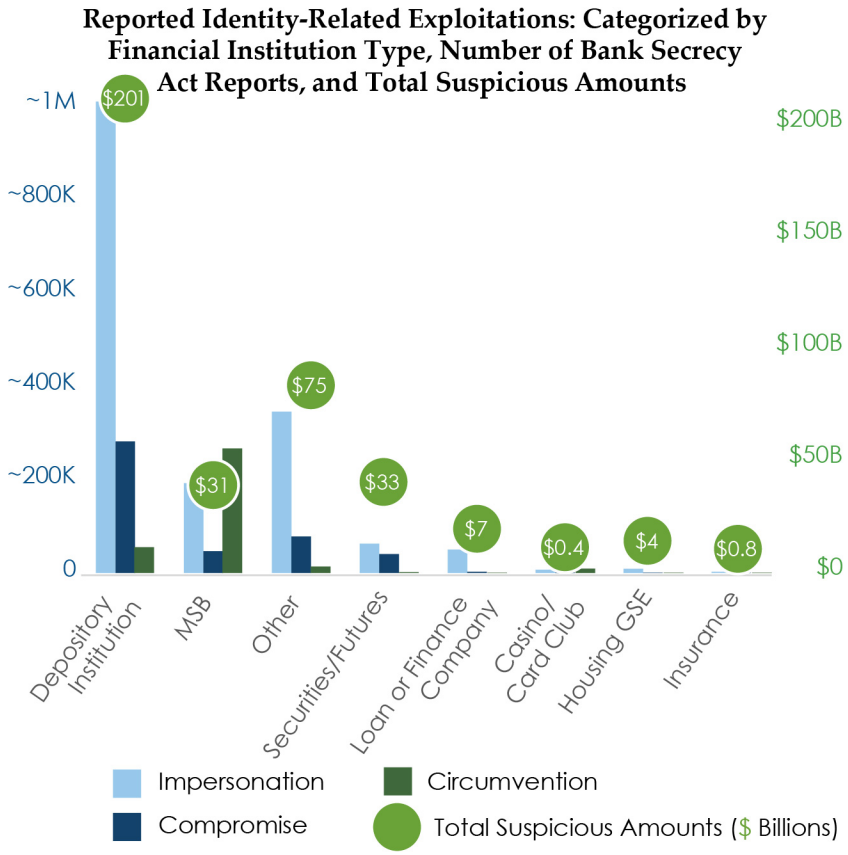
We think that we are onto something with the framework, and we are looking forward to sharing more with you as soon as we can.

We welcome further feedback on the Identity Project framework and Identity Financial Trend Analysis.

Public-Private Partnership

Identity is a network business, and it will take us all working together to mitigate these exploitations to prevent crime.

All types and sizes of institutions are facing these exploitations and, while the impact varies, the challenges are the same (*See figure below*).



Source: FinCEN Identity Financial Trend Analysis, January 9, 2024.
Figure 4 and 5. January to December 2021.

We would like to thank all the members of the Bank Secrecy Act Advisory Group Identity Project Working Group for all their efforts to help us understand the Identity Financial Trend Analysis results.

We appreciate the partnership with the OCC on the Identity Project in particular, for co-hosting this event.

We would also like to thank our federal partners—in particular, the National Institute of Standards and Technology (NIST), the Department of Homeland Security, the Department of Justice, the Pandemic Analytics Center of Excellence (PACE), and our Treasury friends from the Department's Office of Cybersecurity and Critical Infrastructure—for coming here today to highlight their efforts to work with the private sector to buttress existing and emerging digital identity solutions by developing guidelines, converting standards into code, measuring effectiveness, analyzing the data available, and prosecuting the bad guys.

We are also delighted that FinCEN's Identity Project framework was cited in the fraud section of *Finternet*, a working paper published by the Bank of International Settlements (BIS).

Conclusion

In the interim, as we see it, better information around customer identity will support our law enforcement colleagues in investigating suspicious activity, making arrests, successfully prosecuting offenders, and seizing ill-gotten assets.

Transparency around individuals and corporations can bring economic benefits as well, by protecting our financial system, reducing due diligence costs, enabling fair business competition, and increasing tax revenue.

We know success will depend on our partnerships with private industry and other stakeholders.

Financial institutions, in particular, remain crucial in the fight against financial crime and will continue to be key partners on work related to mitigating identity exploitations.

Opportunities exist for emerging technologies, such as digital identity solutions, AI, and privacy enhancing technologies, to help address identity-related exploitations and combat a wide variety of illicit finance typologies.

Through these and all our actions, working with you in the private sector, we are making our country safer and more prosperous, and we are contributing to global security and prosperity.

Thank you for the opportunity to share insights.

###