

Media Contact:

Will Wiquist
will.wiquist@fcc.gov

For Immediate Release

**FCC ORDERS BLOCKING OF CALLS FROM GATEWAY
FACILITATOR OF ILLEGAL ROBOCALLS FROM OVERSEAS**
Enforcement Bureau Issues First-Ever RoboBlocking Order Against One Eye

WASHINGTON, May 11, 2023—The FCC’s Enforcement Bureau today ordered voice service providers to block and cease accepting traffic from international gateway provider One Eye. Gateway providers serve as the on-ramps to U.S. phone networks for calls from outside the country, and they have important obligations to block illegal robocall traffic from getting to consumers. The robocall campaigns most recently facilitated by One Eye pertained to the impersonation of a major financial institution and claims of “preauthorized order[s]” placed in consumers’ names.

One Eye received a formal notice in February requiring it to cease carrying robocall traffic that FCC investigators and the Industry Traceback Group identified the company to be facilitating. With today’s RoboBlocking Order, the FCC requires any provider immediately downstream from One Eye to block and cease accepting traffic from One Eye beginning no later than 30 days from today.

FCC Leadership:

Chairwoman Jessica Rosenworcel: “This company—what’s left of it—will now have a place in robocall history. We can and will continue to shut off providers that help scammers. Because these junk calls are not just annoying, they are illegal, and facilitating them deserves serious consequences.”

Enforcement Bureau:

Chief Loyaan Egal: “The Enforcement Bureau team has built a fair, transparent, but tough process by which we can essentially shut down access to U.S. communications networks by companies such as One Eye that are targeting consumers with illegal robocalls. Today’s action demonstrates another cutting-edge tool in our robocall enforcement options and represents a landmark date in our efforts to protect consumers from scam calls.”

How We Got Here:

The Commission gave One Eye notice and ample opportunity to end its facilitation of illegal robocall campaigns. Despite these chances to get on the right side of the law, One Eye continued to participate in illegal robocall campaigns, in violation of FCC rules. In order to protect consumers while giving the company a chance to rectify its actions before facing industry-wide blocking, the FCC Enforcement Bureau:

1. Cited the company’s predecessor entity, PZ/Illum Telecommunication, for transmitting illegal robocall campaigns;

2. Made clear to One Eye through a [cease-and-desist letter](#) in February that the company's attempts to evade enforcement by rebranding had not worked and that it must cease transmitting the identified illegal traffic;
3. Issued a "[K4 Notice](#)" in February to encourage other providers to refrain from carrying One Eye's traffic;
4. Determined that One Eye was in violation of FCC consumer protection rules and thus issued an [Initial Determination Order](#) in April formally demanding that the company block the illegal traffic; and
5. Blocked the company's access to other providers following the company's repeated failure to take required steps to mitigate the illegal calling activity on its network and comply with FCC call authentication rules.

The FCC has solidified its robocall defenses when it comes to gateway providers, including by adopting the Gateway Provider Order on May 19, 2022 which increased the obligations of these providers to police their own networks and imposed consequences on gateway providers that fail to do so. This built upon the Commission's call blocking rules by requiring gateway providers to block illegal traffic when notified of such traffic by the Commission. Under FCC rules, once a gateway provider receives a notification of suspected illegal traffic from the Enforcement Bureau, the provider has a minimum of 14 days to comply with the notice by investigating and reporting the results of the investigation to the Bureau. The provider must also block the traffic if its investigation determines that it served as the gateway provider for the traffic. If the gateway provider does not block the traffic, it must explain to the Bureau why the identified traffic was not illegal.

The Bigger Picture:

Chairwoman Rosenworcel established the FCC's Robocall Response Team to serve as an FCC staff working group to combat the unyielding menace of illegal spoofed, or scam, robocalls. The team pulls together expertise from across the agency to leverage the talents of enforcers, attorneys, policy makers, engineers, economists, and outreach experts.

Getting Results:

- Blocking *active* robocall scam campaigns by issuing first-of-their-kind actions:
 - 99% [drop](#) in auto warranty scam robocalls after an FCC action;
 - 88% month-to-month [drop](#) in student loan scam robocalls;
 - Halted predatory mortgage robocalls targeting homeowners nationwide;
- Fining companies record-breaking amounts for illegal robocalls and spoofing;
- Closing gateways used by international robocallers to reach Americans' phones;
- Widespread implementation of STIR/SHAKEN caller ID authentication standards – including applying the requirements to include gateway providers;
- Working with industry to traceback illegal calls to their sources;
- Ensuring voice service providers meet FCC robocall mitigation requirements;
- Signing robocall investigation partnerships with [44 states, District of Columbia, Guam](#) and international partners;
- Establishing first-of-their-kind regulations targeting scam text messaging; and
- Launched the Robocall Mitigation Database to monitor STIR/SHAKEN compliance.

###

Media Relations: (202) 418-0500 / ASL: (844) 432-2275 / Twitter: @FCC / www.fcc.gov

This is an unofficial announcement of Commission action. Release of the full text of a Commission order constitutes official action. See MCI v. FCC, 515 F.2d 385 (D.C. Cir. 1974).