PL
INNOVATING WITH TRUST WITH LightRiver
REINVENTING DATA CENTER DESIGN WITH ZincFive
DEFENDING THE FRONT LINES WITH TransUnion
LOSING THE SPACE RACE
A GUIDE TO EMBRACING INNOVATION FROM ORACLE
MANAGING INNOVATION UNCERTAINTY
THE BRIGHT & DARK SIDE OF PROGRESS
+
GENAI INNOVATION
NAVIGATING THE MOON
AUTONOMOUS NETWORKS
INNOVATION

www.pipelinepub.com
Volume 21, Issue 8

Defending the Front Lines: For Telecom Security, Customers Need Protection After Cyber Incidents

By: Dan Carella

Fraud losses are mounting across the telecommunications sector, with threats evolving in volume and sophistication. While telecom companies focus on perimeter defenses, cybercriminals target a more vulnerable access point: people. What's more, it appears that what happens after a data breach—from any source—is becoming more critically important to telecom security and fraud prevention.

TransUnion's 2025 Telecommunications Industry Fraud Report paints a troubling picture: Nearly 70% of telecom executives reported a rise in fraud attempts over the past three years. The cost of fraud now averages 3% of revenue, a significant hit to telecommunications businesses already facing rising operational costs and shifting customer expectations. What's equally concerning is that many of these attacks don't rely on technical sophistication alone. They count on a simple formula for gaining access to high-quality breached personal information, poor credential hygiene, and a lack of post-incident protection.

Most telecom providers know their services are more than just connecting calls and data. They are today's gatekeepers of digital identities. Mobile devices are primary interfaces connecting users to everything from banking to healthcare to corporate systems. Telecom accounts become especially attractive to attackers when the door is open to exploit compromised credentials.

The impact of account takeover fraud

Telecom fraud takes shape in many ways — from new account fraud and SIM swaps to payment fraud and synthetic identity fraud. Yet, account takeover (ATO) has emerged as a particularly outsized threat to providers and customers. Enabled by a combination of weak or reused passwords and inadequate identity security protocols, ATO typically begins with reusing stolen credentials harvested through data breaches, phishing attacks, or malware.

Once inside a customer's account, fraudsters can wreak havoc — locking them out, manipulating billing details, intercepting messages, or even impersonating them to attack others. Affected customers face rapidly mounting stress from service disruptions, potential financial losses, and data privacy risks.

The effects on telecom companies are also multifaceted. Fraud places extra burdens on customer service teams, and despite their best efforts, providers may still experience reputational damage and customer loss.

ATO fraud can also be more difficult to contain. Once a customer account is compromised, attackers can misuse it to conduct phishing and social engineering attacks against the victim's contact list. Fraud can spread laterally through the customer base, blossoming from a single incident into broad network exposure.

Post-breach protection matters more than ever

The sad reality is that nearly every telecom consumer has had their personal data compromised in one or more data breaches. The black market for consumer credentials isn't just mature but it's thriving. Fraudsters often begin their attacks with valid usernames, email addresses and passwords in hand.

Telecom customer accounts are attractive to fraudsters because they can do so much within a compromised account. Stolen credentials give them license to impersonate subscribers, reroute SIM cards, order new devices, make other unauthorized purchases, and more. The stakes are uniquely high because telecom accounts are gateways to a host of downstream fraud schemes. Telecoms must tackle protecting and supporting customers whose information has already been exposed.

Providers must operate under the assumption that fraudsters already have access to customer credentials, so perimeter security defenses must include tools and processes to help protect customers from breaches originating elsewhere.

The ROI of protecting compromised users is tangible, not just because every incident prevented or contained stems from financial and reputational damage. Bundling proactive protection strategies enables telecom providers to differentiate themselves in a highly competitive marketplace, and customers who feel more protected are more likely to stay loyal.

Turning exposure into empowerment

Given the broad exposure of credentials, telecom providers must accept a new reality: Most customers are vulnerable to downstream fraud — whether or not the breach occurred within the telecom's ecosystem. While fraud isn't inevitable, ideas about the telecom's role in customer protection must evolve.

Through proactive fraud prevention strategies, providers can meaningfully shield customers from the effects of compromised identities. This strengthens the provider's competitive positioning by building trust, which deepens customer relationships.

Proactive protection is also a fraud containment strategy. By recognizing the downstream risks of breached credentials, telecoms better prevent further attacks and limit the cascading damage that often follows successful ATO attacks.

What does proactive protection look like? A multipronged approach is best, particularly when it includes:

Timely, actionable alerts. Alerts notify customers when their personal information may be at risk. The timeliness of the information enables them to take corrective action while there's still time to reduce damage. Such mitigation can include freezing credit, changing passwords, or warning their telecom provider or financial institution before an account takeover or fraudulent transaction occurs. For these alerts to be effective, they must be clear and actionable. The information presented to customers should be easy to understand, with guidance about the steps they need to take. This empowers customers to act quickly and decisively — making them active partners in the telecom's fraud prevention efforts.