ADAPTIVE AI

A Proactive Strategy for Stopping Scam and Fraud Calls

A HIYA PROTECT FEATURE OVERVIEW FOR CARRIERS

It’s time to outsmart – and stop – scammers NOW

While an age-old problem, scam call campaigns are still making global headlines because of the impact cybercriminals manage to achieve through fraudulent financial transactions or the capture of confidential personal information.

Make no mistake, scamming is a lucrative business. European officials recently arrested members of an organized crime group that reportedly defrauded victims around the world via fake investment opportunities that generated more than $3 million per month.

Criminals have perfected the art of scamming, plaguing the voice network with high-reward campaigns that are cheap to operate and easy to run anonymously. Data published in the Hiya State of the Call 2022 report shows the impact that scammers had in 2021 in six countries resulted in:

- An estimated 117 billion scam and fraud calls
- An average of 14 scam and fraud calls per month per user
- An average loss of $542 for the 25% of targets that became victims

Financial impact of spam and fraud calls in 2021

United States
80.1B total spam and fraud calls
18 per user per month
$567.41 average loss per victim

France
12.4B total spam and fraud calls
21 per user per month
$289.27 average loss per victim

Canada
3.1B total spam and fraud calls
6 per user per month
$804.69 average loss per victim

Germany
5.9B total spam and fraud calls
6 per user per month
$273.81 average loss per victim

United Kingdom
6.6B total spam and fraud calls
12 per user per month
$680.17 average loss per victim

Spain
8.9B total spam and fraud calls
20 per user per month
$423.16 average loss per victim

Never underestimate a scammer

Scammers are successful because they operate highly profitable businesses based on techniques that are low in risk, investment, and cost. They easily cross global borders to find the most vulnerable targets through high-volume scams, like the **Wangiri** campaign that netted billions in fraud charges.

The best scammers have deep pockets and can invest in the research, testing, and development of proven, highly sophisticated techniques and how they work on various populations. The scammers ensure success and elude capture by continuously and aggressively changing campaign tactics. When the results of one start to fade, no problem – they just move on to another.

As an example of their sophistication, scammers figured out that **Norwegians** tend to return their calls more than people in neighboring countries, which most likely has led to a higher hit rate and more fraud in Norway.

Scammers often impersonate or spoof legitimate businesses, such as banks, government agencies, or other recognizable organizations, coaxing unsuspecting people to give them personal identity or financial information. The menu of scamming topics is broad, with auto warranties, IRS payments, and student loans as the hot ones in the United States.

We have seen scammers change scripts, target groups, originating carriers, or originating phone numbers – all within minutes. They also may call from a person's area code, or a neighboring one, to see the effect on pickup rates. Recordings and scripts often change to measure the impact of the changes on call duration.

Change Targets

- **Geography**
- **Demography**

Change Appearance

- **Originating Carrier**
- **Originating Number**

Change Approach

- **Script Variations**
- **Robocall vs Human**

Scammers think they still have the upper hand

Global governments, security organizations, and technology companies have been developing new regulations, guidance, and tools to stop scammers, but they are still eluding detection and hard to capture.

- **STIR/SHAKEN**, the framework designed by the Federal Communications Commission (FCC) to reduce robocalls by verifying the digital signature of the outbound call, is a good example. The volume of scam calls went down after the implementation of this framework in mid-2021, but the impact was short-lived and the volume is on the rise again as scammers have figured a way around it. STIR/SHAKEN has been effective in combating the spoofing of mobile numbers. However, scammers can employ other robocall tactics in their attempts to defraud consumers, making people wary of answering a call unless they know exactly who is calling.
- **Reactive number-based programs**, or static phone number tracking, help to stop scammers, but these too are only moderately effective. These programs require extensive programming and depend on probability models based on a snapshot of historical data. This means they are quickly outdated and can't keep up with emerging scam techniques.

Who do the consumers and businesses blame? The carriers.

The FCC's top consumer tip in regards to unwanted robocalls and phone scams is simply to not answer calls from unwanted numbers. And this is what people are now doing, as our research indicates that:

- **94% of people think unidentified calls are fraudulent**
- **Only 20% of unidentified calls are answered**

While not answering the phone helps your consumer subscribers, unfortunately, this means your legitimate business customers can't reach their valued customers. In fact, 50% of the businesses we recently surveyed reported that they lost a customer or a deal by not being able to reach them by phone.

only 42% **of consumers globally think their carrier is currently doing enough to reduce scam and fraud calls**

Adaptive AI can now outsmart the best scammers

There is finally a way to stop and block scammers in real-time with call protection that has up to a 90% effective rate – and it was developed first here at Hiya.

Adaptive Artificial Intelligence (AI) is a critical feature of Hiya Protect. Unlike any other capability on the market today, Adaptive AI is powered by machine learning (ML) that proactively hunts and shuts down scam campaigns using both historical and tactical call intelligence. With the ability to stay ahead of scammers, Adaptive AI works in real-time, without the need for human intervention or any updating of existing AI models.

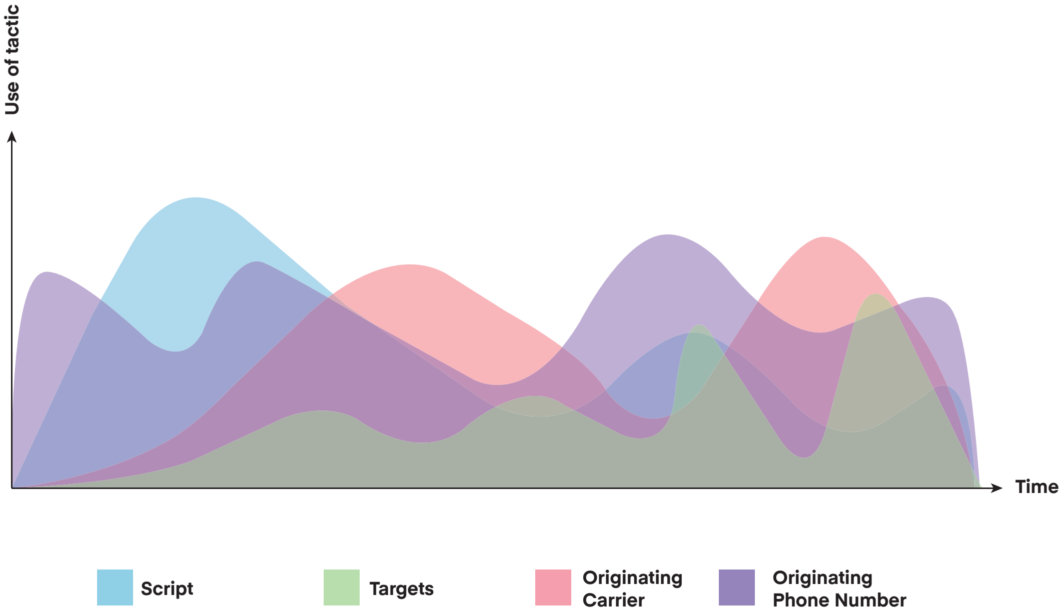
Spammers move fast. We move faster.

Here is a quick look at how the self-learning, real-time Adaptive AI capability works in conjunction with other Hiya technology and services.

1. **Known scammer tactics.** Adaptive AI starts with a risk profile based on the latest known scammer campaign tactics that include the carriers used, network signals, how established the caller is, and the targeted demographics. It even covers basic tactics like the time of day a call is placed, like during lunch or dinnertime. Hiya's dedicated Data Science team is continuously monitoring these tactics to ensure Adaptive AI is prepared for anything.
2. **Real-time data.** Adaptive AI is also informed by live data streams from wireless carriers, smartphone devices, and apps. It evaluates every call in real-time to look for new emerging patterns of scammers. It looks at details including the originating carrier and its reputation based on past user complaints, the country where the call originated, and if the network signature indicates scam risk.
3. **Learned patterns.** Adaptive AI has the unique ability to recognize the underlying patterns in call volumes, call durations, answer rates, user reports, network signals, and much more. It observes and shifts to react to changes in the patterns left by scammers in the network traffic.

4. **Real-time detection and blockage.** After Adaptive AI detects scam calls, it can block them without any human intervention and reduce scam risks in real-time. For instance, through Hiya's automated real-time process, network calls can be terminated by the carrier or pushed to voicemail before they reach customers' phones. For individual users, Hiya blocks the calls through a real-time auto-decline.

Adaptive AI in Real-Time Action



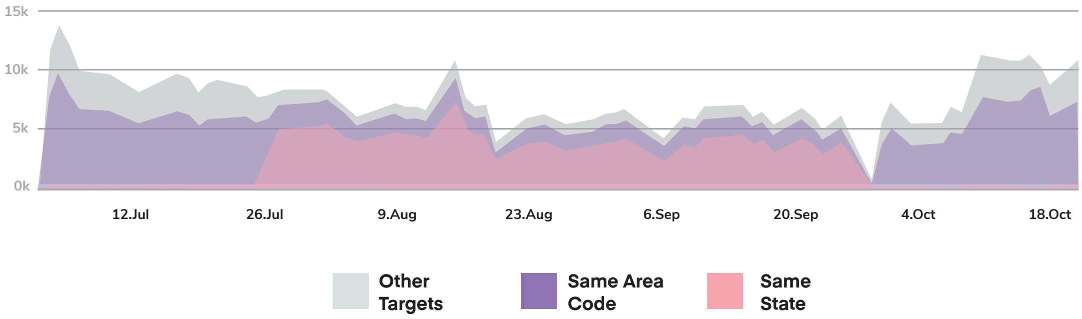
As tactics change, so does Adaptive AI

Hiya's Adaptive AI is designed to detect different types of tactics, as evidenced by its capability to detect the various maneuvers used in the recent car warranty scam that has been rampant in the United States. Over a three-month period, we observed robocallers change tactics several times as they tried to evade detection. However, Adaptive AI was able to detect their tactical moves in real-time and stop 90% of the calls.

Below are the various sets of changing tactics we discovered in the car warranty campaign thanks to Adaptive AI.

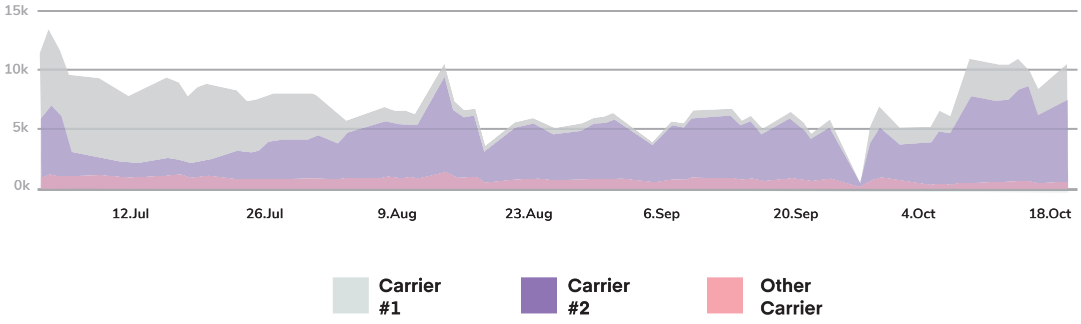
Changing area codes – during the campaign, robocallers changed their area codes from the recipients to other area codes within the same state.

Targeting

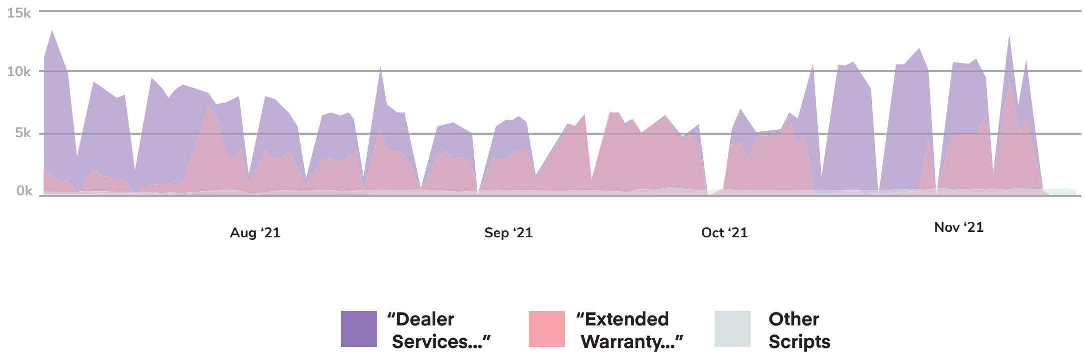


Swapping carriers – the robocallers also changed the VOIP carriers they used throughout the period studied.

Carriers



Swapping scripts – the robocallers tested two main scripts that they modified with minor changes or delivered in different voices.



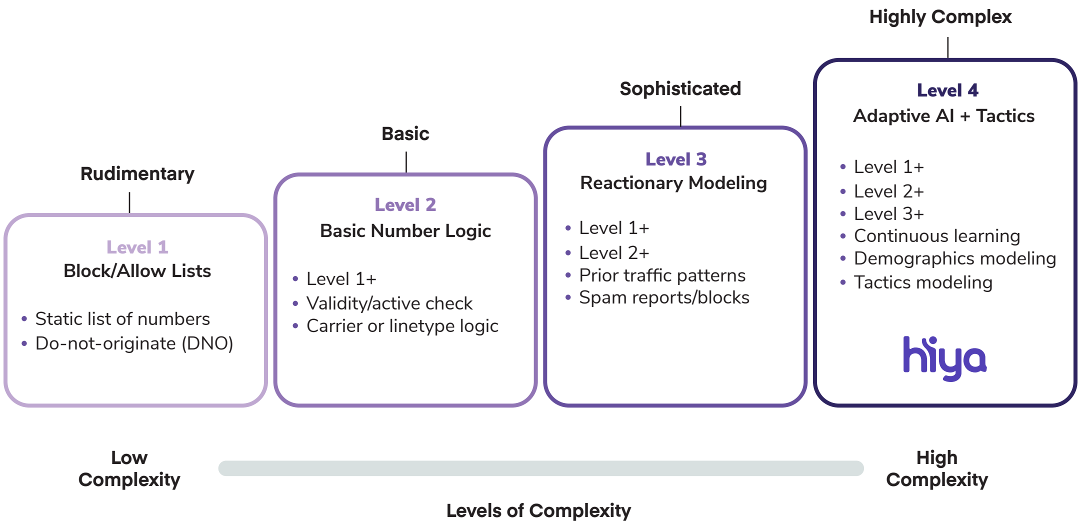
Script

Adaptive AI analyzed each of these shifts as they happened, adjusting the call protection model based on the changes in order to block the calls in real-time.

Adaptive AI versus reactive calling

As a highly advanced solution, Adaptive AI can identify and block new scams, often long before a reactionary modeling system or basic call protection tool even becomes aware of the threat. In fact, Hiya Protect can detect 20% more scam calls than the reactive number-based technologies currently on the market, even if scammers change their phone numbers, carriers, call paths, or other tactics.

Hiya Protect versus other call protection offerings



Rudimentary

Level 1
Block/Allow Lists

- Static list of numbers
- Do-not-originate (DNO)

Basic

Level 2
Basic Number Logic

- Level 1+
- Validity/active check
- Carrier or linetype logic

Sophisticated

Level 3
Reactionary Modeling

- Level 1+
- Level 2+
- Prior traffic patterns
- Spam reports/blocks

Highly Complex

Level 4
Adaptive AI + Tactics

- Level 1+
- Level 2+
- Level 3+
- Continuous learning
- Demographics modeling
- Tactics modeling

Conclusion

Scammers constantly change who they target, how they appear in the network, and their approach. Static systems only track the reputation status of phone numbers. Adaptive systems with capabilities like those in Hiya Protect can also track campaigns and tactics.

With Adaptive AI, we help carriers get one step ahead of scammers, so you can start to rebuild trust in consumers and help your legitimate business customers reach their customers again.

Adaptive AI is just one element of **Hiya Protect**, Hiya's voice performance platform provides the following benefits to carriers, OEMs, and network providers:

Filters or blocks for unwanted and illegal spam calls from reaching end customers.

Identification of wanted calls to end customers.

Improved customer satisfaction with the provider network or communication service.

Proof of carrier anti-spam initiatives for customers, regulators, and internal stakeholders.

To learn more about how Adaptive AI works with carriers, **send us an email**.