THE EDITOR'S CORNER

SIM City

I was recently the victim of a SIM swap scam—a modern form of identity theft where criminals hijack your phone number to access your bank accounts and personal data. With just a few clicks, they can reroute your calls and texts, lock you out of your phone, and drain your accounts before you even realize what's happened. In my case, tens of thousands of dollars were stolen in a matter of hours. The experience left me stunned, vulnerable, and more aware than ever of the fragility of our digital security.

A SIM swap scam begins when criminals gather enough personal information—often through phishing, data breaches, or social media—to impersonate you. The thieves then convince your wireless carrier to transfer your phone number to a SIM card that they control. This allows them to intercept text codes sent for two-factor authentication and use them to reset your banking passwords. Within minutes, you're locked out of your phone and bank account.

Picture this terrifying scenario: I'm at work at the end of a busy day when I get an e-mail congratulating me on my new iPhone. I dismiss it as spam—until a second e-mail alerts me that my bank password has been changed. Suddenly, I'm locked out of my phone and bank account. The alerts keep coming. Money is being withdrawn in real time.

With a sinking feeling and no way to contact the bank, I jump in my car and begin the hour-long drive home. When I arrive, I call the bank from our landline. With no sense of urgency, customer service bounces me between agents and the fraud department. Money continues to vanish, one transaction at a time. Once one account is empty, the thief moves on to the next. But the stolen money is only the start of my problems.

The attack occurred on a Thursday night, which meant staff payroll bounced the next morning. Fortunately, my personal account wasn't compromised, or I would have had no access to cash while waiting for new bank cards to arrive. I wired my staff their paychecks from my personal account and closed all business bank accounts. I froze my credit to keep the thieves from taking out a loan in my name, then opened new accounts. Nevertheless, insurance electronic funds transfers continued to be deposited into the old accounts, requiring the constant hassle of visiting the bank to transfer funds.

SIM swap scams have been around for almost a decade. Why, then, are banks and mobile carriers still behind? One reason text messages are still used for security is their familiarity to older customers just beginning to bank online. When fraud occurs, however, banks blame the carriers and carriers blame the banks, allowing neither to take full responsibility. Until stronger security protections—such as authenticator apps, biometric logins, or hardware security keys—become the default, users shoulder the risk.

The best way to avoid a SIM swap scam is to stop relying on your phone number for account security. Set a PIN or password with your mobile carrier to block unauthorized SIM card changes. Remove your number as a recovery option for your bank accounts. Rather than use text messages for two-factor authentication, log in to accounts with an authenticator app such as Google Authenticator or a physical security key such as YubiKey, which I now use. (For more tips for defending yourself and your practice from digital threats, see cybersecurity expert Gary Salman's guide in this issue.) In combination with strong passwords, these steps are your best protection in a world run by crooks.

NDK