White Paper

Navigating Synthetic Identity Fraud: Trends, Challenges, and Countermeasures in Banking

Sponsored by: Early Warning

Sean O'Malley Aaron Press
May 2024

EXECUTIVE SUMMARY

Synthetic identity fraud is an emerging fraud risk type that has been perpetuated by fraudsters with such stealth and success that there are few estimates regarding the magnitude of impact for this type of fraud. The range of loss estimates, reflecting the degree of success fraudsters are having with synthetic identity fraud, are in the billions of dollars. The impact estimates range from single-digit billions to double-digit billions, and some experts have even concluded that the precise magnitude of losses due to synthetic identity fraud are unknown at this time.

A survey of financial institutions has been conducted to obtain information regarding their perceptions about synthetic identity fraud. The survey gathered the opinions and perceptions of financial institutions regarding the banking products most associated with synthetic identity fraud, the tools currently being used to combat it, the expectations with respect to future investments to address this emerging fraud risk type, and what types of functionality and capabilities financial institutions will be seeking from those vendor solutions addressing synthetic identify fraud.

METHODOLOGY

This white paper makes several references to survey data collected by IDC on behalf of Early Warning regarding the opinions gathered from bankers regarding synthetic identity fraud. This survey was conducted by gathering responses from 100 individuals working at U.S. banks and credit unions, segmented by asset size and the individual's role with respect to decision-making regarding know-your-customer (KYC) solutions (see Table 1).

TABLE 1

Survey Respondent Demographics

Category	Information
Total respondents	▪ 100
Institution type	▪ **Banks:** 88 ▪ **Credit unions:** 12
Institution asset size	▪ **$30+ billion:** 22 ▪ **$8 billion–30 billion:** 78

Source: IDC's *Early Warning Banking Identity Survey,* December 2023

Key Findings

- 62% of financial institutions surveyed say synthetic identity fraud is increasing.
- Credit cards, deposit accounts, and loans like mortgages, personal loans, auto loans, and home equity loans are the banking products most associated with synthetic identity fraud.
- There are several challenges banks and credit unions face in the process of identifying and remediating synthetic identity fraud including the fact that some "real" information is used in creating these fabricated identities and that consumers whose data is used to create synthetic identities are typically unaware that an account was opened using their information.
- 70% of financial institutions say they are increasing their investment in solutions to prevent synthetic identity fraud.
- There are several pain points commonly associated with vendor solutions designed to address fraud risk including inefficiencies created by too many false positives, having insufficient data to aid in fraud identification, solutions that produce delayed results, and functional challenges from a user perspective.
- The capabilities considered most critical by financial institutions when selecting an identity solution provider include risk scores, risk indicators or flags, and predictive insights.

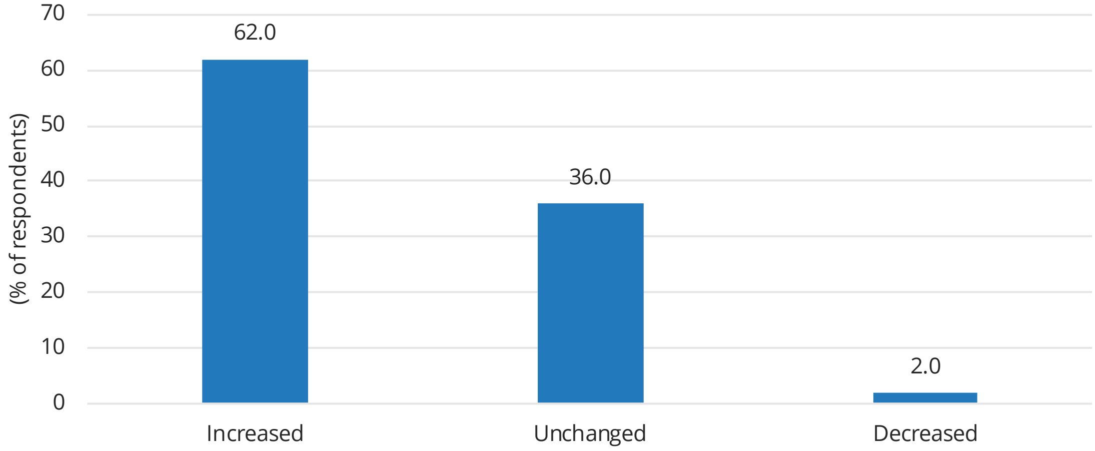
CURRENT STATE OF SYNTHETIC IDENTITY FRAUD

The presence of synthetic identity fraud (using pieces of data from an actual identity combined with pieces of "synthetic" personal data) has become significantly more prevalent in recent years. Some experts believe that this type of fraud has increased in part due to the increased use of "contactless" and remote onboarding of customers in financial services during the recent COVID-19 pandemic. Some experts also believe that the expansion of financial technology companies has helped provide cybersecurity hackers with additional potential sources of customer data for use in perpetrating synthetic identity fraud.

What is clear is that cybersecurity hackers continue to target the acquisition of personal data for use in identity fraud, account takeover, and synthetic identity fraud. The targeting of personally identifiable information (PII) by bad actors is certainly nothing new, but the capability of using such information to open banking accounts using synthetic identity fraud, due to the increased remote account application and onboarding procedures, has created an emerging and increasing risk with respect to synthetic identity fraud (see Figure 1).

FIGURE 1

Change in Synthetic Identity Fraud



n = 100 (all respondents)

Notes:

Data is not weighted.

Use caution when interpreting small sample sizes.

Source: IDC's *Early Warning Banking Identity Survey,* December 2023

To better understand synthetic identity fraud, it's important to understand some of the reasons why fraudsters are interested in opening accounts with a synthetic identity and what types of bank products are most commonly associated with synthetic identity fraud.

One of the most common synthetic identity fraud trends is to create "money mule" accounts. Typically a DDA, these accounts are where the proceeds sent by scam victims are collected. From there, the funds can be sent, often offshore, to the perpetrators of the fraud scam.

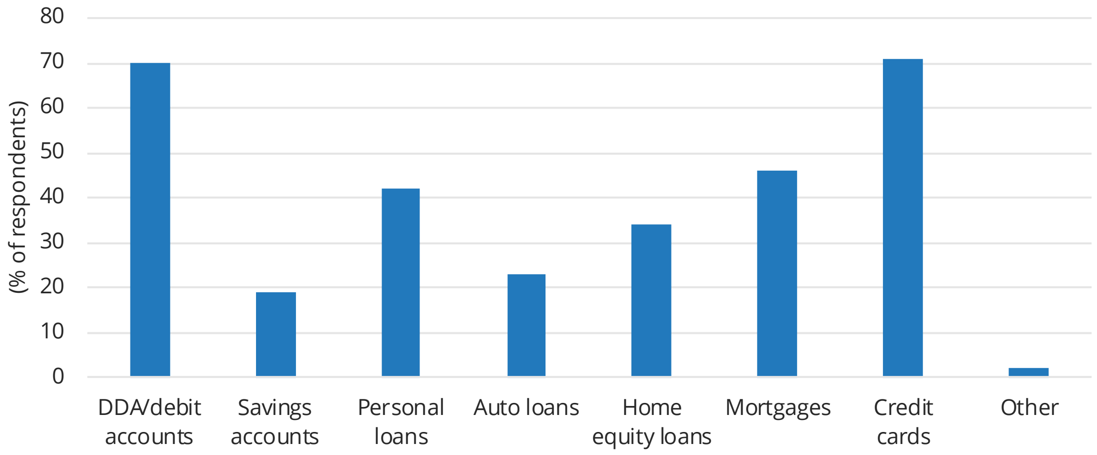
In a similar scenario, an account opened using a synthetic identity will be used to facilitate money laundering. The account is used as a financial funnel, sitting relatively dormant, only to have significant funds from other locations simultaneously transferred into it and then quickly withdrawn (often sent offshore through a large wire transaction).

Particularly insidious, credit or loan fraud is a long-game scam whereby the account is nurtured, often over a period of months or even years. Starting with a nominal amount of credit (either on a credit card or via a loan), the fraudster will make payments, appearing to be a good customer, and receive an increased credit line. When they have expanded their line of credit sufficiently, the fraudster will maximize the value of the account and suddenly stop making payments, vanishing, literally without a trace.

Figure 2 reinforces the reasons for using synthetic identity fraud to open a bank account. The most common products, according to the survey results, are credit cards, direct deposit accounts, and loans (mortgages, personal loans, auto loans, and home equity loans). The types of banking products can be used to facilitate one, or more, of the fraud types described previously.

FIGURE 2

Banking Products Most Used with Synthetic Identity Fraud



n = 100 (all respondents)

Notes:

Data is not weighted.

Use caution when interpreting small sample sizes.

Source: IDC's *Early Warning Banking Identity Survey,* December 2023

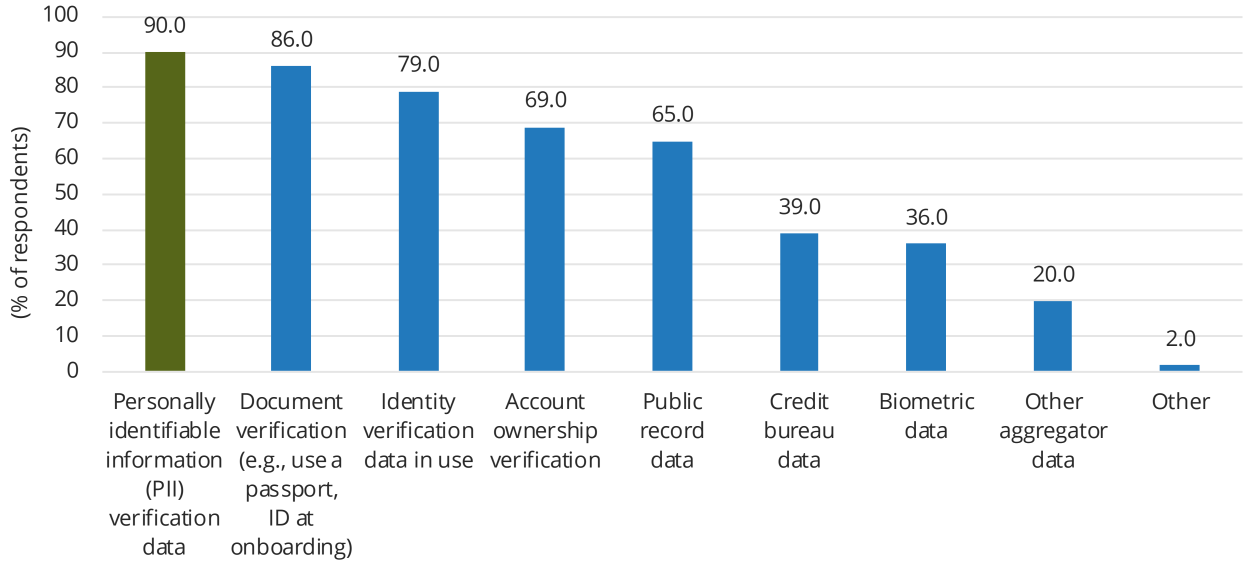
Onboarding and KYC

Know Your Customer, the Customer Identification Program (CIP), and customer onboarding are banking processes that are designed to confirm the identity of the customer seeking an account and verify the information being provided is accurate. Figure 3 illustrates, and ranks, the types of information used during the customer onboarding process, according to the survey respondents.

Figure 3 also illustrates one of the reasons that synthetic identity fraud is both difficult to detect and challenging to remediate. Fraudsters are using some pieces of personally identifiable information, the most common information source referenced during the onboarding process, to create a synthetic identity. Banks are in the unenviable position of trying to confirm an identity that has all of the required data components (some real and some synthetic), as they are trying to confirm the identity of the account applicant – in most cases, without having a complete customer record of the actual person on whom the personal data is based. Synthetic identity fraud is very challenging to detect, both at customer onboarding and through monitoring ongoing transactional activity. Fraudsters rely on having at least some level of success in obtaining bank accounts using synthetic identities. Fraudsters don't need to "win" every time they try to open a bank account with a synthetic identity; they just need to win some of the time. They will disproportionately target those banks where they have a higher level of success in perpetrating synthetic identity fraud. And once a synthetic identity gets traction, and thus an air of legitimacy, detection becomes even harder.

FIGURE 3

Information Types Collected During Onboarding



n = 100 (all respondents)

Notes:

Data is not weighted.

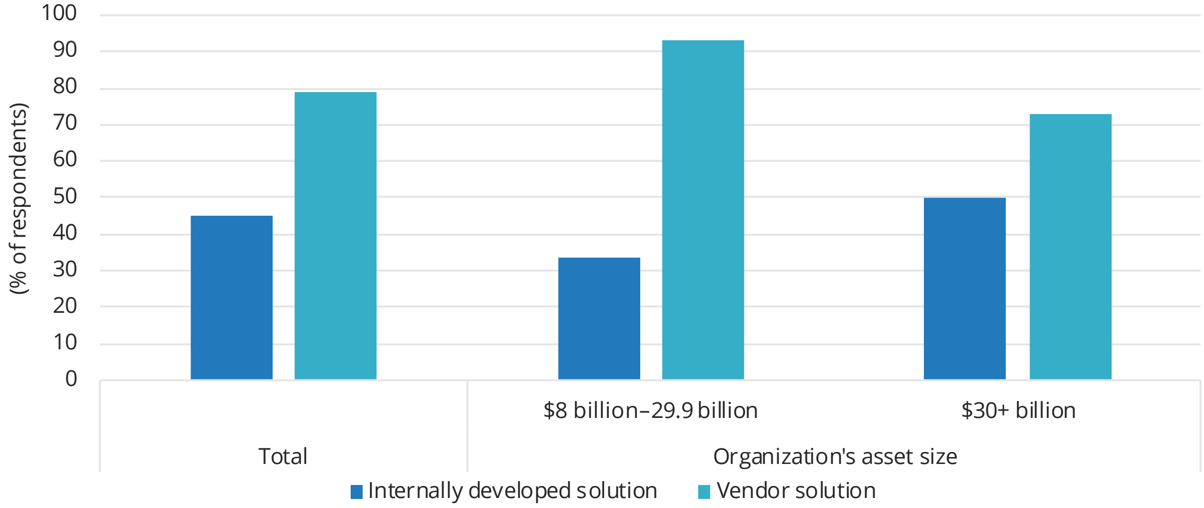
Use caution when interpreting small sample sizes.

Source: IDC's *Early Warning Banking Identity Survey,* December 2023

Figure 4 illustrates the reliance banks have with respect to vendor solutions for Know Your Customer, which will be important to have as reference when viewing some of the other graphs illustrating the use of and investment in vendor solutions dealing with fraud in general and, more specifically, synthetic identity fraud.

FIGURE 4

KYC Solutions



n = 100 (all respondents)

Notes:

Data is not weighted.

Use caution when interpreting small sample sizes.

Source: IDC's *Early Warning Banking Identity Survey,* December 2023

Fraud Types and Fraud Tools

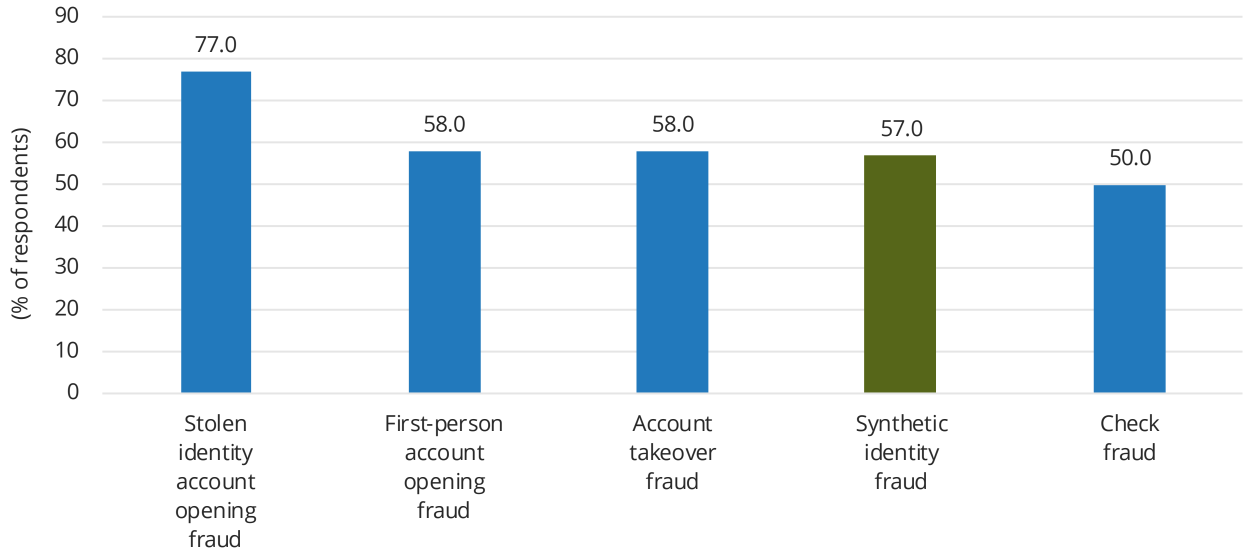
First, let's examine the different fraud types experienced by the survey respondents within the past 12 months. Figure 5 shows the top 4 fraud types that all deal with identity in some way — stolen identity fraud, first-person account opening fraud, account takeover fraud, and synthetic identity fraud.

Two of these fraud types involve an outside party — that is, not the customer, having access or control of their account taken over by the outside party — often by having that outside party obtain control of the account using another individual's personal information to open the account (stolen identity account opening fraud) or using the account information to take over the account. The other two fraud types, first-person account opening fraud and synthetic identity fraud, involve the outside party using personal information to obtain a bank account using the personal data of someone that is not involved in the account opening.

When considering which types of fraud are harder to detect, consider that with first-person account opening fraud and synthetic identity fraud, the person whose information has been used by the fraudster to open the account is unaware that an account has been opened in their name.

FIGURE 5

Fraud Types Experienced in the Past 12 Months



n = 100 (all respondents)

Notes:

Data is not weighted.

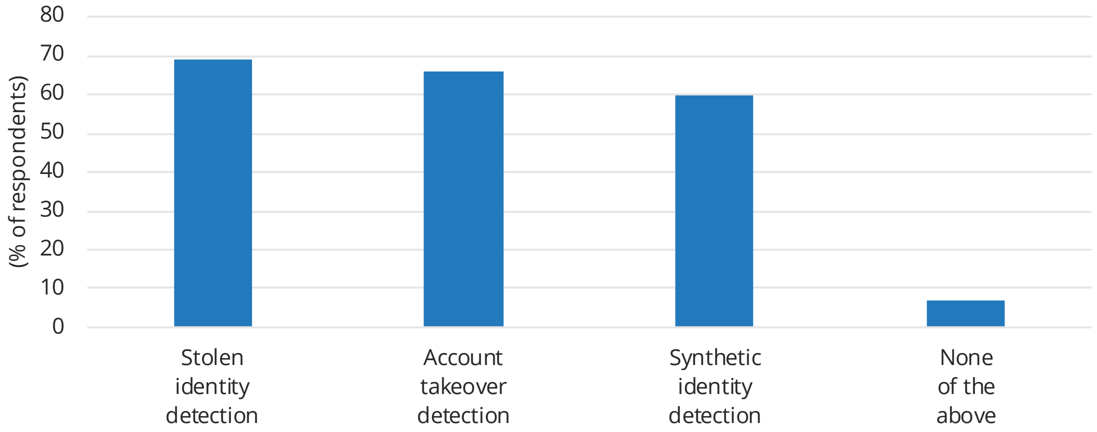
Use caution when interpreting small sample sizes.

Source: IDC's *Early Warning Banking Identity Survey,* December 2023

Looking at the reasons banks are increasing their investment in fraud solutions reinforces the prior analysis regarding fraud types. Figure 6 shows that banks are increasing their investment in fraud solutions to address the risks associated with synthetic identity detection (commonly associated with first-person account opening fraud), account takeover detection, and synthetic identity fraud. Both synthetic identity detection and synthetic identity fraud tie back to those two fraud types that are more challenging to detect because the person whose information has been used by the fraudster to open the account is unaware that an account has been opened in their name or with some of their identity attributes.

FIGURE 6

Fraud Solutions — Investment



n = 100 (all respondents)

Notes:

Data is not weighted.

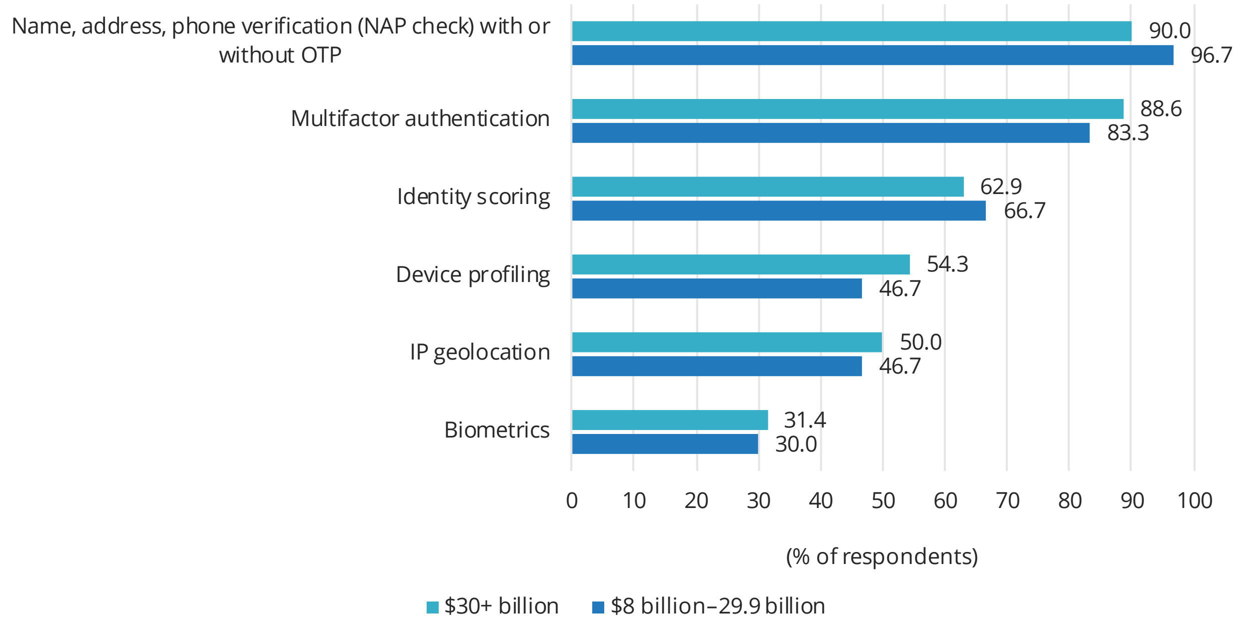
Use caution when interpreting small sample sizes.

Source: IDC's *Early Warning Banking Identity Survey,* December 2023

While the investment in fraud solutions is designed to improve the future capabilities of banks to combat fraud, some of the current set of tools being used to combat fraud are based largely on existing access controls (name/address/phone verification, multifactor authentication, device profiling, IP geolocation, and biometrics) or customer risk scoring tools (identity scoring) that are repurposed in efforts to identify or prevent synthetic identity fraud. Figure 7 shows which fraud prevention tools are identified by survey respondents as those most commonly used in fraud prevention at this time.

FIGURE 7

Identity Fraud Prevention Tools



n = 100 (all respondents)

Notes:

Data is not weighted.

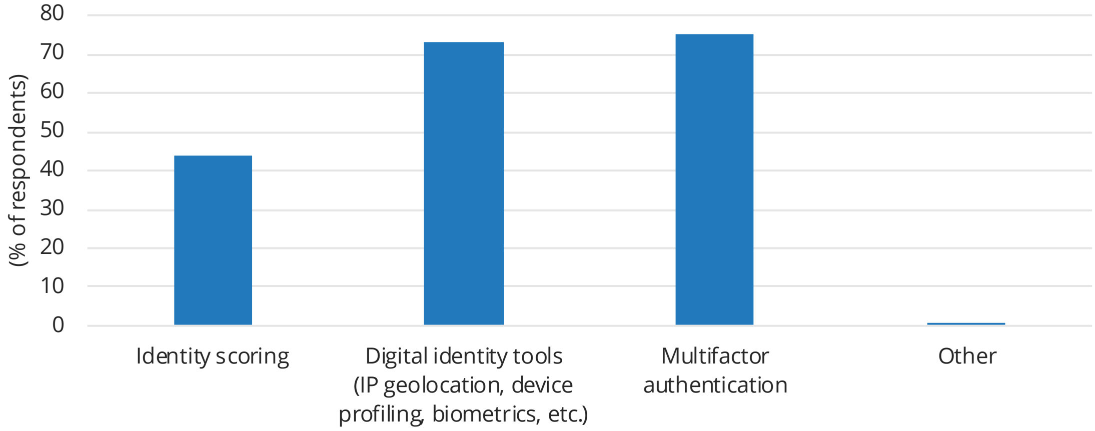
Use caution when interpreting small sample sizes.

Source: IDC's *Early Warning Banking Identity Survey,* December 2023

The set of tools from Figure 7 that survey respondents considered to be the most effective at combating synthetic identity fraud are illustrated in Figure 8. It should not be surprising that the top 3 identity fraud prevention tools currently in use are also considered the top 3 most effective tools at combating synthetic identity fraud at this time. Given that these tools, techniques, and technologies were adapted for use in trying to combat synthetic identity fraud reflects the gap with respect to new tools, techniques, and technologies designed to address the increasing risk associated with synthetic identity fraud.

FIGURE 8

Effective Tools Against Synthetic Identity Fraud



n = 100 (all respondents)

Notes:

Data is not weighted.

Use caution when interpreting small sample sizes.

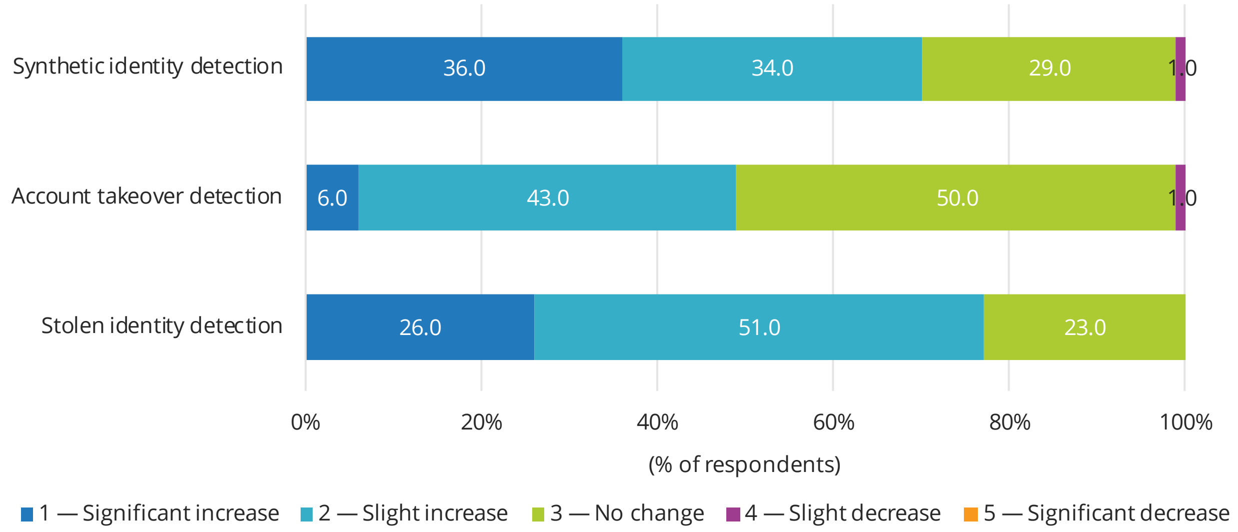
Source: IDC's *Early Warning Banking Identity Survey,* December 2023

Finally, let's look at what banks are saying with respect to their level of investment with respect to detection and prevention of synthetic identity fraud. Figure 9 illustrates that, for most institutions, the investment in synthetic identity fraud solutions will be increasing (with 36% of all institutions indicating a significant increase in investment, and 34% indicating a slight increase in investment).

It's also important to note that, among the institutions indicating plans to significantly increase in their synthetic identity fraud investment, 40% are larger institutions. As it is often common for larger institutions to lead smaller institutions in terms of their investments, this shift could indicate that the proportion of institutions expecting to increase spending with respect to synthetic identity fraud could further increase in the future, as more smaller banks follow the lead of their larger counterparts. Smaller institutions also often have more significant budgetary and resource constraints than larger institutions, which can have an impact on spending, leading to fewer smaller institutions increasing investments to address synthetic identity fraud.

FIGURE 9

Change in Investment for Synthetic Identity Fraud



n = 100 (all respondents)

Notes:

Data is not weighted.

Use caution when interpreting small sample sizes.

Source: IDC's *Early Warning Banking Identity Survey,* December 2023

CHALLENGES

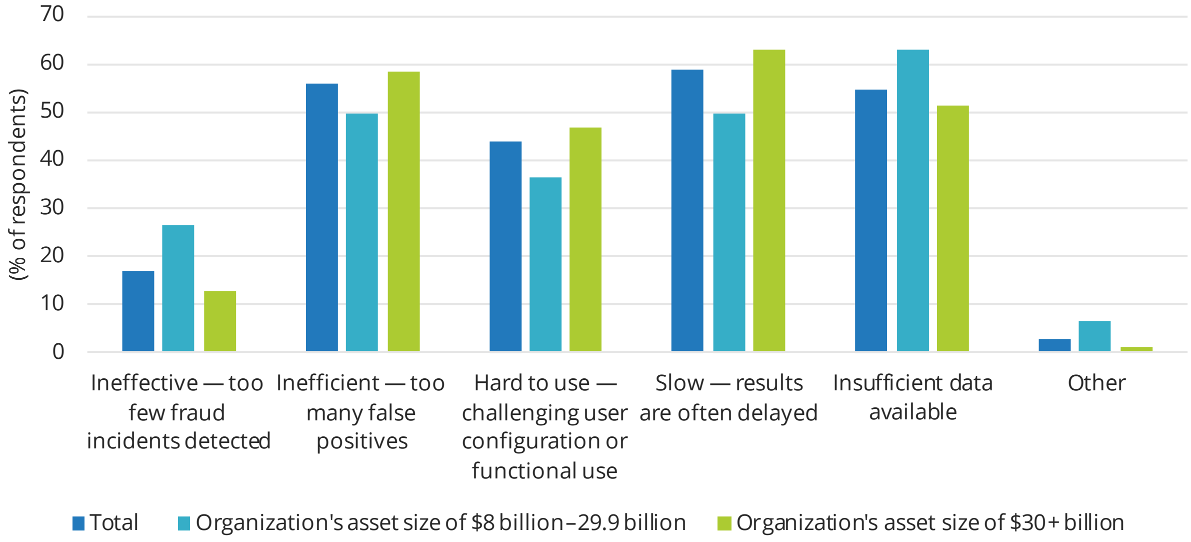
Some of the challenges with respect to identifying and remediating synthetic identity fraud have already been mentioned — the difficulty in identifying synthetic identity fraud due to the use of some "real" personal data, and the challenges in detection because any customer whose personal information is used in opening an account via synthetic identity fraud is largely unaware that any account was opened using their personal data.

But there are also other challenges, which we refer to as "pain points" (see Figure 10), with respect to existing fraud solutions. Several of these pain points are operational in nature, such as the critique that existing fraud solutions are inefficient because they produce too many false positives. That is a very common complaint with many solutions, not only in fraud but across financial crime compliance. The number of false-positive alerts generated can be very frustrating to analyze, very expensive to process, and very unproductive. It's important for each institution to find the right balance between the expense and operational burden of alerts generated, and the benefit of finding "true hits."

Other pain points include having insufficient data to aid in the appropriate identification of fraud, fraud solutions or processes that produce delayed results (increasingly fraud is trying to be addressed in real time, or as close to near time as possible), and fraud solutions that are functionally challenging from the user perspective.

FIGURE 10

Pain Points with Current Fraud Detection



n = 100 (all respondents)

Notes:

Data is not weighted.

Use caution when interpreting small sample sizes.

Source: IDC's *Early Warning Banking Identity Survey,* December 2023

The industry is already well along the path of working to mitigate many of these issues. Adapting tools and methods from AML and transaction fraud management solutions, banks are finding success with better anomaly detection by leveraging additional signals, beyond identity attributes, such as device profiling and behavioral biometrics. And one key to managing the additional data is the application of machine learning to build and maintain models that are more predictive and less prone to false positives. In addition, the industry is increasingly looking to artificial intelligence (AI), both traditional and generative. This technology can be harnessed to make human review faster and more accurate by highlighting issues with suspicious customers or transactions, locating additional relevant data, and recommending follow-up actions.

CONCLUSION

Looking back at the results of the survey, several things are clear.

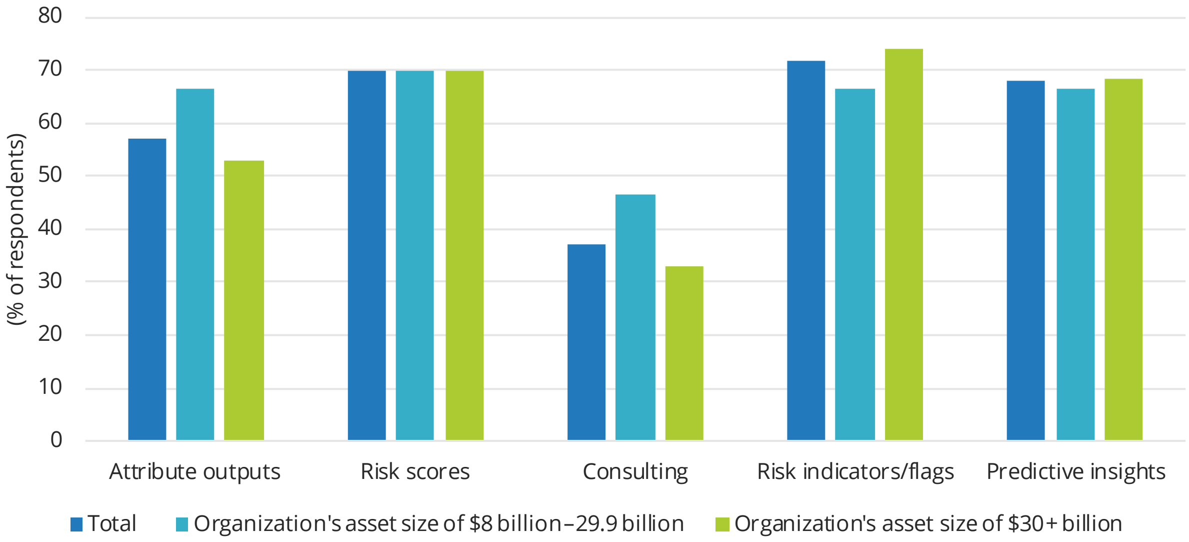
The majority of financial institutions surveyed indicate synthetic fraud is increasing and that credit cards, deposit accounts, and loans are the banking products most associated with synthetic identity fraud. There are several challenges in the process of identifying and remediating synthetic identity fraud including the fact that some "real" information is used in creating these fabricated identities and that consumers whose data is used to create synthetic identities are typically unaware that an account was opened using their information.

As banks and credit unions look for ways to confront these challenges, investment in addressing synthetic identity fraud is expected to increase. There are several pain points commonly associated with vendor solutions designed to address fraud risk including inefficiencies created by too many false positives, having insufficient data to aid in fraud identification, solutions that produce delayed results, and functional challenges from a user perspective.

The survey results seem to indicate that there is a need for a vendor solution to address synthetic identity fraud based on new tools, techniques, and/or technologies. This raises the logical question regarding the capabilities that financial institutions will prioritize in considering an identity solution provider. Figure 11 illustrates those capabilities considered most critical by the survey respondents regarding what they want from an identity solution provider including risk scores, risk indicators or flags, and predictive insights.

FIGURE 11

Critical Capabilities When Selecting an Identity Solution Provider



n = 100 (all respondents)

Notes:

Data is not weighted.

Use caution when interpreting small sample sizes.

Source: IDC's *Early Warning Banking Identity Survey,* December 2023

As we look forward to solutions that can effectively meet these needs and address existing pain points, it's apparent there is a need for identity solutions that can provide financial institutions with real-time insights that give them a full view of a potential customer's risk profile and help them predict the likelihood of a synthetic identity. By using existing solutions like PII cross-checks to validate a consumer's identity with accuracy and using machine learning and/or AI to further augment this data and provide enhanced risk evaluations, financial institutions will hopefully be able to get ahead of synthetic identity fraud in the first place.

The solution provider that is best able to address the issues with the emerging synthetic identity fraud trends, meet the challenges identified in the pain points, and possess the critical capabilities sought by financial institutions will have the best chance of success as a leading synthetic identity fraud vendor.

MESSAGE FROM THE SPONSOR

About Verify Identity from Early Warning

Verify Identity leverages data from thousands of financial institutions to provide a more reliable and timely assessment of an applicant's identity credentials. The service combines predictive scoring with rules-based solutions to determine the likelihood that an applicant truly is who they claim to be. When you incorporate Verify Identity insights into your digital application process, you can make more confident consumer assessments, while complying with banking regulations.

Early Warning Services, LLC, a financial services technology leader, has been empowering and protecting consumers, small businesses, and the U.S. financial services ecosystem with cutting-edge fraud and payment solutions for more than three decades. Through unmatched network intelligence and partnerships with more than 2,500 bank and credit union brands, we increase access to financial services and products, and protect financial transactions. To learn more about Early Warning, visit www.earlywarning.com.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.