When the Defenders Become the Attackers: Cybersecurity Experts Indicted for BlackCat Ransomware Operations

Published: 2025-11-03 · Archived: 2026-04-06 00:59:33 UTC

The Shocking Case That's Rocking the Cybersecurity Industry

Computer Security

In a stunning turn of events that reads like a cybercrime thriller, three former employees of cybersecurity incident response companies have been indicted for allegedly conducting the very ransomware attacks they were supposedly hired to prevent. The case has sent shockwaves through an industry already grappling with questions about the ethics of ransomware negotiation and payment facilitation.

The Accused: Insiders Turned Criminals

The defendants include Kevin Tyler Martin, 28, of Roanoke, Texas, Ryan Clifford Goldberg, 33, of Watkinsville, Georgia, and an unnamed co-conspirator identified only as "Co-Conspirator 1" who resided in Land O'Lakes, Florida.

According to the indictment and FBI affidavits, Martin and Co-Conspirator 1 both worked as ransomware negotiators at DigitalMint, a Chicago-based (River North neighborhood) cybersecurity incident response firm that helps victims recover from ransomware attacks and, in some cases, facilitates ransom payments. Goldberg served as a director of incident response for Sygnia Cybersecurity Services, a multinational cybersecurity company where he managed incident response operations.

Antivirus & Malware

fbi-affidavit-re-ransomware-negotiatorsfbi-affidavit-re-ransomware-negotiators.pdf498 KB.a{fill:none;stroke:currentColor;stroke-linecap:round;stroke-linejoin:round;stroke-width:1.5px;}download-circleThe charges filed in the U.S. District Court for the Southern District of Florida are severe: conspiracy to interfere with interstate commerce by extortion (18 U.S.C. § 1951(a)), interference with interstate commerce by extortion, and intentional damage to protected computers (18 U.S.C. § 1030(a)(5)(A)). If convicted, Martin and Goldberg each face up to 20 years in prison for the extortion charges and 10 years for the computer damage charges, plus supervised release, fines up to $250,000 (or twice the gross gain or loss from the offense), and forfeiture of all proceeds from their criminal activity.

What makes this case particularly troubling is the position of trust these individuals held. As ransomware negotiators and incident responders, they had intimate knowledge of victim vulnerabilities, negotiation tactics, and the psychological pressure points that make ransomware attacks so effective. They were the very people companies turned to in their most desperate hour—and they allegedly exploited that trust to identify and attack new victims.

indictment-of-ransomware-negotiatorsindictment-of-ransomware-negotiators.pdf384 KB.a{fill:none;stroke:currentColor;stroke-linecap:round;stroke-linejoin:round;stroke-width:1.5px;}download-circle## The Alleged Crime Spree

Between May 2023 and April 2025, the defendants allegedly operated as ALPHV BlackCat affiliates, systematically targeting companies across multiple states. The indictment filed on October 2, 2025, details a coordinated campaign of extortion that left victims facing devastating choices between paying millions or losing access to critical business data.

The Victims and Ransom Demands:

Computer Hardware

Victim 1 - Tampa Medical Device Manufacturer (May 13, 2023): Goldberg, Martin, and Co-Conspirator 1 encrypted the company's servers and demanded approximately $10 million to decrypt the data and prevent publication of stolen information. The attack caused immediate operational paralysis—employees living and working in the Southern District of Florida were unable to work because their devices could not access data and applications necessary for their jobs, contributing to operational delays and lost business. Under duress, the company paid $1,274,781.23 in cryptocurrency. The conspirators then paid the ALPHV BlackCat administrators their percentage and split the remainder among themselves.

Victim 2 - Maryland Pharmaceutical Company (May 2023): The group encrypted the pharmaceutical company's servers and demanded a ransom payment. While the indictment doesn't indicate whether this victim paid, the attack involved stealing sensitive data and threatening to publish it—a double extortion tactic designed to maximize pressure on the victim.

Victim 3 - California Doctor's Office (July 2023): The conspirators encrypted the medical practice's servers and demanded approximately $5 million. The attack on a healthcare provider is particularly egregious, as medical facilities often face life-or-death decisions about whether to pay ransoms to restore access to patient records and operational systems.

Victim 4 - California Engineering Firm (October 2023): The group encrypted the engineering company's servers and demanded approximately $1 million to decrypt the data and prevent data publication. Goldberg specifically mentioned this victim in his FBI interview, acknowledging the attack though indicating they were unsuccessful in extracting payment.

Victim 5 - Virginia Drone Manufacturer (November 2023): In their final documented attack, the conspirators encrypted the drone manufacturer's servers and demanded approximately $300,000. As a manufacturer engaged in interstate commerce—and potentially defense-related work—this victim's compromise could have had broader national security implications.

Hacking & Cracking

The ransom demands ranged from $300,000 to $10 million, demonstrating the group's ability to calibrate their extortion based on the victim's size and perceived ability to pay. According to FBI affidavits, the conspiracy continued until April 2025, suggesting there may be additional unreported victims.

The BlackCat Connection: A Ransomware Empire

Understanding the scope of this case requires understanding ALPHV BlackCat itself and how the defendants integrated into its criminal infrastructure. For more background, see our comprehensive profile of BlackCat/ALPHV ransomware and our coverage of the DOJ's disruption campaign against the group.

The Ransomware-as-a-Service Model

ALPHV BlackCat operated as a sophisticated ransomware-as-a-service (RaaS) operation. In this model, "developers" created and updated the ransomware, then recruited and vetted "affiliates" who would identify and attack victims using the malware. The developers provided affiliates with the ransomware through a password-protected "panel" available on the dark web via the Tor network, customized to each affiliate.

In May 2023, Co-Conspirator 1 obtained an affiliate account on the ALPHV BlackCat panel and shared access with Goldberg and Martin. This gave the trio access to BlackCat's ransomware toolkit and criminal infrastructure. The three conspirators agreed to use the ALPHV BlackCat ransomware and panel to attack and extort victims, sharing the ransom proceeds among themselves and paying a percentage to the ALPHV BlackCat administrators.

Antivirus & Malware

The Attack Methodology

The typical ALPHV BlackCat attack followed a standard pattern that the defendants replicated:

- The affiliate gained unauthorized access to the victim's network
- They stole sensitive data before deploying the ransomware
- They deployed the encryption malware, locking the victim out of their systems
- They left a ransom note directing victims to an ALPHV BlackCat panel on the dark web
- Victims could communicate with the attackers through this panel to negotiate ransom
- Once payment was agreed upon, the attackers provided Bitcoin or Monero cryptocurrency addresses
- Ransom payments were split up and moved through various cryptocurrency addresses via multiple transactions to obscure the source before cashing out to fiat currency

The Scale of BlackCat Operations

As of September 2023, ALPHV BlackCat affiliates had compromised over 1,000 entities—nearly 75 percent in the United States and approximately 250 outside the U.S. The operation demanded over $500 million and received nearly $300 million in ransom payments. There were over twenty ALPHV BlackCat ransomware victims in the Southern District of Florida alone, where this case was prosecuted.

The FBI identified ALPHV/Blackcat actors as having compromised prominent government entities including municipal governments, defense contractors, and critical infrastructure organizations. The ransomware attacks caused tens of millions in cryptocurrency ransom payments, major disruptions in ongoing operations, and large losses of proprietary information.

Since mid-December 2023, of the nearly 70 leaked victims, the healthcare sector was the most commonly victimized—likely in response to ALPHV BlackCat administrators encouraging affiliates to target hospitals after law enforcement action against the group in early December 2023.

How the Investigation Unfolded

On June 17, 2025, the FBI conducted a consensual recorded interview of Ryan Clifford Goldberg. After initially denying involvement in ransomware attacks, Goldberg confessed that he was recruited by Co-Conspirator 1 (the unnamed Florida-based DigitalMint employee) to "try and ransom some companies."

In his confession, Goldberg admitted that he, Co-Conspirator 1, and Martin "successfully ransomed" the Tampa medical device company (Victim 1). He also acknowledged conducting attacks on other companies, including the California engineering firm (Victim 4), though those attacks were unsuccessful. Goldberg confirmed they used ALPHV BlackCat ransomware to conduct the attacks.

Most damning was Goldberg's admission about their money laundering operation. After Victim 1 paid the ransom, they routed the cryptocurrency through a mixing service and then through multiple cryptocurrency wallets, believing this would make the funds harder to trace. Goldberg told FBI agents he conducted the attacks to get out of debt and that he feared he was "going to federal prison for the rest of [his] life."

The investigation also revealed that Goldberg learned about the FBI's actions against his co-conspirators. According to his statement, Co-Conspirator 2 (Martin) contacted him after the FBI raided Co-Conspirator 1's home on April 3, 2025. Martin was "freaking out about the FBI raiding [Co-Conspirator 1]."

Forensic analysis of devices used by Goldberg and seized pursuant to search warrant revealed digital breadcrumbs of the conspiracy. On or about May 4, 2023—approximately six days before the attack on the Maryland pharmaceutical company—Goldberg used a search engine to look up Victim 2's name. The next day, May 5, 2023, Goldberg conducted multiple internet searches, including one for Co-Conspirator 1's name followed by "doj.gov."

Court records show that Martin spoke at the Technology Law Conference in Austin, Texas in May 2024, where he was described as a current DigitalMint employee explaining how he worked to negotiate ransom payments on behalf of companies—all while allegedly having stolen more than $1 million in such an attack just a year earlier.

Flight to Europe: A Desperate Escape

Ten days after his FBI interview, on June 27, 2025, Ryan Clifford Goldberg and his wife boarded a one-way flight from Atlanta, Georgia to Paris, France. The tickets were purchased just two days before travel—on June 25, 2025—suggesting a hasty departure following his confession to federal agents.

As of the date of the criminal complaint filed in September 2025, the FBI believed Goldberg and his wife were still in Europe. The Bureau was unaware of any flights purchased by Goldberg to return to the United States, indicating he may be attempting to avoid prosecution by remaining overseas.

This flight to Europe adds another layer of complexity to the case and demonstrates Goldberg's apparent consciousness of guilt. His decision to leave the country shortly after admitting to federal crimes suggests he understood the severity of the charges he would face.

Goldberg was eventually taken into federal custody in September 2023 and has remained detained since then, while Martin was released on $400,000 bond after his arrest.

Company Responses: Damage Control Mode

Both DigitalMint and Sygnia moved quickly to distance themselves from the accused.

DigitalMint stated that Martin acted "completely outside the scope of his employment" and emphasized that the indictment does not allege the company had any knowledge of or involvement in the criminal activity. The company confirmed it has been cooperating with the investigation and noted that the charged conduct took place outside of DigitalMint's infrastructure and systems, with the co-conspirators not accessing or compromising client data.

Sygnia CEO Guy Segal confirmed that Goldberg was terminated after the company learned of his alleged involvement with the ransomware attacks. The company declined further comment, citing the ongoing FBI investigation.

Antivirus & Malware

A Pattern of Questionable Ethics in Ransomware Recovery

While shocking, this case is not occurring in a vacuum. The ransomware negotiation industry has long faced questions about transparency and ethics—and this isn't even the first time DigitalMint has been under federal investigation.

The Earlier DOJ Investigation

In July 2024, the Department of Justice launched a criminal investigation into a former DigitalMint employee over allegations that the individual secretly coordinated with BlackCat/ALPHV hackers to receive kickbacks from ransom payments. That investigation, first reported by Bloomberg, focused on whether the employee violated federal laws including conspiracy, wire fraud, and money laundering by allegedly receiving a cut of ransoms while facilitating cryptocurrency payments to the very threat actors who conducted the attacks.

The ProPublica Exposé: A Broader Industry Problem

A landmark 2019 ProPublica investigation revealed systematic deception across the ransomware recovery industry. The investigation uncovered that prominent U.S. data recovery firms, including Proven Data Recovery (based in Elmsford, New York) and Florida-based MonsterCloud, secretly paid ransomware gangs while claiming to use proprietary "high-tech" decryption solutions—and charged clients substantial fees on top of the ransom amounts.

The ProPublica investigation documented how these firms:

Deceived Clients About Their Methods: Firms promised to unlock files using "the latest technology" and "proprietary software" when they were actually just paying the ransoms. Some firms used "canned responses"

offering clients two options—pay the ransom or use the firm's technology—when the second option didn't actually exist.

Developed Relationships with Hackers: Former Proven Data employee Jonathan Storfer revealed that the company developed such close relationships with ransomware operators like SamSam that the hackers would recommend victims work with Proven Data. The SamSam attackers would tell victims: "If you need assistance with this, contact Proven Data." Storfer described having to "almost befriend" cybercriminals to negotiate better prices, maintaining a list of hackers who could supply decryption keys quickly and cheaply.

Used Aliases to Hide Their Activities: Both companies used pseudonyms for employees when communicating with victims. Proven Data used the alias "Brad Miller" for overseas freelancers, while MonsterCloud employee "Zack Green"—who held titles including "Ransomware Recovery Expert" and "Cyber Counterterrorism Expert"—was revealed to be using an alias. When asked about this, MonsterCloud's CEO Zohar Pinhasi said, "We go based on aliases, because we're dealing with cyberterrorists."

Misled Law Enforcement: Multiple police departments that hired MonsterCloud believed the firm had unlocked their files without paying ransoms. Chief Deputy Ward Calhoun of Mississippi's Lauderdale County Sheriff's Office told ProPublica: "The danger is, even if you give money to hackers, you don't know you're gonna be able to unlock your data anyway. We decided we weren't going to do that. We went with MonsterCloud instead." MonsterCloud had actually paid the ransom but never disclosed it.

Potentially Funded Sanctioned Entities: ProPublica traced bitcoin payments from Proven Data to SamSam ransomware attackers who were later identified as Iranian nationals and indicted by the DOJ. The payments continued until those bitcoin wallets were sanctioned by the U.S. Treasury Department for supporting the Iranian regime. Between 2017 and 2018, Proven Data made numerous payments to SamSam, continuing until twelve days before the Iranian hackers were indicted in November 2018.

The FBI's Investigation: The FBI's 2018 investigation of Proven Data, triggered by a victim in Anchorage, Alaska, revealed the extent of the deception. An FBI affidavit stated: "Subsequent investigation by the FBI confirmed that PDR was only able to decrypt the victim's files by paying the subject the ransom amount." The victim, real estate broker Leif Herrington, had been told Proven Data had "proprietary software they developed to unencrypt" when the firm had simply paid the $1,680 ransom and charged him $6,000.

Industry-Wide Testing Exposes the Practice: Security researcher Fabian Wosar conducted "Operation Bleeding Cloud" in 2016, creating fake ransomware and posing as a victim to test multiple data recovery firms. He found that firms including MonsterCloud and Proven Data "all claimed to be able to decrypt ransomware families that definitely weren't decryptable and didn't mention that they paid the ransom. Quite the contrary actually. They all seemed very proud not to pay ransomers." Soon after, the anonymous email addresses Wosar had set up for his imaginary attacker received offers to pay the ransom from these same firms.

Antivirus & Malware

The fundamental issue is this: ransomware negotiation exists in a moral gray area. On one hand, these professionals help victims recover from devastating attacks and often reduce ransom demands. On the other,

paying ransoms can be seen as funding criminal activities, perpetuating the ransomware business model, and potentially financing terrorism and other forms of cybercrime.

The Current Case: History Repeating

The current indictment of Martin, Goldberg, and their co-conspirator represents an escalation—not just paying ransoms secretly, but actually conducting the attacks themselves. This progression from questionable business practices to alleged criminal conspiracy demonstrates how the lack of regulation and oversight in the ransomware negotiation industry can enable increasingly brazen misconduct.

The Insider Threat Amplified

What makes this case particularly alarming for the cybersecurity industry is the nature of the insider threat it represents. These weren't ordinary employees—they were trusted specialists with:

- **Deep knowledge of victim psychology**: Understanding exactly what pressures make victims pay
- **Technical expertise**: Knowing how to deploy ransomware and cover their tracks
- **Access to victim information**: Through their legitimate work, potentially identifying vulnerable targets
- **Negotiation experience**: Understanding how to extract maximum payments
- **Cryptocurrency expertise**: Knowing how to receive and launder ransom payments

This case demonstrates how insider threats can emerge even in cybersecurity firms themselves. The defenders who understand attack methodologies can become the most dangerous attackers.

Industry Implications and Trust Erosion

The ramifications extend far beyond these three individuals:

Computer Security

For Incident Response Firms: This case will likely trigger enhanced background checks, monitoring of employee activities, and stricter controls around access to sensitive information. Trust but verify will become the new normal.

For Victims: Organizations now face an additional layer of concern when engaging ransomware negotiators. How can you be certain the person helping you isn't also the one who attacked you—or won't become your next attacker?

For the Insurance Industry: Cyber insurance carriers, already tightening ransomware coverage, may impose additional scrutiny on approved incident response vendors.

For Law Enforcement: This case provides a template for investigating insider threats within the cybersecurity industry itself, an area that has received relatively little attention.

The Broader Context: Ransomware's Unstoppable Growth

Over the past 18 months before December 2023, ALPHV/Blackcat emerged as the second most prolific ransomware-as-a-service variant in the world based on the hundreds of millions of dollars in ransoms paid by victims.

The FBI developed a decryption tool that allowed them to work with dozens of victims, saving multiple victims from ransom demands totaling approximately $68 million. In December 2023, the Department of Justice successfully disrupted BlackCat's operations, seizing several websites and providing decryption tools to over 500 victims.

However, despite law enforcement disruption campaigns against major operations like LockBit and ALPHV/BlackCat, a representative for BlackCat announced the group was shutting down in March 2024 following the Change Healthcare ransomware attack. This was likely part of a rebranding strategy common among major ransomware operations—when one brand becomes too hot due to law enforcement attention, operators simply rebrand and continue.

The 2025 cybersecurity landscape shows that following these major disruptions, the ransomware ecosystem has become more fragmented, with 70-80 active groups now identified. While this creates a more complex threat environment, attacks continue at unprecedented levels—Q1 2025 saw a 126% increase in ransomware incidents compared to Q1 2024.

Legal and Ethical Questions for Negotiators

The indictment raises critical questions for the ransomware negotiation industry:

Antivirus & Malware

- **Should negotiators be licensed or regulated?** Currently, almost anyone can become a ransomware negotiator. Should there be formal qualifications, background checks, or oversight?
- **What level of transparency is required?** Should negotiators be required to disclose when they're paying ransoms versus using other recovery methods?
- **Are conflicts of interest adequately managed?** How do firms ensure negotiators aren't cultivating relationships with threat actors that cross ethical lines?
- **Should there be industry standards?** Organizations like the Ransomware Task Force have proposed frameworks, but adoption remains voluntary.

Lessons for Organizations

For organizations relying on incident response firms, this case offers several critical lessons:

Vet Your Vendors Thoroughly: Don't just look at technical capabilities. Examine ethical frameworks, employee vetting processes, and internal controls.

Understand the Process: Ask explicit questions about how your incident response firm operates. Will they pay the ransom? How do they handle negotiations? What reporting do they provide?

Maintain Your Own Oversight: Even when working with external negotiators, maintain internal oversight of the process. Don't outsource your responsibility entirely.

Prioritize Prevention: The best ransomware defense remains strong cybersecurity hygiene: regular backups, network segmentation, multi-factor authentication, and employee training.

Have a Pre-Breach Plan: Identify and vet incident response partners before you need them. During a crisis is not the time to evaluate whether you can trust your negotiator.

The Path Forward

This case should serve as a wake-up call for the cybersecurity industry. While the vast majority of incident responders and ransomware negotiators operate ethically, the potential for abuse is real and the consequences devastating.

Computer Security

The industry needs:

- **Greater transparency** about how ransomware recovery actually works
- **Professional standards** and codes of ethics for negotiators
- **Better vetting** of personnel in sensitive positions
- **Enhanced monitoring** to detect insider threats
- **Clear regulatory frameworks** that balance victim needs with crime prevention

Conclusion: Trust But Verify

Ryan Clifford Goldberg has been in federal custody since September 2023 and remains detained pending trial. Kevin Tyler Martin was released on $400,000 bond. Both have pleaded not guilty, and their trials will ultimately determine their guilt or innocence. Co-Conspirator 1, whose identity has not been publicly disclosed, has not been indicted as of the time of this writing, though the investigation remains ongoing.

The case number 25-CR-20443-MOORE/D'ANGELO in the U.S. District Court for the Southern District of Florida is expected to take approximately five days for trial, according to court filings. The indictment was filed on October 2, 2025, following a criminal complaint and FBI affidavit submitted in September 2025.

Regardless of the trial outcomes, this case has already achieved one thing: it has forced the cybersecurity industry to confront uncomfortable questions about insider threats, ethical standards, and the sometimes-murky world of ransomware negotiation.

For organizations facing the growing threat of ransomware, the message is clear: your defenders must be above reproach. When those who promise to protect you become the attackers themselves, everyone loses—except the ransomware gangs who continue to profit from fear, desperation, and broken trust.

The cybersecurity industry must do better. The stakes are simply too high for anything less.

Case Details:

- **Case Number**: 25-CR-20443-MOORE/D'ANGELO
- **Court**: U.S. District Court, Southern District of Florida
- **Indictment Filed**: October 2, 2025
- **Charges**: 18 U.S.C. § 1951(a) (Conspiracy to Interfere with Interstate Commerce by Extortion), 18 U.S.C. § 1951(a) (Interference with Interstate Commerce by Extortion), 18 U.S.C. § 1030(a)(5)(A) (Intentional Damage to a Protected Computer)
- **Maximum Penalties**: Up to 20 years for extortion charges, 10 years for computer damage, plus fines and forfeiture

As this case develops through the legal system, it will likely establish precedents for how insider threats within cybersecurity firms are prosecuted and may lead to significant changes in how the ransomware negotiation industry operates. Organizations should stay informed about developments and reassess their incident response partnerships accordingly.

Computer Hardware
