Meta statement to Go Public

We know that losing and recovering access to your online accounts can be a frustrating experience. We invest heavily in designing account security systems to help prevent account compromise in the first place, and educating our users, including by regularly sharing new security features and tips for how people can stay safe and vigilant against potential targeting by hackers. But we also know that bad actors, including scammers, target people across the internet and constantly adapt to evade detection by social media platforms like ours, email and telecom providers, banks and others. To detect malicious activity and help protect people who may have gotten compromised via email phishing, malware or other means, we also constantly improve our detection, enforcement and support systems, in addition to providing channels where people can report account access issues to us, working with law enforcement and taking legal action against malicious groups.

Additional background:

- Scams are a highly adversarial space and we are constantly evolving our techniques to keep pace with changing behaviour online. We currently use, and continue to explore, a variety of methods such as new machine learning techniques to identify content and accounts that violate our policies, as well as working with government, NGOs, and law enforcement agencies to understand new techniques that hackers and scammers may deploy to circumvent our systems.
- Our work goes beyond enforcing our rules against scams whenever we see someone violating them. We also take legal action against coordinated malicious groups whenever appropriate, give people an easy means to report potential violations when they see them and empower our users with tips and tools they can use to protect themselves.
- We know our work will never be perfect. That’s why we’re always working to evolve our approach, improve our enforcement, engage with experts to

ensure that our strategies reflect best practices and stay on top of the latest trends so that we can stay ahead of emerging threats.

- Across our services, we have policies that outline what people can and cannot do on our platform, advertising products and commercial surfaces.
- For example:
    - Across Facebook and Instagram, we have a specific Fraud and Deception policy to protect people and businesses. Under our Fraud and Deception policy, we remove content that purposefully deceives, willfully misrepresents or otherwise defrauds or exploits others for money or property. This includes content that seeks to coordinate or promote these activities using our services,
    - OurAdvertising Standards strictly prohibit deception and misleading behaviour, and
    - OurCommerce Policies prohibit listings with misleading offers.
- We use a combination of technology and review teams to help Meta detect and review potentially violating content and accounts on Facebook and Instagram.
    - Learn more about how we detect violations here: https://transparency.fb.com/enforcement/detecting-violations/
- Scams are often run by people who manually operate fake accounts. That is why our efforts to detect and stop fake accounts are so crucial.
- To combat fake accounts, we deploy technology to prevent them from being created and also detect and remove them from the platform.
- Our detection technology helps us block millions of attempts to create fake accounts every day and detect millions more often within minutes after

creation. As outlined in our quarterly Community Standards Enforcement Report, in Q4 2023, for example:

- We actioned 691 million fake accounts on Facebook, 99.2% of which we detected proactively ourselves via artificial intelligence before a user reported it to us. This is in addition to the millions of fake accounts that we block at the point of creation every day.
- We actioned 964 million pieces of spam content on Facebook, 99.1% of which we detected proactively ourselves via artificial intelligence.

Hacking Prevention Tips:

- We encourage strong security hygiene not just on our platform, but across the internet.
  - Pick a strong password and do not share it across services.
  - We encourage two-factor authentication not only for Facebook and Instagram accounts, but also across all of your online accounts that offer this added protection.
  - We and many other services offer a variety of two-factor authentication options, including SMS-based, authentication apps, and physical security keys. While these measures might add some friction to set up, over the long run, these simple steps help to prevent the vast majority of compromise attempts at scale.
- **Watch out for malicious software:** Malicious software can cause damage to a computer, server or computer network.Learn the signs of an infected computer or device and how to remove malicious software. Keep your web browser up to date and remove suspicious applications or browser add-ons. More on protecting against malware here and here.

- If someone suspects their accounts have been hacked, the best course of action to take is to visit facebook.com/hacked for Facebook or instagram.com/hacked for Instagram and follow the steps outlined there.