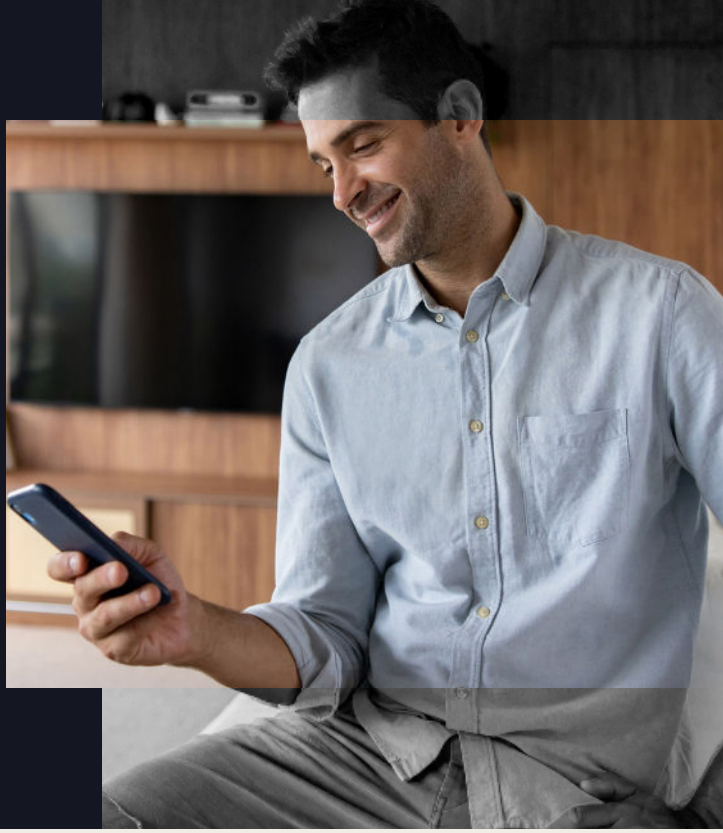
BLACKCLOAK®

Private Client Overcomes SIM Swap Attack with BlackCloak's Expert Response



The warning signs were immediate and alarming. A seemingly routine phone trade-in quickly spiraled into a devastating SIM swap attack, leading to widespread personal and financial exposure for this individual.

- A sudden inability to receive calls or texts.
- Relentless attempts to log into her Apple ID, which she could not complete.
- Unexpected and fraudulent charges appearing on her American Express card.
- A massive "spam bomb" attack, inundating her email with hundreds of messages overnight.

The Problem

Our private client experienced a severe cybersecurity incident when her phone number was hijacked through a SIM swap, occurring shortly after she traded in an old iPhone. Despite assurances that her old device would be wiped, bad actors gained control of her phone number, leveraging it to bypass multi-factor authentication (MFA) across numerous critical accounts. This immediate loss of her phone service was quickly followed by fraudulent American Express charges totaling tens of thousands of dollars, attempts to open new bank accounts for illicit money transfers, and a debilitating spam attack on her email. She found herself locked out of virtually all her online services, including her business email, CapitalOne, PayPal, Venmo, and social media, as her MFA was critically tied to the compromised phone number.

She needed help from a trusted partner. She turned to BlackCloak.

To learn more, please visit:

blackcloak.io

BlackCloak's Guidance

Our Security Operations team immediately launched a remote support session to assess the full extent of the compromise. We quickly identified the SIM swap as the root cause, understanding how the attackers had exploited her phone number to gain unauthorized access to her digital life. Our team confirmed the widespread account lockouts, the fraudulent financial activity, and the business email compromise.

Our four-step plan:

1. **Harden Her Accounts:** We prioritized regaining control of her compromised phone number, which was critical for restoring her digital identity. Our team assisted her in changing passwords for her business email, social media, and other affected accounts. We then implemented stronger, device-specific multi-factor authentication (MFA) using authenticator apps like Authy, ensuring that future access attempts would require a physical device not tied to her SIM card. We also worked to disconnect any unauthorized devices from her Verizon account.

2. **Changed Account Permissions:** While the primary vector was the SIM swap, we systematically reviewed and secured her new Apple ID account, ensuring recovery keys were set up and that no unauthorized devices or numbers could be linked. We also ensured that the Verizon account portal itself was hardened, enabling number locks and credit/identity protection features to prevent future unauthorized transfers.

3. **Identified Other "Pivot Points"** Accessed by the Bad Actor: The threat actor had successfully gained access to numerous personal and financial accounts, including her Apple ID, American Express, CapitalOne, PayPal, Venmo, Facebook, Instagram, Delta Airlines, and Amazon. We meticulously worked through each compromised platform, changing passwords, setting up robust MFA, disputing fraudulent charges (like the $13,000 on AMEX and a line of credit on PayPal), and submitting information to reactivate suspended accounts like Venmo.

4. **Began Ongoing Identity Monitoring:** The client had already initiated credit freezes and filed FTC and police reports. BlackCloak guided her through the process of extending fraud alerts and onboarded her to our identity monitoring services. We also began the crucial process of digital footprint minimization, scrubbing her personal information from data broker sites to reduce future exposure risks.

The Result

Once the BlackCloak team secured our client's compromised accounts and digital footprint, we conducted a workshop to teach her about cybersecurity hygiene best practices, emphasizing the importance of authenticator apps over SMS-based MFA. We ensured MFA was set up on all her personal accounts where possible and moved her to an external password manager to protect and manage her login credentials securely.

On an ongoing basis, we keep her personal devices protected through the BlackCloak endpoint detection and response (EDR) and anti-malware solution, which detects malicious files and is monitored by the Security Operations Center (SOC) 24/7. The BlackCloak Security Operations Center (SOC) is also available to help assess the validity of emails she receives. We provide ongoing identity monitoring and conduct periodic digital footprint assessments to give her peace of mind that she will not fall victim to another malicious scam.

This is just one of many examples demonstrating BlackCloak's unwavering commitment to providing our customers with trusted, superior Digital Executive Protection and highlights the effectiveness of our holistic approach to cybersecurity.