HUNGARIAN COMPETITION AUTHORITY

The GVH is urging consumers to be cautious when banking online

The competition authority has closed its proceedings against Google

Budapest, June 02, 2026 – Due to a lack of provability, no infringement could be established, nor was any result expected from continuing the proceedings; therefore, the Hungarian Competition Authority (GVH) discontinued the competition supervision proceeding initiated in 2025 against Google Ireland Limited, the subsidiary responsible for Alphabet Inc.'s European operations. During the proceedings, Google Ireland Limited stated that it will pay even greater attention to monitoring and filtering phishing ads in the future. In relation to the case, the GVH is drawing consumers' attention to the importance of conscious and careful online banking.

In the fall of 2025, the Hungarian Competition Authority (GVH) initiated a competition supervision proceeding against Google Ireland Limited (the European subsidiary of Alphabet Inc., which operates the Google search platform; hereinafter: Google Ireland). According to the GVH's initial suspicion, the company failed to act in accordance with the requirements of professional diligence in the operation of the Google Ads advertising platform, resulting in fraudulent banking websites that misused the name of MBH Bank Nyrt. for phishing purposes appearing as paid ads at the top of Google's search results.

Following the initiation of the proceeding, the Hungarian Competition Authority sent detailed requests for information to the undertaking subject to the proceeding. In addition, the competition authority contacted Google Számítástechnikai Szolgáltató Kft. (hereinafter: Google Kft.), which is independent of the undertaking under investigation (but is also a subsidiary of Alphabet Inc.), as well as MBH Bank Nyrt., which was affected by the data fishing activities.

During the proceeding, Google Ireland explained that, to ensure the legal compliance of advertisements appearing on Google Ads, it maintains a multi-step, complex internal review process – both pre- and post-publication – that combines artificial intelligence with human review. The monitoring process begins with the creation of the advert and continues even after its approval, covering its headline, description, images, videos, and landing page. The company highlighted that, in the specific case, it was only able to identify an associated advertiser account for one of the pages, which it suspended immediately upon detecting the phishing content.

In addition, Google Kft. stated in response to the GVH's inquiry that the handling of complaints and reports regarding advertisements falls within the jurisdiction of Google Ireland but added that it had done everything in its power to ensure that the misuse of MBH Bank Nyrt.'s name would not cause harm to consumers either during the period under review or in the future.

As part of its investigation into professional diligence, the Hungarian Competition Authority determined that, following the detection of phishing activities misusing the name of MBH Bank Nyrt., Google Ireland took steps to remove the infringing content and suspend certain related advertising accounts. It was not possible however, to reconstruct the full scope of the domains and advertising accounts involved in the phishing activity, nor the circumstances and timing of their management, and the partial evidence available did not allow for a substantive assessment

of whether the control mechanisms established by the company were suitable for addressing the infringements under investigation. Since no substantive results were expected from further procedural steps, the GVH closed the proceedings.

In connection with the case, the competition authority reminds consumers of the importance of cautious, responsible, and informed online banking. When using online banking platforms – whether via a web browser or an app – always verify the authenticity of the site before entering any login details. (Manually typing in the bank's web address is one of the most effective ways to protect against phishing.) If in doubt, saving the commonly used banking interface as a bookmark, checking the link displayed in the search bar (e.g., a phishing link might show "bamk" instead of "bank," "nu" instead of "hu," etc.), and checking for the "padlock" icon next to the search bar, which indicates a secure connection and is always present on official banking websites, can help.

In order to help consumers avoid online banking fraud, the GVH also recommends the detailed information available on the Hungarian National Bank's „Pénzügyi Navigátor" website.

The official registration number of the case is **VJ/42/2025.**

GVH Press
Further information:
Horváth Bálint, Head of Communications +36 20 238 6939