US indictment: data recovery firm co-founder accused of secretly paying ransomware gangs



A US grand jury has indicted a Florida data recovery firm co-founder for allegedly paying ransomware actors in secret while claiming his firm could decrypt data without payment. The case is a reminder to vet recovery vendors.

- The co-founder faces three counts of wire fraud, each carrying up to 20 years in prison, in the District of Rhode Island.
- Prosecutors allege the firm claimed proprietary decryption technology it did not have and instead negotiated with attackers behind clients' backs.
- In an FBI undercover operation in June 2026, he allegedly paid about $6,000 in Bitcoin for a key and billed the supposed victim about $13,260.
- Prosecutors say the proceeds were used to buy several properties in Florida.

> - In July, a former ransomware negotiator at DigitalMint was sentenced to 70 months for leaking negotiation details to BlackCat (ALPHV) operators.

What is alleged

The US Department of Justice says a federal grand jury in the District of Rhode Island has indicted Juan Ricardo Palacio Escobar, a co-founder of a Florida data recovery firm, on three counts of wire fraud. He was arrested in Las Vegas on October 22. These are allegations, not findings of guilt.

According to the indictment, the company told ransomware victims it had sophisticated decryption technology able to recover data without paying a ransom. Prosecutors allege it had no such technology. Instead, he is accused of negotiating with the attackers without telling clients, paying them, and charging clients a higher sum to keep the difference.

The undercover evidence

The case relies on an FBI operation in June 2026, in which agents posed both as a company hit by ransomware and as the attacker holding its data. Palacio allegedly paid the fake attacker about $6,000 in Bitcoin for a decryption key, then billed the undercover company about $13,260, more than double.

The source also notes a related prosecution: in July, Angelo Martino, a former ransomware negotiator at incident response firm DigitalMint, was sentenced to 70 months in prison for passing confidential negotiation details, including insurance policy limits, to BlackCat (ALPHV) operators, who used them to raise ransom demands.

Why it matters for regulated institutions

Both cases involve third parties trusted during a crisis, when decisions are made quickly and under pressure. Organisations that depend on external recovery or negotiation specialists should treat those providers as high-risk suppliers, with clear contractual transparency and oversight of any contact with attackers.

What to do now

1. Vet any data recovery or ransomware negotiation provider before an incident: verify credentials, references and the technical basis of recovery claims.
2. Require contract terms that disclose any contact or payment to attackers and make costs auditable against provider invoices.
3. Keep a pre-approved incident response retainer so decisions are not made under pressure with unknown vendors.
4. Restrict sensitive details, such as cyber insurance limits, to those who need them, and include them in third-party confidentiality clauses.

5. Maintain tested offline backups and a recovery plan to reduce reliance on third-party decryption claims.
6. Define internal approval and legal review steps, including engagement with competent Saudi authorities, before any ransom-related decision.