RANSOM OR RESIST? A CASE STUDY IN IDENTITY-BASED INSURANCE FRAUD

WHY SIUS MUST TREAT CYBER RANSOMWARE ATTACKS AS A NEW CATEGORY OF FRAUD

By Richard Wickliffe, ARM, CLU, CPCU, FCLS

Insurance fraud isn't standing still, and neither should we. For decades, Special Investigation Units have focused on staged accidents, inflated medical billing, or arson-for-profit schemes. But today's fraudsters have taken their crimes online, swapping tow yards for call centers and crowbars for keyboards. Instead of faking injuries or torching cars, they steal identities, hijack corporate systems, and extort millions, often under the same insurance policies meant to protect the victims.

That shift is more than an IT problem. It is an emerging fraud problem, and it's redefining how insurers, claims managers, and investigators must respond.

IDENTITY-BASED FRAUD: THE NEW FRONT LINE

The National Insurance Crime Bureau (NICB) recently projected a **49% increase in fraud tied to identity theft**, including criminals impersonating others to gain financial advantage.[1] In the cyber realm, that identity-based fraud is now the fastest-growing M.O.

Take the prolific cybercriminal group known as *Scattered Spider*. Their attacks have targeted some of the largest corporations, and increasingly, insurance carriers themselves. Their playbook is deceptively simple:

- They call a company's help desk, armed with enough personal data to convincingly impersonate an employee.
- Request a reset of multifactor authentication (MFA) or a new enrollment link.
- Use the link to gain access and leverage self-service password reset functions.
- Once inside, lock systems, steal data, and demand payment.

[1]National Insurance Crime Bureau, Press Release, Sept 2, 2023 https://www.nicb.org/news/news-releases/nicb-projects-49-rise-insurance-fraud-linked-identity-theft-2025

This isn't high-tech hacking. It is classic impersonation fraud, updated for the cloud era.

CASE STUDY: LAS VEGAS, SEPTEMBER 2023 — THE ATTACK UNFOLDS

A cyberattack on MGM Resorts rippled across the Las Vegas Strip with startling precision. Imagine: gaming machines went offline, elevators froze between floors, hotel keys stopped working, ATMs couldn't dispense cash, payment systems crashed, and even the lights flickered out, plunging parts of the resort into panic. On top of that, personal data, including names, addresses, dates of birth, driver's license numbers, and Social Security numbers for some customers, were stolen by the attackers.

The perpetrators were members of Scattered Spider. This was not a sneak intrusion, they used social engineering, helped by publicly available employee data (from easy sources as LinkedIn) to impersonate insiders and bypass password resets.

Two weeks earlier, the same adversaries had struck their main competitor, Caesars Entertainment. Their systems were breached via a similar social engineering attack. Caesars discovered that an unauthorized actor had obtained customer loyalty program data, including sensitive personal information such as driver's license and Social Security numbers.

The critical divergence came in how each company responded and how each treated the insurance and fraud consequences.

THE BIG QUESTION: PAY OR DO NOT PAY THE RANSOM?

Here's where things get real for SIU professionals. Caesars responded by negotiating with the attackers. They reportedly settled on a ransom payment of $15 million, negotiated from a demand of $30 million. Once paid, their systems recovered quickly, and customer-facing operations saw less disruption.

How do we know these details for something that would seem to be damaging to publicize? Caesars had to file a Form 8-K with the U.S. Securities and Exchange Commission. In that 8-K, required by law for any event that could impact shareholders, they disclosed the incident, including what was accessed, how they were investigating, and steps being taken to mitigate harm.[2]

By sharp contrast, MGM, staunchly **refused** to pay the attackers, similar to the FBI's "we don't pay terrorists" mindset. Result: their losses were massive. They estimated over $100 million in impact from the attack, plus approximately $10 million in expenses such as legal, consulting, and IT recovery. Their Form 8-K was more ambiguous; it referenced an investigation, law enforcement involvement, "protecting our systems and data," but withheld much detail about what had been compromised or how.[3]

For SIUs, this case should be viewed as more than a cyber incident; it's a fraud claim scenario. A threat actor used impersonation to create a false pretense, caused financial loss, and ultimately triggered an insurance response, as policies contain ransom payment coverage.

CYBER INSURANCE AND THE FRAUD QUESTION

Cyber insurance, once an obscure coverage, now often includes reimbursement for:

- Business interruption losses
- Incident response and forensic costs
- Customer notification and credit monitoring
- Legal defense and settlements
- Ransom payments

This last feature raises fundamental fraud questions. **Does paying a ransom equate to rewarding criminal fraud?** Or is it a legitimate cost-containment strategy under the duty to mitigate losses?

We were taught as children not to pay the bully your lunch money in the schoolyard, because he would only come back for more. From an anti-fraud perspective, paying a ransom seems to carry the same risk of emboldening repeat attacks.

Yet, the math is stark: $15 million paid to restore operations versus $110 million in losses, and that figure continues to climb when you factor in lost customer loyalty and multiple class-action lawsuits. This dilemma is now central to cyber claims management, with fraud examiners increasingly called upon to advise on coverage, subrogation, and recovery.

[2]Caesars Entertainment, Inc., SEC Filing, Form 8K, Sept. 7, 2023, https://investor.caesars.com/node/33686/html

[3]U.S. Securities and Exchange Commission, Oct 5, 2023. https://www.sec.gov/Archives/edgar/data/789570/000119312523251667/d461062d8k.htm

THE FALLOUT: INSURERS ON THE HOOK

MGM claimed coverage under its $200 million cyber policy, reportedly written by AIG with Beazley as an excess carrier, syndicated among others.[4] Caesars carried almost identical coverage. That insurance safety net, while essential for recovery, ultimately pushes costs back into the system.

We all bear the weight. The Coalition Against Insurance Fraud estimates fraud already costs **$932 per consumer annually**.[5] With ransom payments and cyber losses now part of the equation, that number will rise. And unlike traditional claims, these payouts often go directly into the cryptocurrency wallets of international crime groups.

THE EXPANDING TARGET: CARRIERS THEMSELVES

Perhaps the most alarming trend is that the attackers have begun to target insurers directly. This raises the stakes considerably: not only are carriers paying ransom claims, but they risk becoming victims themselves, exposing policyholder data, claims files, and even underwriting systems.

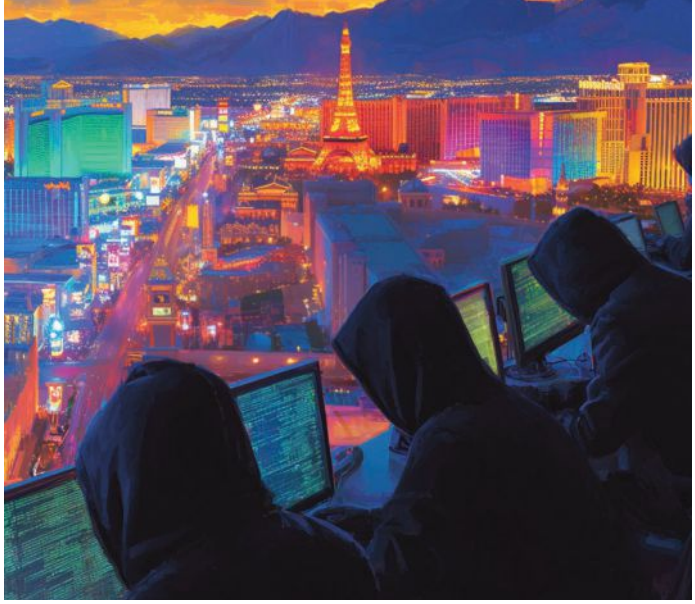
Google's Threat Intelligence Group warned that it is "aware of multiple intrusions in the U.S. which bear the hallmarks of Scattered Spider activity," including incidents that directly impact the insurance sector.

ARE THESE HIGH-TECH MASTERMINDS? NOT QUITE.

When the news first broke about the Las Vegas casino "heists," it was easy to picture a modern *Ocean's Eleven* crew, or scenes out of *Mission: Impossible*, with a team of elite hackers in a criminal headquarters, typing lines of code to bypass world-class security.

But the reality is far less cinematic, and arguably more disturbing. Investigators have learned that many of the so-called "cyber masterminds" were simply teens and young adults living in their parents' homes, armed with little more than a cell phone and a script. Three recent Scattered Spider arrests illustrate the point: **Remington Ogletree (19, Texas), Noah Urban (20, Florida), and Tyler Buchanon (23, UK)**.[6]

Recently, on September 17 of this year, another member turned himself in to Las Vegas authorities in connection with the casino intrusion. The press could not release his name because he was a minor.[7] None of these kids were living in extravagant lairs or using supercomputers.



This should send a chill down the spine of any fraud investigator. If teenagers with a Wi-Fi connection can compromise billion-dollar enterprises, what could a truly organized fraud ring do with the same methods?

LESSONS FOR SIU AND FRAUD PROFESSIONALS

The Las Vegas case demonstrates that **cyber ransom events are a new class of insurance fraud exposure**. Key takeaways for the industry:

1. **Reframe Cybercrime as Fraud:** Treat impersonation-based ransomware as organized fraud, not just an IT failure.
2. **Strengthen Identity Verification:** Partner with claims and HR to tighten MFA, help desk verification, and insider threat controls.
3. **Anticipate Coverage Disputes:** Determine when ransom payments constitute covered loss mitigation versus prohibited enrichment.
4. **Collaborate with Cybersecurity:** SIUs should sit at the table during cyber incident response, just as they would with suspicious fire or theft losses.
5. **Track the Fraud Costs:** Factor ransomware payouts into fraud analytics. They are part of the $308 billion fraud impact that raises premiums for all consumers.

Richard Wickliffe *led SIU teams for over 20 years for the US's largest property-casualty carrier. He is the author of the acclaimed* YOU PAID FOR THIS, *about his 25 years investigating fraud. He enjoys speaking nationally about fraud and cybercrime trends at venues including cyber security conferences and the FBI's InfraGard Counterterrorism meetings, where he received the FBI's Exceptional Service in the Public Interest Award. He's also an award-winning author of crime fiction inspired by our imaginative industry. He can be reached at RLWickliffe@yahoo.com*

[4]"AIG, Beazley among carriers on the breached MGM, Caesars $200M cyber towers", Cyber Risk Insurer, Feb. 15, 2024. https://www.theinsurer.com/cyber-risk/news/aig-beazley-among-carriers-on-breached-mgm-caesars-200mn-cyber-towers/

[5]"Insurance Fraud Costs the U.S. $308.6 Billion Annually," Coalition Against Insurance Fraud, 2022, https://insurancefraud.org/wp-content/uploads/The-Impact-of-Insurance-Fraud-on-the-U.S.-Economy-Report-2022-8.26.2022-1.pdf

[6]"US arrests Scattered Spider suspect linked to telecom hacks," BleepingComputer.com, Dec. 5, 2024, https://www.bleepingcomputer.com/news/security/us-arrests-scattered-spider-suspect-linked-to-telecom-hacks/

[7]Las Vegas Metropolitan Police Press Release, Sept. 19, 2025. https://www.lvmpd.com/Home/Components/News/News/2245/263