Z E R O T R A C E L A B S

A T T A C K C A S E S T U D Y

Julia Goodwin SIM Swap and Physical Attack: When Digital Compromise Escalates to Armed Home Invasion

A retirement-age crypto investor was targeted through carrier-level SIM hijacking, followed by violent physical coercion — exposing the lethal convergence of telecom fraud and real-world violence in crypto theft.

Attack Snapshot

victim	Julia Goodwin — retirement-age individual investor, BlockFi customer, T-Mobile subscriber
date	2025
loss	28 BTC + 1,108 ETH (estimated mid-seven figures USD at 2025 market prices)
attack Type	SIM swap → exchange account takeover → physical coercion / armed home invasion → multi-hop laundering
chain	Bitcoin, Ethereum (multi-chain)
attribution	Unattributed organized criminal group; operational sophistication suggests coordinated team with telecom insider access or social engineering capability, physical enforcement personnel, and laundering infrastructure

Executive Summary

Attackers executed a SIM swap against Julia Goodwin's T-Mobile number while she was traveling in Costa Rica, exploiting the timing window when the victim was geographically displaced from her carrier's support infrastructure and less likely to detect the swap in real time. Using the hijacked number to bypass SMS-based two-factor authentication, the attackers drained 28 BTC and 1,108 ETH from her BlockFi exchange account. The operation then escalated from digital to physical: attackers conducted an armed home invasion, pressing weapons to Goodwin's head and

demanding additional wallet credentials. Stolen funds were subsequently laundered through layered transactions across multiple wallets and centralized exchanges including Binance and Coinbase, complicating recovery. This case is a textbook example of how SIM swap attacks serve as both a primary exploitation vector and a reconnaissance mechanism that can precipitate targeted physical violence.

What Happened

Julia Goodwin represented a profile increasingly targeted by organized crypto-theft rings: a retirement-age investor with substantial digital asset holdings, likely less operationally sophisticated than younger cohorts, and reliant on carrier-provided phone numbers as a primary authentication factor. Her use of BlockFi as a custodial platform and T-Mobile as her carrier placed her squarely within two ecosystems with documented histories of SIM swap vulnerability — T-Mobile has paid hundreds of millions in settlements related to SIM swap failures, and centralized exchange accounts remain high-value targets precisely because they aggregate assets behind a single authentication boundary.

The attackers demonstrated operational awareness by initiating the SIM swap while Goodwin was in Costa Rica. This was not coincidental. Overseas travel creates a near-ideal exploitation window: the victim is in a different time zone, potentially unreachable by her U.S. carrier, unlikely to immediately notice loss of cellular service (which may be attributed to roaming issues), and unable to walk into a domestic carrier store for rapid remediation. The SIM swap itself — whether achieved through a bribed T-Mobile employee, social engineering of carrier support, or exploitation of T-Mobile's account management systems — redirected Goodwin's phone number to an attacker-controlled SIM. This gave the attackers access to any SMS-based one-time passwords and account recovery flows tied to that number.

With control of the phone number, the attackers moved swiftly against her BlockFi account. They initiated transfers of 28 Bitcoin and 1,108 Ether — a portfolio that at 2025 prices likely represented well into seven-figure USD value. BlockFi's reliance on SMS-based 2FA as a recovery or authentication pathway, combined with whatever email or password reset mechanisms the attackers had also compromised (likely via the same phone number controlling email account recovery), allowed the full drain. The speed of execution suggests pre-planned operations: the attackers had already identified Goodwin's holdings, her exchange platform, and her authentication dependencies before triggering the swap.

The case then took a violent turn that distinguishes it from typical SIM swap incidents. Attackers conducted an armed home invasion at Goodwin's residence, pressing weapons to her head and demanding credentials to additional wallets — suggesting the attackers either knew or suspected she held assets beyond the BlockFi account, potentially in self-custodied wallets. This escalation from digital to physical attack is a pattern ZeroTraceLabs has tracked with increasing frequency since 2023: threat actors who breach digital accounts use the information gained (transaction histories, wallet

addresses, portfolio sizes) to assess whether the victim warrants a physical operation to extract remaining assets. The SIM swap was not just an exploitation vector — it was reconnaissance.

Post-theft, the stolen BTC and ETH were routed through a multi-hop laundering chain involving numerous intermediary wallets before touching centralized exchanges including Binance and Coinbase. This layering strategy exploits the gap between on-chain traceability and exchange-level identity verification: if the attackers used accounts registered under stolen or synthetic identities (or exploited exchanges with weaker KYC enforcement in certain jurisdictions), they could convert stolen assets to fiat or stablecoins before law enforcement subpoenas catch up. The use of both Binance and Coinbase — platforms with different regulatory postures and response timelines — suggests deliberate jurisdictional arbitrage.

This incident underscores an uncomfortable reality: for high-net-worth crypto holders, especially those whose personal information is accessible through carrier accounts, public records, or social media, digital security failures can directly precipitate physical danger. The attackers treated Goodwin as a complete target — her digital identity, her financial accounts, and her physical person were all vectors to be exploited in sequence.

Kill Chain

1. **Target identification and reconnaissance**
   Attackers identified Goodwin as a high-value target — likely through leaked BlockFi customer data (BlockFi suffered a 2022 breach affecting customer data), on-chain analysis of known addresses, social engineering of financial advisors, or dark web data broker services. They mapped her carrier (T-Mobile), exchange (BlockFi), approximate holdings, home address, and travel schedule.

2. **SIM swap execution during travel window**
   Attackers ported Goodwin's T-Mobile number to an attacker-controlled SIM while she was in Costa Rica. Method was likely social engineering of T-Mobile support or insider complicity. The overseas travel window was deliberately chosen to maximize dwell time before detection — the victim would attribute loss of service to roaming issues rather than a SIM swap.

3. **Exchange account takeover and asset extraction**
   Using the hijacked phone number, attackers intercepted SMS-based 2FA codes and potentially triggered password resets on Goodwin's BlockFi account (and likely her associated email). They initiated transfers of 28 BTC and 1,108 ETH to attacker-controlled wallets. The entire drain likely occurred within a 30-60 minute window.

4. **Physical coercion — armed home invasion**
   Attackers escalated to physical violence, conducting an armed home invasion at Goodwin's residence. Weapons were pressed to her head as attackers demanded credentials to additional wallets and accounts beyond those already compromised. This step targeted self-custodied assets not accessible through the exchange takeover alone.

5. **Multi-hop laundering through centralized exchanges**

Stolen BTC and ETH were moved through a chain of intermediary wallets — likely including mixers, cross-chain bridges, or peel chains — before being deposited into accounts on Binance and Coinbase for conversion. The layering was designed to break on-chain traceability and exploit exchange AML response latency.

Where Users Failed Themselves

— Reliance on SMS-based two-factor authentication as a primary or sole second factor for a custodial exchange holding seven-figure assets. SMS 2FA is not authentication — it is a carrier trust delegation, and carriers have repeatedly demonstrated they cannot be trusted with that responsibility.

— Concentration of substantial digital asset holdings on a single custodial exchange (BlockFi) rather than distributing across cold storage, multi-sig arrangements, and geographically separated custody solutions proportionate to portfolio size.

— Phone number used as a single point of failure across multiple critical accounts — likely the same T-Mobile number secured the exchange account, email account, and potentially banking relationships, creating a cascading compromise chain from one SIM swap.

— Insufficient operational security around travel patterns and personal information. Attackers knew when Goodwin was abroad, suggesting leaked travel data via social media, compromised email, or surveillance. High-net-worth holders must treat their physical location and travel schedule as sensitive information.

— No apparent use of carrier-level SIM swap protections such as T-Mobile's Account Takeover Protection, a port-out PIN, or migration to a carrier that supports hardware-based account locks. These are imperfect but raise the difficulty bar for attackers.

Prevention Checklist

FOR INDIVIDUAL USERS

☐ Eliminate SMS-based 2FA entirely for any account protecting financial assets. Migrate to hardware security keys (YubiKey, Titan) using FIDO2/WebAuthn. Use TOTP (Authy, Google Authenticator with encrypted backups) only as a fallback where hardware keys are unsupported.

☐ Move the majority of crypto holdings to cold storage (hardware wallets) with multi-signature configurations (e.g., 2-of-3 multi-sig using geographically separated keys). Custodial exchange balances should represent only what is needed for near-term activity.

☐ Port your phone number to a carrier with stronger SIM swap protections (e.g., carriers supporting Number Lock or equivalent), or move critical 2FA to a dedicated VoIP number (Google Voice) that is not tied to a physical SIM and cannot be SIM-swapped through carrier social engineering.

☐ Establish a dedicated email address used exclusively for financial accounts — not tied to your phone number for recovery, not used for any other purpose, protected by hardware key 2FA. Gmail with Advanced Protection Program is a baseline.

☐ Implement a personal operations security (OPSEC) protocol: do not disclose travel plans publicly, do not reveal portfolio size on social media, use a PO Box or registered agent for public-facing addresses, and consider a dedicated phone number for financial institutions separate from personal communications.

☐ Before any international travel, lock your carrier account, notify your exchange(s) to flag the account for enhanced verification, and consider temporarily reducing exchange balances to cold storage.

FOR PROTOCOLS & PROJECTS

☐ Exchanges must deprecate SMS-based 2FA as a standalone second factor and enforce hardware key enrollment for accounts above configurable value thresholds. SMS should never be accepted as a sole authentication factor for withdrawal authorization.

☐ Implement mandatory withdrawal time-locks (24-72 hours) for new withdrawal addresses, with multi-channel notification (email + push + in-app) and a one-click cancellation mechanism. This single control would have stopped this drain.

☐ Deploy behavioral analytics to flag anomalous withdrawal patterns — full account drain, new withdrawal address, geographic IP shift from the user's baseline, and SIM change signals from carrier APIs should all trigger automatic holds requiring enhanced verification.

☐ Exchanges should integrate with carrier SIM-change detection APIs (where available) to flag accounts for review when a SIM swap event is detected on the associated phone number, adding a friction layer before permitting authentication via the newly swapped number.

☐ Establish dedicated high-net-worth client security programs offering multi-party authorization requirements, dedicated account managers for withdrawal approval, and proactive threat intelligence briefings.

FOR THE ECOSYSTEM

☐ Telecom carriers must be held to a higher liability standard for SIM swap fraud. T-Mobile's repeated failures — resulting in hundreds of millions in lawsuit settlements — demonstrate that financial penalties alone have not driven adequate security improvements. Regulatory mandates for port-out verification procedures are overdue.

☐ The FCC's 2023 SIM swap rules requiring carriers to authenticate customers before processing SIM changes must be aggressively enforced, with meaningful penalties for non-compliance and mandatory breach reporting when SIM swaps facilitate financial theft.

☐ Centralized exchanges should participate in shared intelligence networks for SIM swap indicators — when one exchange detects a SIM swap-initiated account takeover, that signal should propagate to other exchanges holding accounts tied to the same phone number, enabling preemptive freezes.

☐ Law enforcement agencies need dedicated fast-track protocols for crypto theft cases involving physical violence. The intersection of digital and physical attack vectors creates compound victim harm that requires coordination between cybercrime and violent crime units.

☐ On-chain analytics firms and exchanges must reduce the latency between theft detection and fund freezing. In this case, stolen assets touching Binance and Coinbase should have been flaggable within hours if the victim reported promptly and exchange compliance teams had automated taint-tracking in place.

Key Takeaway

A phone number is not an identity — it is a transferable token controlled by a minimum-wage carrier employee. Any security architecture that treats a phone number as a trust anchor is one social engineering call away from total compromise, and for high-value holders, that compromise can escalate from digital theft to physical violence in the same operation.

SOURCES

— Court filings and public reporting on Julia Goodwin SIM swap and physical attack case (2025)

— T-Mobile SIM swap vulnerability history — FCC enforcement actions and class action settlements (2021-2024)

— BlockFi data breach disclosure (November 2022) — customer data exposure affecting account-level targeting

— FCC Report and Order on SIM Swap and Port-Out Fraud (FCC 23-95, November 2023)

— ZeroTraceLabs internal threat intelligence on SIM swap-to-physical-attack escalation patterns (2023-2025)

— On-chain analysis of multi-hop laundering patterns through centralized exchanges — Chainalysis and Elliptic public reporting (2024-2025)