**NAPSA Scam Advice Forum March 2025**

**Topic: SIM Swap Attacks**      Cybercriminals are hijacking phone numbers to bypass security, access financial accounts, and steal identities. This presentation will break down how SIM swap attacks happen, the devastating consequences for victims, and the latest law enforcement efforts to combat this growing threat. Featuring a real case study, SA Latham will share information about an actual investigation to reveal how these crimes unfold—and how to identify this crime and protect the clients you serve. SIM means Subscriber Identity Module

**Speaker:** Special Agent Daniel Latham has served with the FBI since 2016, beginning in Los Angeles with complex financial crime investigations before shifting to cybercrime. His work has focused on SIM swaps, malware, and computer intrusions, including leading the FBI’s Qakbot malware takedown in August 2023.

 **Co-Hosts:** Steve Baker and Debbie Deem

Sign up for Steve’s weekly ‘www.Bakerfraudreport.com’ for news/trends/ arrests/prosecutions worldwide on transnational frauds/scams.

**National Elder Fraud Hotline (U.S. DOJ)** 1-833-372-8311

National federal hotline for adults 60 and over to report fraud and providing support and resources/safety tips. Help with filing IC3 and FTC reports. Language line. <https://ovc.ojp.gov/program/stop-elder-fraud/providing-help-restoring-hope>

**Report Fraud to Local Police/APS as Well as One or More of These Federal Govt. Databases/Agencies**

* **FBI Internet Crime Complaint Center** [www.ic3.gov](http://www.ic3.gov)
* **Federal Trade Commission** [www.reportfraud.ftc.gov](http://www.reportfraud.ftc.gov)
* **Report Identity Theft to the FTC** [www.identitytheft.gov](http://www.identitytheft.gov)
* **U.S Postal Inspection Service (USPIS)** www.uspis.gov/report

**Or 1-877-876-2455**

* **U.S. Secret Service:** If Crypto Investment Confidence Fraud - contact your local U.S. Secret Service office, in addition to filing an IC3 report. You can also file at CryptoFraud@SecretService.gov
* **FBI Guidance For Crypto-Currency Scam Victims in Completing an IC3 report** https://www.ic3.gov/Media/Y2023/PSA230824

**SIM Swap Attacks/Fraud (Port-Out Fraud, SIM cloning fraud, Subscriber fraud)**

* IC3 warning: Criminals Increasing SIM Swap Schemes to Steal Millions of Dollars from US Public <https://www.ic3.gov/PSA/2022/PSA220208>
* File a report with the local police and file a report with the Internet Crime Complaint Center at www.ic3.gov.

**Prevention and Protection Recommendations:**

* Use an authenticator app or hardware-based two-factor authentication instead of SMS-based methods.
* Set up a PIN or password with your mobile provider to prevent unauthorized SIM swaps.
* Be cautious of phishing attempts and safeguard personal information.
* Regularly monitor financial and personal accounts for unusual activity.
* Place a freeze on credit reports.

**Recognizing and Responding to SIM Swapping**: **Signs of an attack:**

* Sudden loss of phone service.
* Inability to send or receive calls and texts.
* Receiving alerts about account activity you didn’t initiate.

**Immediate actions:**

* Contact your mobile provider to verify your account status.
* Change passwords for sensitive financial and social media accounts.
* Notify financial institutions, place alerts and monitor for unauthorized transactions.
* Place a freeze on credit reports, if not done before.
* Report to local authorities and to IC3.gov.

**Federal Communications Commission (FCC)**

* Guide to Cell Phone Fraud: https://www.fcc.gov/consumers/guides/cell-phone-fraud
* What is a SIM Card, and an E-Sim Card? https://www.fcc.gov/consumers/guides/esim-cards-faq
* SIM Swapping Info Guide: https://www.fcc.gov/sites/default/files/sim\_swap\_tip\_card.pdf
* What is Port- Out-Fraud? https://www.fcc.gov/consumers/scam-alert/port-out-fraud-targets-your-private-accounts

**Other articles of Interest**

* AARP How To Avoid Sim Swap Scams <https://www.aarp.org/home-family/personal-technology/info-2021/how-to-avoid-sim-swap-scams.html>
* How SIM Swap Hackers Steal Millions https://www.youtube.com/watch?v=2Ple9F5XOdE

# Bank America Customer Out $38K After Falling Victim To SIM Swapping

 https://www.youtube.com/watch?v=C9Z2Lg4ZgPE

* How to Protect Yourself From Sim Swapping (good explanation for victims) https://www.youtube.com/watch?v=3YEvMPe-h98
* **6 Signs You Have Been SIM Swapped (Forbes)** Being aware of the warning signs can help you protect your identity. Below are key indicators that your SIM may have been compromised:<https://www.forbes.com/sites/alexvakulov/2024/09/20/8-simple-steps-to-prevent-sim-swap-fraud/>
1. Your cell phone suddenly loses signal or cannot make calls.
2. You are locked out of accounts that are usually accessible through your phone, such as banking, social media, or email accounts; investigate further.
3. Unexpected changes in your online accounts, such as password reset requests or notifications you did not initiate.
4. You receive texts or emails from your mobile carrier about changes to your account that you did not authorize.
5. Your contacts receive strange messages from you that you did not send.
6. Unfamiliar account access alerts from services you use about logins from unfamiliar devices or locations.

**Sample Federal and State Investigations/Prosecutions:**

* **Josh Jones SIM Swap**: In 2020, a 17-year-old Canadian individual perpetrated a SIM-swap scheme, resulting in the theft of $37 million from a Santa Monica resident. This incident marked the most significant SIM swap theft from a single individual at the time. Through collaborative efforts with local Canadian authorities, SA Latham successfully identified and apprehended the perpetrator within three months of the case’s initiation.<https://torontolife.com/city/the-case-of-the-missing-46-million/>
<https://financialpost.com/fp-finance/cryptocurrency/teen-in-hamilton-crypto-case-was-detained-following-gta-raid-last-year-source>

* Michigan SIM Swapper – A Michigan man used SIM swapping to steal cryptocurrency and high-value Instagram accounts from victims.  He was arrested and confronted with evidence he recorded on his phone.  SA Latham will show how SIM swapping is done from the hacker’s perspective <https://www.justice.gov/usao-cdca/pr/michigan-man-sentenced-3-years-prison-role-sim-swapping-led-account-takeovers-and>
* Florida Man Charged in Sim-Swapping Spree is Key Suspect in Hacker Groups Oktapus, Scattered Spider <https://krebsonsecurity.com/2024/01/fla-man-charged-in-sim-swapping-spree-is-key-suspect-in-hacker-groups-oktapus-scattered-spider/>
* Joel Ortez, The College Student Who Stole $7.5M via SIM Swapping (Santa Clara County DA’s Office, Prosecutor Erin West and REACT TF) <https://www.youtube.com/watch?v=2rFLGR5hlIA>

**Free National Online Support Programs (for all ages)**

* **AARP Fraud Support Group** Support for victims and family members of these frauds: To register (you don’t have to be AARP member, no age restriction).
	+ <https://www.aarp.org/money/scams-fraud/fraud-victim-support-group/?cmp=RDRCT-CSN-FRD-NEW-SUPPORT_GROUP_PAGE>

* **Cybercrime Support Network** Free romance imposter fraud 10 week online peer support program.
	+ https://fightcybercrime.org/programs/romance-scam-recovery-group/
* **GiveAnHour**  Monthly free support programs for fraud victims and family members.
	+ https://giveanhour.org/financial-fraud/
* **Cathy Wilson, Therapist Lifepaths Counseling**
	+ https://www.scamsurvivorhealing.com/
	+ Free video series for victims of romance imposter and other frauds/scams.
		- https://www.scamsurvivorhealing.com/video-1/
		- https://www.youtube.com/@fraudpsychology