Tethr®

The rise of fraudbots

Understanding chat fraud and how AI can overcome it.

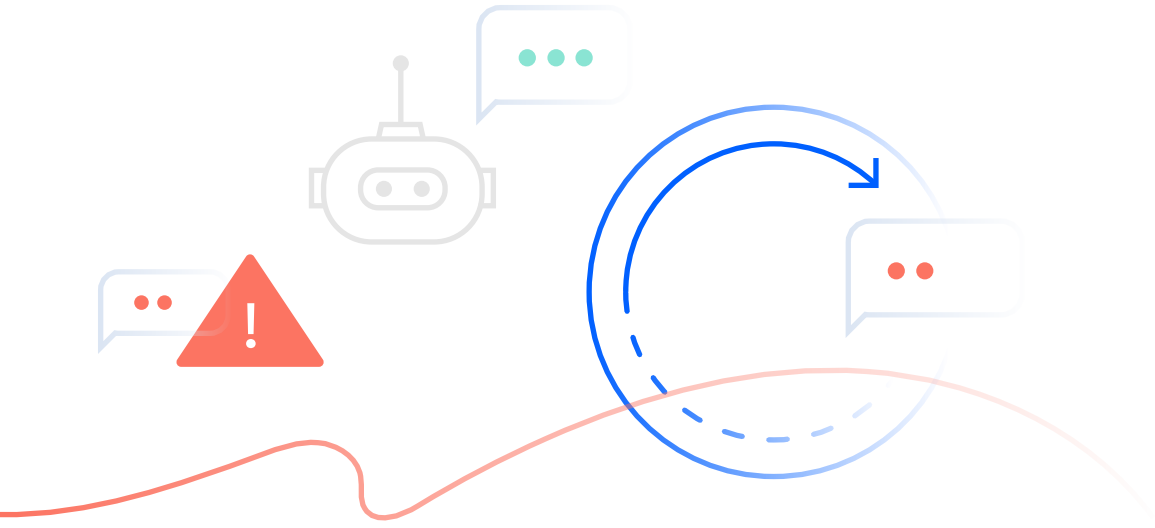
As businesses turn to digital customer support channels, a new threat targets both companies and consumers. With alarmingly high success, bots created by cybercriminals access customer data, undermine your security, and commit identity theft.

INSIDE, LEARN:

+ Why fraudbot risk is rising
+ The 4 goals of fraudbots
+ How fraudbots operate
+ Warning signs fraudbots are attacking
+ 4 methods to protect your company

PLUS:

Fraud uncovered: *How Tethr identified active fraudbots that wasted 1.8 million minutes of agent time and were* ***47% successful*** *in opening closed accounts and jeopardizing sensitive customer information.*



If you read those sentences and thought a customer said them, you could be wrong. Those are just a few examples of what we've seen in **customer support chats**. The only problem with them? They didn't come from actual customers. They came from **bots operated by cybercriminals**.

Meet the fraudbot: the latest creation from the cyber underworld that attacks customer support chat systems.

We've likely all heard warnings about identity theft. In earlier forms, criminals posed as company representatives and extracted information from people over the phone. This tactic still thrives today - but this recent twist on the old method could soon overtake it.

In tech support fraud, criminals claim to provide customer or technical support to defraud an unsuspecting customer into making payments or revealing login credentials. In 2021, tech support fraud amounted to $347 million in losses, according to the FBI's annual Internet Crime Report, which compiled information from 23,903 complaints in 70 countries. It's part of a larger cybercrime problem that totaled 2.7 million complaints and $18.7 billion in losses in the last five years.

Newer methods of the same scam involve fake copies of company websites. Customers may enter their real account information on a copycat website or chat with fake customer support.

Fraudbots turn the old scam on its head. Instead of an individual scammer calling an unwitting individual, fraudbots contact companies. They pose as legitimate customers experiencing problems with their accounts. **The difference? It's done at scale.** One fraudbot can attack a company thousands of times, with alarmingly high success rates.

The fraudbots start a conversation with a goal. They aim to reactivate old accounts, access personal information, obtain discounts, or create new, false accounts. From there, they can use personal information, such as stored credit cards, to commit identity fraud.

The fraudbots start a conversation with a goal. They aim to reactivate old accounts, access personal information, obtain discounts, or create new, false accounts. From there, they can use personal information, such as stored credit cards, to commit identity fraud. **The dangerous part? You'd never guess it by reading the chat transcript.**

Fraudbots aim to:

+ Reactivate old accounts
+ Access personal customer information
+ Obtain discounts
+ Create new accounts

Why fraudbot risk is rising

Customers expect different, more digital, and faster experiences than they used to, even compared to just a few years ago. More companies turn to chat to meet the growing demand for instant answers and services delivered digitally–both administered through chatbots and live agent support chat.

Chatbots direct customers to self-service articles and information. Live chat offers customers the same customized help of an individual agent without requiring them to pick up their phone, wait on hold, and talk to an agent. Meanwhile, live chat agents can juggle three to four support chats at once, boosting productivity.

Research proves customers - and companies - both benefit.

Consider this:

- In many cases, customers prefer chatbots. Research found 69% of customers prefer chatbots when they need a quick answer to something simple. [1]
- Customers prefer live chat to other customer support channels[2] such as phone, email, or chatbot.
- Chat capabilities help maximize agent productivity. An agent live chatting with customers can handle three to four chats at a time[3], compared to one phone call at a time. There's no limit to handling capacity when it comes to chatbots.
- Even live chats operated by individual agents drive contact center costs down dramatically, reducing average costs per customer interaction by as much as half.

1] Source: Salesforce | 2] Source: Kayako | 3] Source: Freshworks

All these reasons contribute to a rise in chat support usage. As more companies adopt the technology, they also increase their risk factor for falling prey to fraud.

How fraudbots operate

AI-powered conversation can go both ways. Company chatbots direct customers to information and can perform basic account activities. Likewise, criminals create bots that mimic customer conversations.

A programmer just needs to have a few conversations with your customer support chat system to know which questions agents will ask. They can use that to develop and script responses, adding a few variations, and begin deploying a bot to attack your chat system.

They can then sync the bot with a database of personal information. Using email addresses and phone numbers obtained through data breaches, they can impersonate those people to other companies.

If they gain access to those accounts, they then tap into more information: payment methods, mailing addresses, and other personal identifying information.

Are you chatting with a fraudbot?

Like those examples of fraudulent chats show, many of the nefarious conversations don't seem fake. Cybercriminals get creative when creating conversations that could easily fool unsuspecting customer service agents. It's not obvious - they think they're chatting with a human.

Here's an example: At Tethr, we analyzed chat conversations for one of our customers, a global consumer technology corporation. These fraudulent chats included various elements that humanized them. The fraudbots would do things that seem human, even seemingly expressing emotion or making personal statements.

The bottom line: If you're chatting with a fraudbot, you won't likely know.

Would you know if you were talking to a fraudbot? Probably not. If the bot said they were frustrated by a long wait, it might seem unremarkable. Even if you happened to encounter the bot again, its unlikely you could recognize a pattern because of variations in bot messages. Many live customer support agents chat with hundreds of customers a day. A similar conversation may not raise alarm bells until it had been deployed for weeks or months- especially if the conversation is routine.

How can companies detect fraudbots?

Fraudbots operate with sophisticated language that doesn't seem obvious or unusual, so the conversations may never raise a red flag. Until your real customers contact you about unauthorized use of their account, you might not know. Targeted customers who become victims of identity theft may also struggle to learn where information such as one payment method was compromised - leaving you in the dark.

To help your chat support team understand the threat, you can educate them on the warning signs of fraud.

Detecting fraud requires a solution that enables you to identify and eliminate fraudbots as quickly as they attack.

To protect against fraudulent chatbots, you need to proactively monitor for bots attacking your system - not wait until data breaches occur. To monitor your chat conversations at scale, you need a fraudbot detection system that combines advanced conversation intelligence with AI-powered fraud pattern recognition. Platforms with deep machine learning capabilities and advanced linguistics understanding can examine your conversations and detect when a bot attacks your system.

Warning signs of fraudbots at work:

+ Customers asking to access closed accounts
+ People asking to access non-existing accounts
+ Rise in fraudulent accounts or customers reporting unauthorized use of accounts
+ People can't answer personal questions beyond account information
+ Refusal to get on the phone

How can you protect against fraudbots?

High-tech threats require high-tech solutions. Cybercriminals use artificial intelligence to mimic human interactions. You can use the same technology to help detect fraud and end threats.

Finding fraudbots without AI is impossible. Our minds can't process all of the words, phrases, behaviors, timing, and digital fingerprints that identify a fraudbot.

To comb your chats for fraudbots, you have to analyze your chats on a large scale, regularly, for suspicious elements. Detection requires more than chat analytics or conversation intelligence.

Instead, you need a specially designed fraud detection system capable of identifying bots that are attacking your company.

> If you uncover a fraudbot, you can take action.

You can program your chat system to recognize known bots. Your team can learn which phrases should raise red flags. You can also see what bots tried to accomplish and modify or create policies if needed.

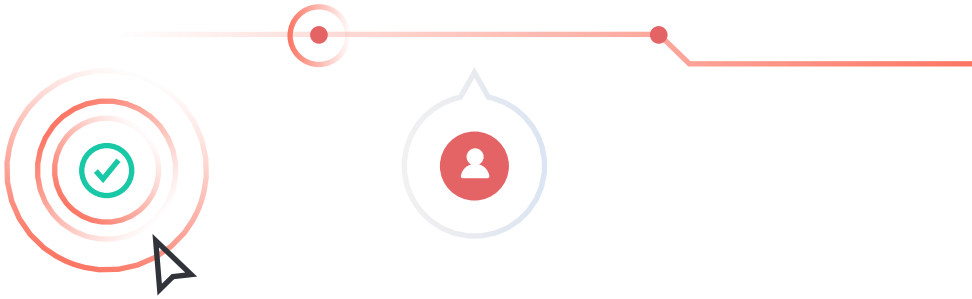
But above all, you can be on guard. Routinely monitor your system for active fraudbots at work, conduct fraud audits, and take measures to prevent them from successfully accessing your customer information.

Fraudbot protection:

+ Regularly analyze chats at scale
+ Keep customer service team up to date on red flags detected
+ Implement heightened security measures

Suspect a fraudbot?

+ Ask a human question
+ Secure transactions with a phone call
+ Alert your team to suspicious language
+ Statistical analysis of conversations with AI-powered conversation intelligence



CASE STUDY

Fraudbots at work

Tethr, an AI-powered conversation intelligence platform, includes a fraudbot detection module that analyzes customer support chats for fraud using the same technology that it uses to help companies optimize customer experience.

In one case, we analyzed customer support chats for a global consumer technology corporation, looking for signs of fraudbots. We found:

- **8 active fraudbots** during a 2 week-period
- 1 bot attacked **83,000** times resulting in **1 million minutes** of chat sessions and **$250,000** of wasted agent time
- Another bot attacked **65,000** times. The average chat time lasted **12.4 minutes**, resulting in a total **847,128 minutes** of wasted agent time. This equates to roughly **$211,782** in agent cost - plus the impact of the actual fraud.

The success rate:

One fraudbots attempted to get agents to reopen previously closed accounts. Tethr found this fraudbot to have a **47% success** rate in opening accounts. These accounts had credit cards attached to them, which exposed the risk for fraudulent transactions to occur.

Removing the fraudbot

Once our customer had information key to the fraudbot's operations, they were able to shut down the attacks with conversation detection, policy changes, and agent education.

However, the work isn't over. Cybercrimine constantly evolves, and the effort to create a new bot is minimal compared to the potential rewards. It takes diligent, continuous monitoring to protect consumer data. **With Tethr, our customers continue to identify and shut down new threats as they emerge.**

Want to see if your chats are a target for fraud?

Set up a call with our product experts who can talk about Tethr's chat analytics solutions and how we identify fraud.