# How to Thwart Fast-Changing Fraud Workflows

*Combining AI and biometrics-based authentication to reduce fraud team burdens*

opusresearch

opusresearch | Report »

# How to Thwart Fast-Changing Fraud Workflows

*Combining AI and biometrics-based authentication to reduce fraud team burdens*

**The post-pandemic world has become a playground for identity thieves who make their living by exploiting security vulnerabilities in businesses. To help withstand the threat of fraudsters, organizations should employ holistic authentication and fraud detection solutions to simultaneously streamline authentication, strengthen security, and free up employees to focus on more-valuable work. The strongest defense against fraud is in applying both biometrics and AI in ways that build trust between companies and their customers while minimizing burdens on contact center agents and fraud investigators.**

June 2021

**Dan Miller,** Lead Analyst & Founder, Opus Research

**Opus Research, Inc.**
**893 Hague Ave.**
**Saint Paul, MN 55104**

www.opusresearch.net

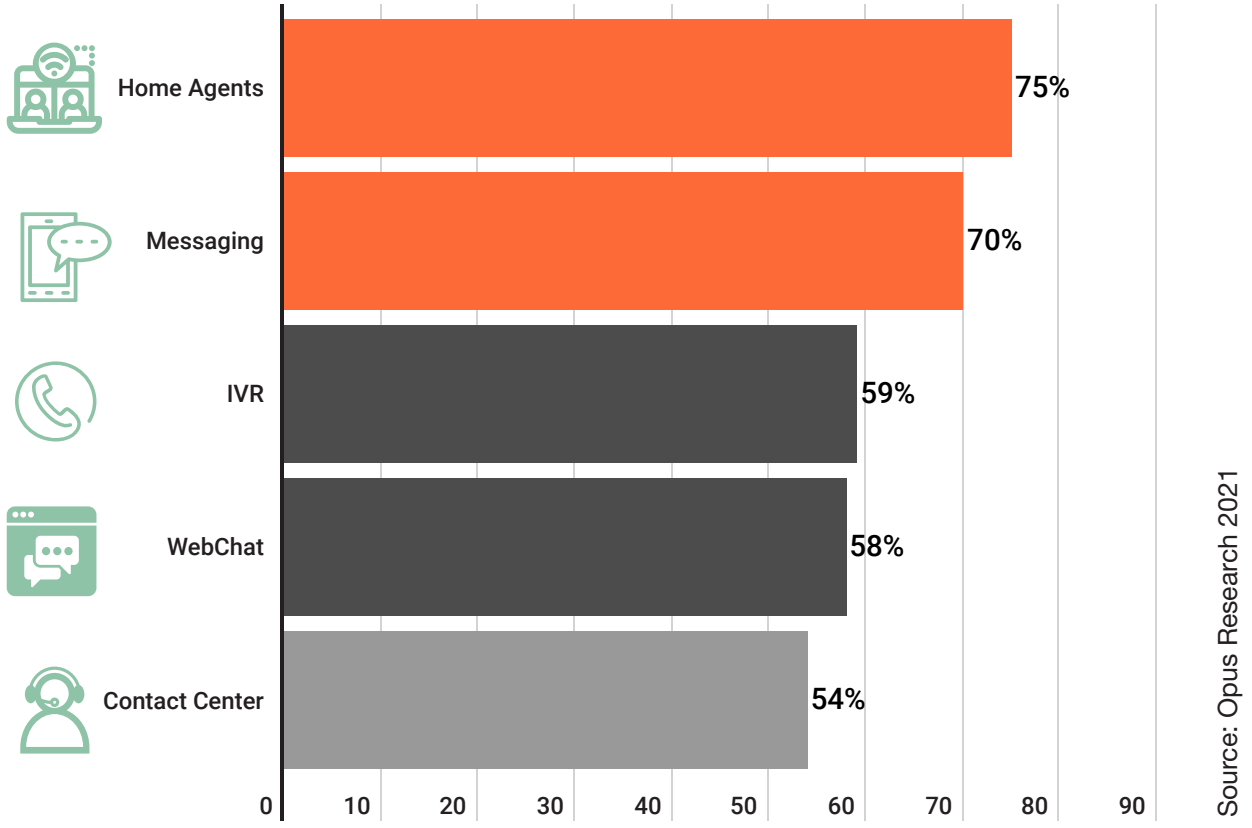
### Research Reflects Dramatic Changes in the Nature of Consumer Fraud

The post-pandemic world has become a playground for identity thieves and others who make their living by stealing customer data, taking over accounts, and committing other forms of fraud. The pandemic has also accelerated a migration of customer service representatives from secure, brick-and-mortar contact centers into work-from-home (WFH) environments. Separately, these trends demand action; together, they create an imperative for companies to modernize their authentication and fraud prevention strategies.

The "State of Intelligent Authentication and Fraud Prevention 2021" survey conducted by Opus Research reveals security and authentication trends in customer engagement channels and how organizations are responding.

According to the survey, organizations report a significant increase in Covid-driven fraud in every channel.

## Figure 1: Organizations Reporting Increased Fraud (By Channel)




As illustrated in Figure 1, survey respondents report significant increase in Covid-driven fraud activity by channel. This phenomenon spans all channels; but an increase among "work from home agents" is the most-frequently cited cause for concern (75%). Fraud conducted through messaging platforms shows similar growth, reflecting the increased importance of this channel in the digital age. Webchat and contact centers also see growth, which indicates fraudsters still mostly focus on channels where they can exploit human vulnerability and manipulate employees.

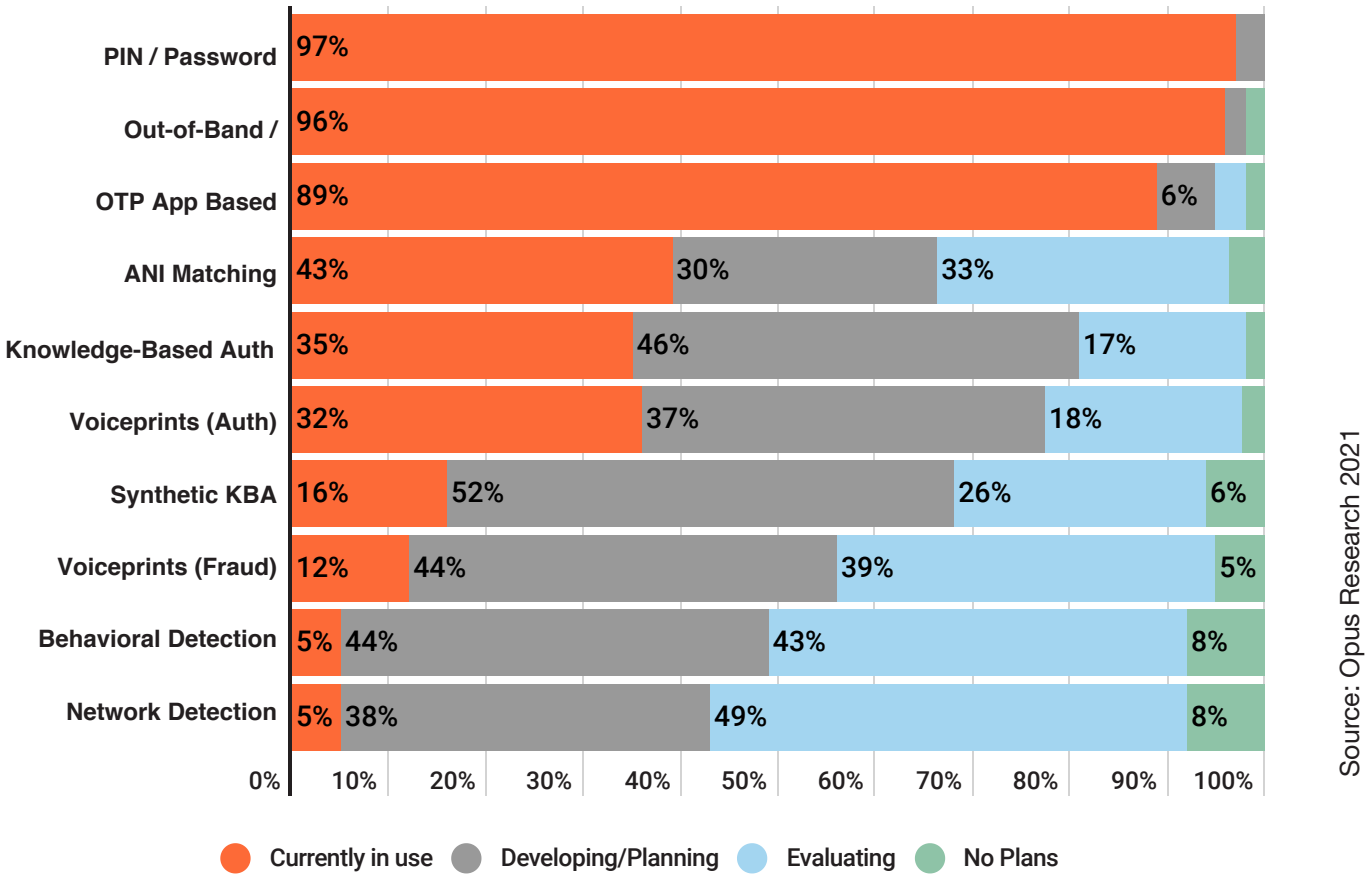
It's no surprise, then, that 88% of respondents say they plan to accelerate spending on security and authentication strategies in 2021.

### The Explicit Link Between Authentication and Fraud-Loss Prevention

In a separate question, 92% of respondents agreed or strongly agreed with the statement, "Work-from-home agents have created security concerns for our customer service operations." Respondents were even more certain that "customer authentication [across all channels] has a direct impact on fraud detection and fraud prevention," with a rare 100% of respondents agreeing or strongly agreeing with the statement. Clearly, decision-makers are coming around to acknowledging the link between strong authentication and fraud-loss prevention.

When asked about which authentication and fraud detection methods they use, organizations report a wide range of strategies and factors (Figure 2, below).

## Figure 2: Enterprises Employee Multiple Authentication Factors




Source: Opus Research 2021

As Figure 2 shows, survey respondents tend to mix-and-match a set of authentication and fraud prevention methods. PINs/Passwords are still the most common factor in use, but respondents also incorporate other factors including ANI-matching, out-of-band delivery of one-time-passwords, and knowledge-based

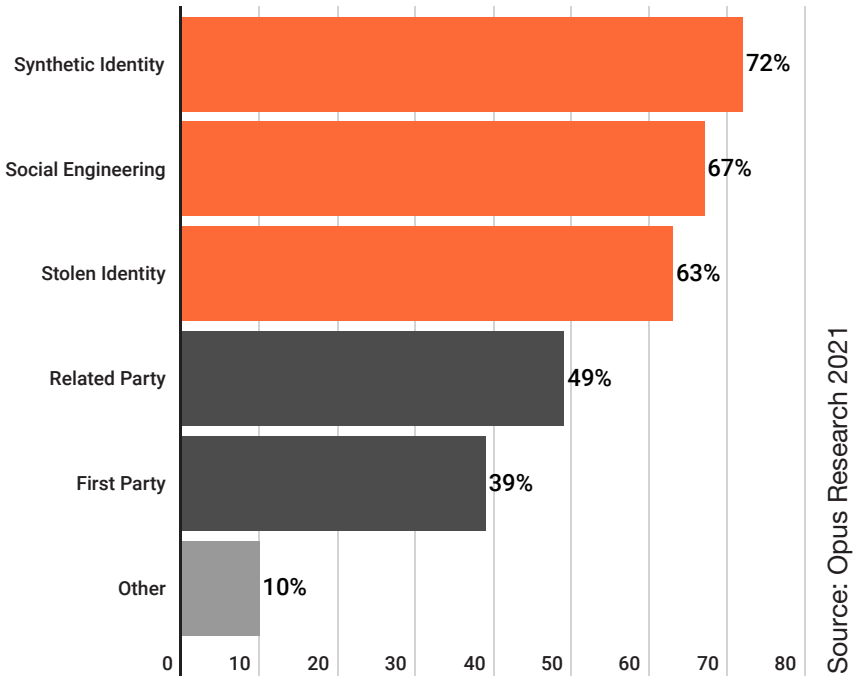
authentication via security questions. Particularly worth noting is that a growing number are adopting voice biometrics and behavioral biometrics solutions. Voice biometrics analyze everything that goes into creating a person's unique voice signature, including physical factors such as vocal tract and mouth structures, and speech delivery elements such as speed, pronunciation, and emphasis. "Behavioral biometrics" analyze the unique way each user interacts with a device, such as the way you type with a keyboard or hold a mobile device. These advanced biometrics deliver authentication that is both faster and more secure than traditional methods by verifying people based on who they are, rather than something they know or something they have.

All told, the average respondent is employing 5 different techniques for customer authentication. But with so many competing factors in play, companies are overwhelming their fraud departments with false alerts. Therefore, companies should look to deploy holistic authentication solutions that cut down on false alerts and help fraud teams improve their workflows.

### Life Mirrors Research

Empirical observations validate the story that emerges from the Opus Research survey. Respondents were also asked which fraud attack types create the highest perceived security threat. "Synthetic identity fraud" (SIF) is the most frequently cited attack vector of concern in the survey, with 72% of respondents reporting an increase in SIF (Figure 3).

## Figure 3: Highest Perceived Security Threats (By Fraud Attack)




SIF involves creating an entirely fabricated identity to defraud companies of services and benefits. A fraudster might create a synthetic identity by using fake customer or worker ID numbers, then taking an action that compels a company to perform a credit check (e.g. opening a new account over the phone). Even though the first check will return "no hit" as a response from a credit bureau, it creates an entry. Over time, through further credit inquiries, the fraudster builds enough credibility to start receiving "thin file" responses on their synthetic identity. Eventually, its credit score reaches a point where its file, once queried, returns the same results as a legitimate credit file. The door is open for the fraudster to create new accounts, obtain services, open lines of credit, and so on.

SIF is a practice that takes time and is performed over several channels. Fraud detection platforms that look for dozens or hundreds of calls into an IVR originating from the same number can programmatically flag that number as a probable fraudster. But such an approach is destined to failure because synthetic identity fraudsters will take ownership of a phone number for each identity he or she is curating. By employing multiple burner phones or pre-paid SIM cards they can avoid detection in the IVR, making biometrics the only fraud prevention method to stop synthetic ID crimes.

The second most-cited form of increased fraud is "social engineering" whereby a fraudster cajoles customer information directly from an individual. Social engineering is carried out through conversations during which a fraudster "charms" a contact center agent to provide information on legitimate customers; this enables the fraudster to "fill in the blanks" and eventually take over an account. This may occur over time and through multiple interactions, or through a single conversation.

Of course, activity alone does not equate to successful creation of a false identity or completion of an account takeover. But automated detection, flagging, and blocking of activity by known fraudsters is a giant step toward eliminating fraud loss with a minimum of human intervention.

Very little fraud takes place during a session with an IVR, for instance. Yet repeated calls from a single number into an IVR signals that a fraudster is in the reconnaissance stage of his or her efforts to take over an account. Their next step might be to reach out to an agent to re-route a package or update personal information. Artificial intelligence (AI) and machine learning (ML) can be used to detect suspicious these call patterns and flag suspected fraudsters. But even that solution may be transitory because fraudsters will change their calling method, leveraging easy-to-use tools online, using burner phones or SIM boxes; or they will simply find a way to get straight to a human agent to socially engineer.

This is why organizations should always focus on where the "real" losses are happening. Trying to prevent account testing in the IVR is missing the point, because fraudsters will always find a way to talk to an agent to perform the high-value transactions that lead to material losses. But by deploying voice authentication in the IVR, organizations can detect the fraudster in real time and thwart their efforts to reach a live agent.

When deployed intelligently, the combination of AI and biometrics-based authentication stops fraud losses while actually reducing false positives, easing the burden on fraud teams.

## All Solutions Must Take the Human Dimension into Account

Authentication and anti-fraud systems come under attack and scrutiny from many angles. Fraudsters approach them head-on as they attempt to take over accounts or funnel goods and funds their way; legitimate customers find cumbersome authentication techniques to be time-consuming nuisances and attempt to avoid or get through them as fast as possible; and agents find authentication procedures like challenge questions to be a burdensome waste of time and often undermine them by "coaching" callers.

As a result, the investigators that make up a “Fraud Team” are central to detection and assessment of possible fraud loss, yet high false positive rates and mountains of manual reviews force them to devote their valuable time to busywork.

Consider that every successful fraud attack is the result of a series of activities that took place over time, involving a number of channels and touchpoints. Therefore, anti-fraud technologies must help fraud teams gain an accurate understanding of where theft actually takes place and what activities and attacks led up to it.

Therefore, organizations should employ holistic, unified authentication and fraud solutions to simultaneously streamline authentication, strengthen security, and free up employees to focus on more-valuable work, like helping customers, building an accurate picture of a company’s exposure to fraud, and ascertaining what activity by which individuals leads to the greatest loss..

Based on our research and reinforced by empirical observation, a primary benefit of the holistic approach is in protecting a business and its employees against social engineering. This means focusing less on low-value automated tests in the IVR and more on where high-value transactions take place: with human agents or within conversational IVRs that allow complex requests. By making holistic risk assessments that factor in high-fidelity signals like voice biometrics, organizations can increase security and trust while minimizing agent involvement in authentication activities. This approach also reduces false alerts, thereby easing the burden on fraud teams and freeing them to concentrate on investigating the events and activities that result in actual fraud loss.

## The Benefits of a Holistic, Biometrics-first Approach

Fraudsters, contact center agents and fraud investigators each have separate but inter-dependent workflows. The best fraud prevention solutions take them all into account with special attention to agent experience and fraud investigation.

Fraudsters are continuously evolving and adapting their strategies and workflows. Fraud teams that base their detection on comparison to a “normal” customer interaction are already a step behind, because fraudsters don’t follow “normal” flows. There’s little value in adding more locks on the front door if fraudsters can still just enter through a back door.

What’s more, there is great risk in believing that a combination of 24/7 monitoring and application of “black-box AI” will enable you to “predict” fraud with certainty. Detecting and preventing fraud where it actually occurs relies on a holistic, biometrics-first approach that takes into account the human dimensions at the root of fraud risk, agent productivity, and investigator efficiency. It also coincides with an expanded awareness of the areas where Fraud teams and Customer Experience teams share common goals.

In short, the strongest defense against fraud is in applying both biometrics and AI in ways that build trust between companies and their customers while minimizing burdens on contact center agents and fraud investigators.

Distilled into simple rules, organizations deploying anti-fraud technologies must take the human dimension into account by:

- **Deploying a unique solution that allows for global visibility on fraudsters' journey: from the web, to the IVR – conversational or not – to the agent**
- **Helping manage the fraud team's workflow by building cases around fraudsters instead of transactions or abstract behavior**
- **Reducing employee exposure to social engineering by intercepting and deflecting fraudulent calls even before they reach an agent**
- **Detecting and stopping repeat fraudsters by building a watchlist of suspicious behavior patterns, compromised ANIs, and unique biometric prints**
- **Using biometrics to tie multiple cases and losses back to the individual behind them**
- **Respecting the workflows of the fraud team by taking a proactive approach to early detection and watch-listing of potential fraudsters**

Following these rules enable fraud investigators to build cases around the actual fraudster, instead of around transactions or abstract behaviors. This in turn helps fraud teams manage their workflows by reducing false positives as well as by tracing groups of cases and losses back to the individual person behind them. In this way, biometrics-based fraud solutions can be used to take the fraud efforts beyond simple loss mitigation. With biometrics, fraud analysts disrupt fraudsters' business models and help build cases for law enforcement to bring fraudsters to justice.

A holistic, biometrics-at-the-core approach also allows teams to expand their focus beyond external threats by leveraging the same technology to monitor and protect against internal fraud. This is especially relevant in the context of work-from-home, where agents lack the traditional structures of supervision and support that scaffolded them in the physical contact center environment. Biometrics can be used to continuously monitor remote employees for suspicious or anomalous behavior, or to check that they haven't handed their workstation off to someone else. Using biometrics for customer authentication also helps organizations reduce their exposure to data leakage by eliminating the need to display personally identifiable information to agents in the first place.

## Checklist: What to Ask your Solution Provider

- Are you offering a point solution or taking a holistic approach?
- Do you offer more than just authentication/fraud solutions (a broader technology stack)?
- Can you be a partner in modernization of our CX platform, via conversation IVRs, virtual assistants, chatbots, etc.?
- How do you support/improve upon our current practices in the contact center and fraud investigation operations?
- Do you have fraud experts with field experience in house, or do you just focus on authentication and try to repurpose that technology?
- How do you enlist assistance from fraud investigation teams? Is there courseware and are there tools provided to enlist their participation?
- Can you facilitate change management across multiple channels and use cases?
- Do your experts have first-hand experience and working knowledge of fraud prevention?
- Do you have direct understanding of relevant legislation, regulation and guidelines, as well as vertical industry strictures?
- Can you share a reference customer in my region you successfully accompanied through the deployment of a biometrics solution?

## About Opus Research

Opus Research is a diversified advisory and analysis firm providing critical insight on software and services that support digital transformation. Opus Research is focused on the merging of intelligent assistance, NLU, machine learning, conversational AI, conversational intelligence, intelligent authentication, service automation and digital commerce. www.opusresearch.net

**For sales inquires please e-mail info@opusresearch.net or call +1(415) 904-7666**