GTA VI hacker sentenced to seven years and released on license; hotel Fire Stick used in 2022 intrusions



A UK court sentenced Arion Kurtaj, who breached Rockstar Games, Uber and Revolut in 2022, to seven years, with release on license for time served. The case shows how unmanaged consumer devices can bypass controls.

- Arion Kurtaj, 21, was sentenced at Woolwich Crown Court in London; the nine-year starting term was cut by two years for time in a psychiatric hospital.
- He was released on license the same day and can be returned to prison if he breaches the conditions.
- In September 2022, aged 17 and on bail, he breached Uber, Revolut and the developer of Grand Theft Auto.
- He carried out the hacks using an Amazon Fire Stick connected to a hotel room television after

police had seized his computer.

- He pleaded guilty to six offenses, including four under the Computer Misuse Act and one of fraud.

What happened

A British court has sentenced Arion Kurtaj, now 21, to seven years in prison for hacking Rockstar Games and leaking footage of Grand Theft Auto VI. The judge set a nine-year term and reduced it by two years for time spent in a psychiatric hospital. Because of time served, he was released on license the same day. He will serve the rest of the sentence under community supervision and can be returned to prison if he breaches the conditions.

He pleaded guilty to six offenses: four under the Computer Misuse Act, one of fraud and one of possessing a mobile phone in prison. Seven further charges will lie on file and do not count as convictions. Police said they would seek a Serious Crime Prevention Order, and BBC News reported that a five-year order already bars him from using Telegram and Discord.

How the intrusions were carried out

In September 2022, aged 17 and on bail, Kurtaj breached Uber, Revolut and the developer of Grand Theft Auto. He had been placed in a hotel for his own protection after threats from rival hackers. Police had taken his computer, yet he carried out the attacks with an Amazon Fire Stick plugged into the hotel room television.

Relevance for regulated institutions

The source does not describe the technical methods used against the victims. The practical lesson is broader: a determined actor can operate from very modest, consumer-grade equipment, so confiscating a laptop does not remove capability. Institutions should therefore focus on controls that hold regardless of the attacker's device: strong authentication, access monitoring and tight control over who can reach internal systems.

What to do now

1. Review multi-factor authentication coverage for staff, contractors and third parties with access to internal systems.
2. Check that monitoring detects unusual logins and access from unmanaged or unfamiliar devices.
3. Confirm that personal and consumer devices cannot connect to corporate networks or sensitive systems without approval.
4. Re-brief staff on social-engineering and credential-theft risks, including for remote and travelling employees.
5. Test incident response and leak-handling procedures, including regulator notification duties, against a scenario of stolen internal data.