WAKEFIELD

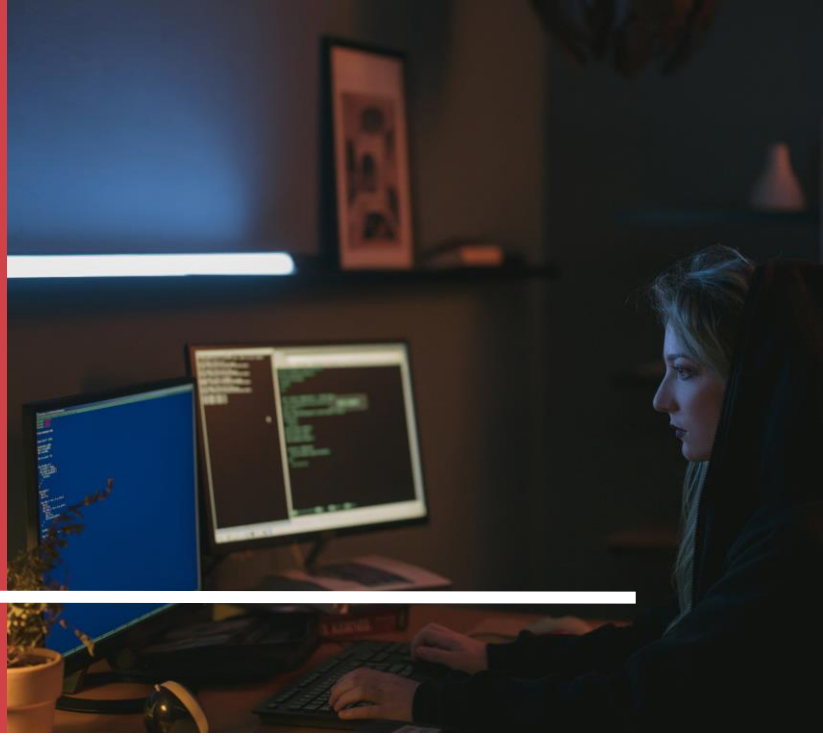
Financial Jeopardy: Companies Losing Fight Against Synthetic Fraud

October 2023

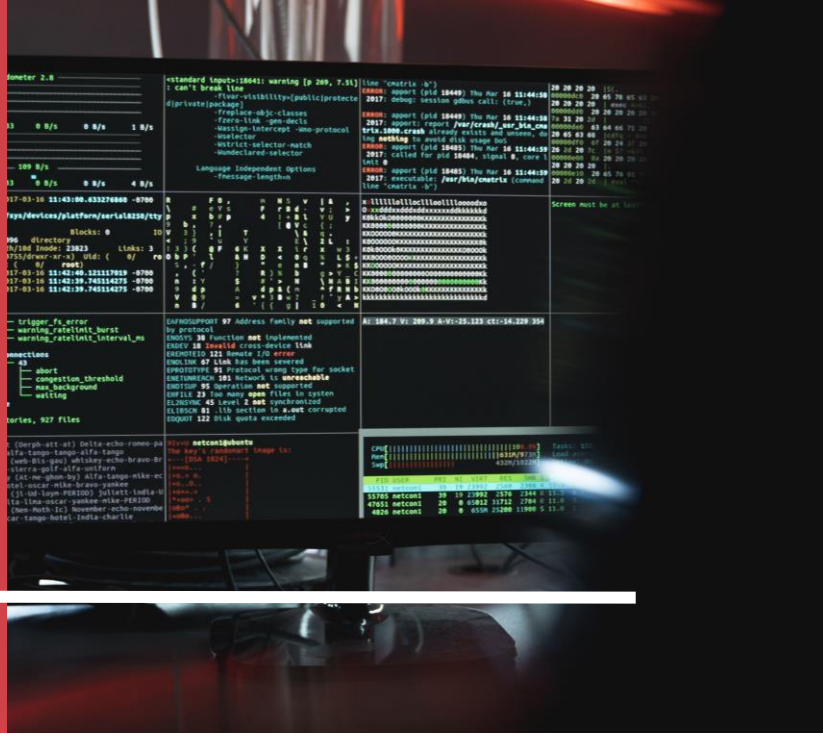
Sponsored by

DEDUCE

Table of Contents



Executive Summary



Synthetic identity fraud's growth is accelerating and financial services and fintech companies are struggling in their efforts to control the threat, to great consequences. **A survey of 500 U.S. fraud and risk professionals with a minimum seniority of manager reveals that for half (50%) their company's synthetic fraud prevention is at best only somewhat effective.** And the ramifications of having inadequate protection are severe: 87% of companies have extended credit to synthetic customers and 1 in 5 (20%) estimate the average monetary loss per incident is between $50K and $100K, while nearly a quarter (23%) put it at more than $100K per incident.

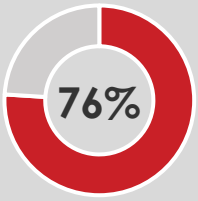
And the inevitability of fraudsters increasing their use of generative AI to raise their schemes' sophistication to unprecedented levels promises to make matters worse. Fraudsters are already becoming more inclined to nurture their accounts over a longer period of time for larger financial gain. The ability of fraud prevention departments to verify accounts will be put to the test as the activity patterns and behaviors even more closely mimic those of legitimate customers.

Companies cannot continue to absorb these losses as the cost of doing business because it will eventually put them at a competitive disadvantage and consumers who may not feel directly impacted by synthetic fraud will ultimately pay the price.

In this report from Deduce, in partnership with Wakefield Research, we detail the prevalence of synthetic fraud, the behaviors of the fraudsters, the impact on companies, and their preparedness for evolving threats.

Key Findings

Synthetic Fraud Surge



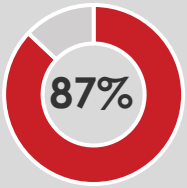
believe their organization already approved accounts for synthetic customers

have synthetic fraud prevention solutions in place

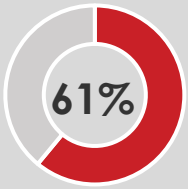
report synthetic fraud has increased in the last 24 months, and on average, by 17%

report their company's synthetic fraud prevention is at best only somewhat effective

Making a Real Impact



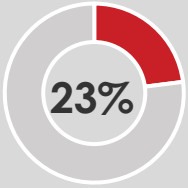
of organizations have extended credit to synthetic customers



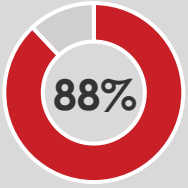
offered credit without customers first applying for it

among those who extended credit to synthetic customers

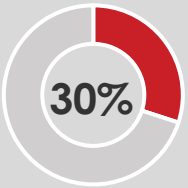
report the average loss per incident of synthetic fraud is between $50K and $100K



place synthetic fraud at $100K or more per incident



agree that AI-generated fraud will get worse before solutions are devised to effectively prevent it



strongly agree that it will get worse before it gets better

Protection Against Synthetic Fraud Failing

Businesses in the financial and banking sectors are under siege from fraudsters blending stolen data such as Social Security numbers, names, and addresses with fabricated data to create new identities. These phony personas are then frequently avoiding detection during the verification processes, leaving the companies vulnerable. In fact, half of fraud and risk professionals at U.S. financial services and fintech companies (50%) report synthetic fraud prevention in their organization is only somewhat effective or worse.

50% of fraud and risk professionals report synthetic fraud prevention in their organization is only somewhat effective or worse

Higher level employees are more likely to be optimistic about their company's ability to weed out the bad actors. Nearly 3 in 5 C-suite or high-level executives (57%) report synthetic fraud prevention is mostly or completely effective at their company. Yet, a minority of director or mid-level employees (46%) agree.

Without the need for advanced technical savvy and presenting minimal risk of an individual victim reporting the issue, criminals can execute synthetic fraud at scale -- and the pool of potential targets is virtually limitless. Fraud and risk professionals place the increase of synthetic fraud at an average of 17% in the last 24 months with 36% of the professionals reporting an increase of 20% to less than 50%.

Synthetic fraud has become the fastest-growing financial crime despite 100% of companies having verification protocols in place for new accounts, which undoubtedly is leaving higher-level executives concerned about how best to mitigate the risk. More than 2 in 5 C-level or high-level execs (44%) say the increase has been 20% to less than 50%, compared to 31% of director or mid-level professionals.

Younger businesses have seen a greater increase in synthetic fraud over the last 24 months, as nearly half of those in business less than 25 years (46%) have seen an increase between 20% to less than 50%, compared to 25% of those in business 25 years or more. Yet this may be as much of an indicator of awareness as it is a measure of incidents.

As it stands, 40% of those who believe their organization currently has synthetic customers report the synthetic fraud increase is between 20% and 50% in the last 24 months compared to 26% of those who do not think they have synthetic customers.

The challenge for businesses, however, is enormous. A shocking 76% of fraud and risk pros believe their organization has accounts that are synthetic customers. Upon closer examination of those findings, banking and finance companies are bearing slightly more of the brunt of the breaches. More than 4 in 5 of those who work in banking/finance believe their company has synthetic customers (82%), compared to 71% of those who work in financial technology. 18% of those who work in banking/finance say they definitely do, compared to 9% of those who work in financial technology.

Spotlight: Inconspicuous Behavior

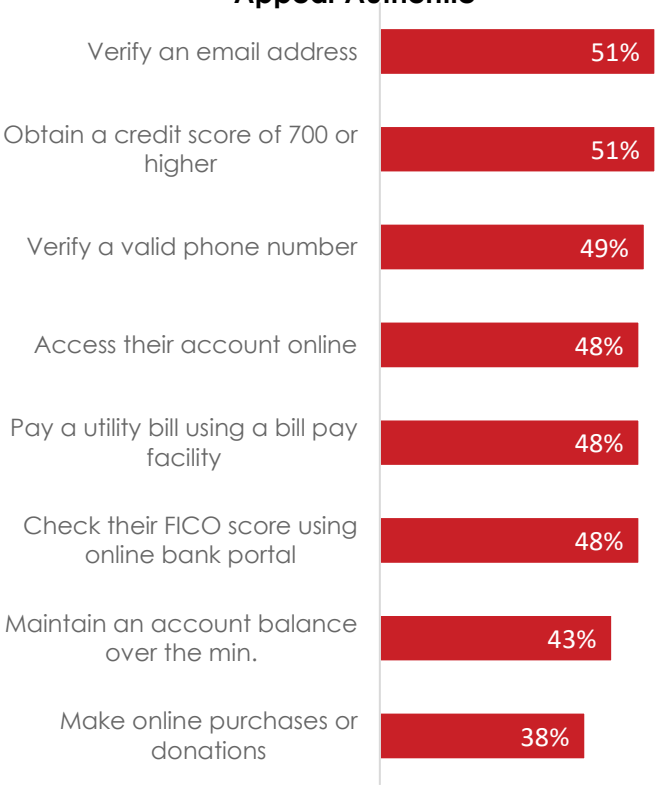
Scrutiny is the enemy of fraudsters. Their goal is to fly under the radar of financial institutions' verification processes, lull them into a false sense of security by building a credible credit history through common financial activity, and now often lying patiently in wait for months on end to bust out with all they can.

About half of fraud and risk professionals have seen the bad actors take the following actions in their synthetic accounts in an attempt to appear real – verify an email address (51%), obtain a credit score of 700 or higher (51%), verify a valid phone number (49%), access their account online (48%), pay a utility bill using a bill pay facility (48%), and check their FICO score using the company's online banking portal (48%). Other common actions observed include maintaining an account balance over the minimum (43%) and making online purchases or donations (38%).

The majority of those who believe their organization currently has synthetic fraud accounts as customers have seen accounts verify phone numbers (52%) and more than 2 in 5 have seen them make online purchases or donations (41%).

Those who do not believe they currently have synthetic fraud accounts as customers are significantly less likely to have seen fraudsters verifying phone numbers (42%) and making online purchases or donations (31%).

Have Seen Synthetic Accounts Do the Following to Appear Authentic



Paying the Price for Vulnerability

An astounding 87% of organizations have extended credit to synthetic customers. While it is not uncommon for financial companies to extend credit through a marketing campaign or promotion, it is troubling that of organizations who have extended credit to a synthetic customer, 62% say they did so after receiving an application, while 61% offered the credit to the fraudster without needing an application.

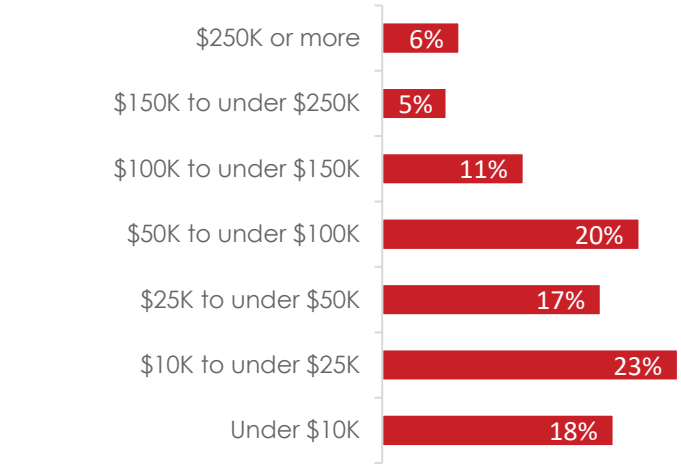
With the inevitability of technological innovation continuing to fuel an already combustible situation, financial institutions have even more reason to be concerned about essentially giving away money. Among those who believe fraudsters are outpacing security measures, nearly 3 in 5 say their company offered the credit (59%), compared to 46% of those who say security measures are getting better more quickly.

And the executives most responsible for ensuring the company hits its financial goals are notably more likely to recognize when they've been scammed. The majority of C-suite or high-level executives' companies (63%) have extended credit when the synthetic customer applied for it, compared to 49% of director or mid-level professionals' companies.

Compounding the problem for the financial institutions, synthetic customers are more inclined to patiently play the long game for higher payouts rather than cashing out after getting the smaller initial offers of credit. Many companies are left to hopelessly attempt to collect from customers that don't exist before writing off the losses.

One in 5 fraud and risk pros (20%) report the average monetary loss per synthetic fraud incident is between $50K and $100K, and almost a quarter (23%) say it is $100K or more.

Average Monetary Loss Per Incident of Synthetic Fraud



Interestingly, there is a significant difference among company leadership about the toll synthetic customers are exacting. About 1 in 8 C-suite or high-level executives (12%) report the average loss per synthetic fraud incident is between $50K and $100K and 17% say $100K or more, compared to 24% of director or mid-level professionals who say between $50K and $100K and 27% who say $100K or more.

And bigger companies are more frequently facing greater consequences. A third of those at companies with 500 employees or more (33%) report the average loss per incident of synthetic fraud is between $50K and $100K with 29% putting it at $100K or more. Compare that to about 1 in 7 of those at companies with under 500 employees (14%) who put the loss per incident between $50K and $100K and 20% have it at $100K or more.

Generally, the more established companies have suffered the bigger financial hit with 31% of those who have been in business 25 years or more reporting losses between $50K and $100K per incident, compared to 11% of those in business less than 25 years.

About a third of those who say the industry is not prepared for synthetic fraud report the loss per incident is $100K or more (32%), compared to 20% of those who say the industry is prepared.

Spotlight: Reality Check

Companies' synthetic fraud prevention solutions and approaches must strike a balance between keeping the bad actors out of the system and not compromising service of legitimate customers. Many companies are relying on traditional methods, which unfortunately are proving to be no longer practical nor effective – particularly if not part of a multi-layered verification approach.

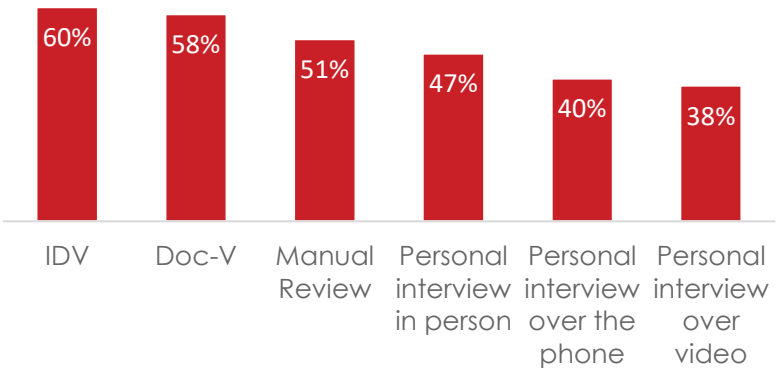
An overwhelming 85% of financial organizations use personal interviews to verify new account holders, including in-person interviews (47%), over the phone (40%), and video conference (38%); and more than half (51%) are doing a manual review. A vast majority (75%) are using ID or document verification, with 60% using IDV and 58% using Dov-V.

Older companies are significantly more likely to want to meet their potential customers. Nearly 3 in 5 companies that have been in business 25 years or more do in-person interviews (58%), compared to 38% of those that have been in business less than 25 years.

On the other hand, the newer companies are more inclined to rely on technology to get to know their customers as 45% of them utilize video conference interviews, compared to 29% of the older companies.

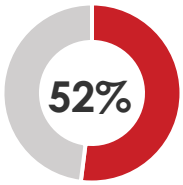
The labor-intensive manual review process remains a key component of the verification process but is becoming increasingly difficult to execute as the deluge of data rapidly grows. More than 3 in 5 of those who do not believe they have synthetic customers use manual reviews (62%), compared to 47% of those who think they have synthetic customers.

Verification Requirements Organizations Have for Reviewing New Financial Accounts



Evolving Threat of Generative AI

Bound by no rules, synthetic customers are only limited by their creativity in coming up with technology-driven schemes to defraud financial institutions. It's not surprising that more than half of fraud and risk professionals report the bad actors' abilities to evade synthetic fraud detection are getting better more quicky (52%), compared to 48% who say security measures to detect synthetic fraud are making more gains.



Fraud and risk professionals report fraudsters' ability to evade synthetic fraud detection is getting better more quickly

The prospect of fraudsters leveraging AI more broadly to fabricate even more robust credit profiles is unsettling. A staggering 88% of fraud and risk pros agree that AI-generated fraud will get worse before solutions are devised to effectively prevent it, including 30% who strongly agree. If that scenario plays out, financial institutions will need to take a more comprehensive approach to analysis of data instead of relying on more narrow insights.

Those closer to the struggle are more likely to see their company losing ground in its efforts to curb synthetic fraud. More than a third of director or mid-level professionals (35%) strongly agree that AI-generated fraud will get worse before solutions are devised to effectively prevent it, compared to 23% of C-suite or high-level executives. Leadership falling behind in the utilization of technology would be a virtual invitation for these fraudsters to embed themselves among legitimate customers and wreak havoc for the foreseeable future.

Younger companies, in particular, have a dim view of the near-term. More than a third (35%) of those whose company has been in business less than 25 years strongly agree that AI-generated fraud will get worse before solutions are devised to effectively prevent it, compared to 25% of those whose company has been in business 25 years or more.

Despite the undisputed havoc synthetic fraud is heaping upon financial institutions, and security measures that are proving ineffective, fraud and risk professionals believe they are equipped to meet the next enormous threat. More than 3 in 4 (76%) think the financial services industry is prepared for AI-generated synthetic fraud, including 15% who think it is very prepared. Yet in spite of this, perhaps, overly optimistic view of readiness, fraud and risk professionals know it will not be immediate. Even among those who believe the industry is prepared, 87% agree AI-generated fraud will get worse before they can establish effective solutions to prevent it. More importantly, no one knows how long financial institutions can endure the big-time breaches or how much AI-generated fraud will disrupt the industry.

Conclusion

Financial services and fintech companies are under relentless assault from synthetic identity fraudsters, wielding generative AI technology and utilizing an increasingly sophisticated approach to cheating the industry out of billions of dollars. Companies can't afford to continue to use legacy technology and techniques as they are largely proving ineffective at detecting the new breed of synthetic identities that demonstrate typical account activity such as obtaining high credit scores, paying bills online, or making online purchases. These accounts are looking more like those of legitimate customers with each passing day.

Not only are companies losing money as a result of not having cutting-edge synthetic identity fraud prevention and identity verification solutions, they also are risking damage to their invaluable brand and falling behind their competition. Furthermore, if they seek to offset the financial impact of synthetic identity fraud by imposing higher rates or fees for their services, or adding unnecessary friction during account creation processes, customers may go elsewhere.

With AI-generated synthetic fraud threatening to raise the stakes, companies need to be prepared for a tough road ahead, as even those in the industry who think they are ready to battle this new threat believe it is going to get worse before there are signs of improvement. A layered approach to synthetic identity fraud should be considered to address this new threat.

Methodological Notes

The Deduce Survey was conducted by Wakefield Research (www.wakefieldresearch.com) among 500 US Fraud and Risk professionals, with a minimum seniority of manager, at financial services and FinTech companies, between September 5th and September 17th, 2023, using an email invitation and an online survey. Includes a company requirement that the company extends credit, for example in the form of personal loans, credit cards, etc. Excludes mortgages.

Results of any sample are subject to sampling variation. The magnitude of the variation is measurable and is affected by the number of interviews and the level of the percentages expressing the results. For the interviews conducted in this particular study, the chances are 95 in 100 that a survey result does not vary, plus or minus, by more than 4.4 percentage points from the result that would be obtained if interviews had been conducted with all persons in the universe represented by the sample.

Thank You

About Wakefield Research

Wakefield Research is a leading, independent provider of quantitative, qualitative, and hybrid market research and market intelligence. Wakefield Research supports the world's most prominent brands and agencies, including 50 of the Fortune 100, in 90 countries. Our work is regularly featured in media.

WakefieldResearch.com