

Joint Oireachtas Committee on Finance, Public Expenditure and Reform
Opening statement by Google
24 October 2023

Thank you to the Cathaoirleach and members of the Joint Committee for inviting us to speak to you today on the topic of Authorised Push Payment (APP) Fraud.

My name is Ryan Meade and I work with Google as Government Affairs and Public Policy Manager here in Ireland. I am joined today by Ollie Irwin, from our Trust & Safety team, who leads our Google Safety Engineering Center here in Dublin.

The core of Google's mission is helping users find reliable and authoritative information. This applies across our products, whether it's helping users navigate the open web through Search, find local business in Maps, or accessing learning and entertainment on YouTube.

Protecting users of our products is central to this mission. We recognise that our products can only be as helpful as they are safe. That's why we take our responsibility seriously to provide access to trustworthy information and content and we are committed to combating fraudulent activity on our platforms.

We invest heavily in the development of systems, detection methods and enforcement measures to stay ahead of new abuse behaviours and patterns. Our teams use a mix of technology, including sophisticated machine learning, and human review to enforce our policies. This combination of technology and human talent means policy violations can be spotted and swift action can be taken to remove violative content and ads.

Our products and services have multiple layers of built-in protections. When operating at scale, it's important to have a structured approach, powered by technology. We think of reducing risk of abuse under 3 pillars: Prevent, Detect and Respond.

- Primarily, we want to **prevent** abuse from occurring. We embed safety-by-design principles across our products to proactively assess risks and engineer solutions.
 - For example, Google Safe Browsing will warn users when they attempt to navigate to a dangerous website or download dangerous files.
 - We are currently piloting new policies that limit ad views for advertisers we are less familiar with in categories that may be prone to abuse, giving them an opportunity to build up user trust before their campaigns have full reach. You can think of it as a "get-to-know-you" period for advertisers.
- Secondly, **detect**: AI-powered classifiers help us to quickly flag potentially harmful content for removal or escalation. Last year we removed 5.2 billion ads that violate our policies and restricted 4.3 billion ads – most of these actions took place before the ad was seen by a user. Content moderation at this scale is only possible with AI.
 - In 2022, classifiers ensured that 99% of Google searches were spam free.
 - Over the past 2 years, we also launched several algorithm updates specifically focused on reducing the appearance of scammy results in Google Search. These efforts also include the reduction of sites appearing in Search results that are seeking to trick people into thinking they're visiting an official or authoritative site.

- Our dedicated intel teams track emerging global trends and third-party reports to understand how we can get ahead of the curve on detection of new abuse methods, and the building of new, sophisticated protections to help keep users safe.
- Finally, **respond**: Because we are often up against sophisticated bad actors - who are evolving new modus operandi and changing tactics — sometimes new malicious behaviour may temporarily evade our systems, but we are constantly improving our technology and detection methods – supplemented by human review and both user and trusted flagger reporting – to ensure that enforcement against bad actors can be taken in an expeditious manners. As mentioned, as a backstop, users can report or “flag” questionable content they encounter, and that signal informs our systems. We also partner with trusted organisations, including government agencies and NGOs, through our Priority Flagger Program, providing priority tools for them to quickly flag problematic content appearing on our services. When a piece of content is flagged we rely on both humans and AI-driven technology to determine whether it has violated our policies and respond appropriately.

At Google, we proactively look for ways to ensure a safe user experience on all of our platforms, including with the advertising they see. When we make decisions about ads and other monetized content on our platforms, user safety is at the very top of our list. In fact, thousands of Googlers work around the clock to prevent malicious use of our advertising network and make it safer for people, businesses and publishers. We do this important work because an ad-supported internet allows everyone to access essential information and diverse content, free of charge. And as the digital world evolves, our policy development and enforcement strategies evolve with it — helping to prevent abuse while allowing businesses to reach new customers and grow.

Online scams are a growing concern for people everywhere and as technology progresses, bad actors are finding new ways to defraud people and businesses. APP fraud is just one aspect of a scam and fraud landscape that is constantly evolving.

We’ve continued to invest in our policies, team of experts and enforcement technology to stay ahead of potential threats, including launching new policies and updating existing ones. In 2022, we added and updated 29 policies for advertisers and publishers. Our continued investment in policy development and enforcement enabled us to block or remove over 5.2 billion ads, restrict over 4.3 billion ads and suspend over 6.7 million advertiser accounts. And we blocked or restricted ads from serving on more than 1.57 billion publisher pages and across more than 143,000 publisher sites, up from 63,000 in 2021.

The recent increase in scams is not exclusive to internet advertising. Criminal gangs are using multiple malicious methods, including phishing emails, spoof phone calls and texts, shopping scams and impersonation scams, with half of adults in Ireland reportedly receiving a fraudulent text message in 2022 - so online advertising leading to scams is one part of a bigger societal problem.

However, we take our responsibility in this space very seriously, and have not waited to act. We know that people and businesses put enormous trust in Google when they use our products. It is very much in Google’s business interest to do the right thing. Our business is heavily dependent on the proper functioning of a healthy ad-supported open internet, and the continued trust of users in that ecosystem. If consumers abandon bad web experiences, the long-term viability of Google’s core business is at stake. That’s why we have thousands of people working around the clock to create and

enforce effective advertiser and publisher policies to prevent abuse while enabling publishers and businesses of all sizes to thrive.

Fraud is a cross-industry issue that requires strong and sustained cooperation from a range of actors. Tackling scams should be a priority and in our view all of the parties involved should work individually and collectively to find the best ways of tackling a problem which involves sophisticated bad actors seeking out routes to scam consumers. We know from experience that organised criminals are adaptable. They will evolve their approach in response to whatever counter-measures we implement and will target any weak spots in the wider system. This underlines the importance of an effective and coordinated response across the industry and from government and law enforcement working together to address the issue.

Thank you for your time and we look forward to the discussion.