Prison Time for 11 Involved in India's Cosmos Bank Heist

By Jayant Chakravarti

Archived: 2026-04-05 16:29:17 UTC

ATM / POS Fraud , Cybercrime , Fraud Management & Cybercrime

North Korean-Led Heist Nabbed $13.5 Million in 2018 (@JayJay_Tech) • April 25, 2023

Image: Shutterstock

An Indian court convicted 11 people for their roles in a North Korean heist of $13.5 million in 2018 from Pune-based Cosmos Cooperative Bank.

See Also: Experts Offer Insights from Theoretical to the Realities of AI-enabled Cybercrime

A judicial magistrate first class court in Pune on April 15 passed an order convicting 11 people accused of stealing in August 2018 up to $1.76 million from Cosmos Cooperative Bank. The Pune police cybercrime cell said that nine of the accused will serve four years in prison and two will serve three years.

A Pune police official told Information Security Media Group that all 11 accused were sentenced after admitting to their roles in the cyber heist.

Cosmos Cooperative Bank, which has 140 branches across India and over 2 million customers, said in its annual report for 2018-19 that it had suffered two separate cyberattacks in 2018 - one on Aug. 11 and the other on Aug. 13. Cybercriminals cashed out more than $10 million from domestic and international ATMs and fraudulently transferred $1.7 million to a Hang Seng Bank account in Hong Kong.

Pune police did not name the threat actor responsible for the attacks, but the United Nations in a 2019 report attributed the thefts to North Korea. The hereditary totalitarian regime that has governed the country since 1948 has long underwritten criminal activity, including financially motivated hacking, in a quest for hard currency it uses to fund development of weapons of mass destruction.

The Cosmos heist was a "well-planned and highly coordinated operation that bypassed three main layers of defense contained in International Criminal Police Organization (INTERPOL) banking/ATM attack mitigation guidance," the U.N. report concluded.

The U.S. government responded to a spate of ATM withdrawal attacks, including an attack against the Banco de Chile, by issuing an alert to banks to be on the lookout for indicators of similar incidents.

The Indian bank said the first cyberattack involved cybercriminals targeting its ATM infrastructure. Though it did not disclose how the attack had taken place, it said the cybercriminals used malware to sever the ATM infrastructure from its core switching system, ensuring that the system did not receive real-time information about cash withdrawals from ATMs.

The cybercriminals carried out more than 12,000 transactions at overseas ATMs using cloned Visa debit cards and more than 2,800 transactions at domestic ATMs using cloned RuPay debit cards, stealing up to $1.76 million in under four hours.

The second attack involved cybercriminals targeting the SWIFT infrastructure to fraudulently transfer $1.7 million to the Hong Kong-based bank account.

The Pune police cybercrime cell, which later took over the investigation, arrested seven suspected money mules in September 2018 based on video footage obtained from multiple ATM outlets. It said the suspects were possibly involved in stealing over $4 million in December 2017 from Chennai-based City Union Bank as well (see: *Seven Arrests in Cosmos Bank Heist*).

With reporting by ISMG's Mihir Bagwe in Mumbai.
