neuroID

A part of experian

Report

The imposter in the session:

An investigative look at the fraud rings abducting your customers' accounts.

Volume 1: The hub and the hive

Table of contents

Fraud rings are as structured and organized as the businesses they attack. Each member has a defined role, and together they execute attacks tailored for their targets and designed for maximum efficiency.[1] Often, they follow detailed playbooks that outline every move.

These playbooks — often sold as toolkits on the dark web (like this 13-page how-to guide) — contain everything fraudsters need: stolen credentials, VPN instructions and step-by-step guidance for bypassing defenses. They're created and sold by the world's largest fraud organizations, then purchased and executed by smaller rings or lone actors. Some rings focus on specific fraud types, including account takeover (ATO), while others diversify and attack in multiple ways.

The stakes are high for businesses. In 2025, 71% of of surveyed banks, credit unions, and fintechs across the US identified fraud rings or financial criminals as the source of attempted fraud.[2] ATO losses reached **$16 billion in 2024**, with attacks growing **24% year-over-year**.[3] Multi-factor authentication (MFA), once considered a gold standard, is now being exploited at scale through strategic ATOs, phishing kits, token theft[4] and prompt bombing.[5] Fraud rings thrive in this environment because they use businesses' defenses to their advantage, exploiting vulnerabilities with sophisticated, coordinated attacks.

This report series flips the script. Using real, anonymized client ATO attacks, we'll reveal what these fraud rings' playbooks look like in action. You'll see the roles fraudsters assume, the signals that expose their coordination and how to stop them before a single compromised account becomes a chain reaction.

In this edition, we examine an attack on a leading peer-to-peer payments provider (>$1 billion in net assets and millions of customers) — a business where account sharing is common, but unauthorized takeovers can be costly. The difference between a legitimate shared account and a fraudster-controlled one is razor-thin. By connecting the dots from a seemingly routine login attempt, we uncovered a fraud ring in motion and shut it down before it scaled. Here's what it looked like:

How NeuroID spots fraud rings in action

NeuroID, a part of Experian, uncovers fraud rings using three layers: **persistent device recognition, IP intelligence and behavioral intelligence**. We recognize devices we've seen before, with 99.5% accuracy, determining its approximate location and assessing behavioral patterns in the process. If a device appears in different location than was associated with the account and the user's behavior at a login has been seen before but not on that account, it signals that device may be part of a coordinated attack.

When risk spikes, **we collaborate with our customers to investigate**. We map connected devices and accounts first, then layer in masking signals like VPNs, proxies, Apple relays and GPS spoofing, and finally analyze intent: Are users navigating with unusual precision, copying credentials or repeating steps across accounts? We pull these layers into network graphs to reveal the size and sophistication of the attack. While fraud rings continue to spoof networks and devices, behavior remains the hardest to fake at scale — making it the ultimate safety net against ATO rings like this one.

1. Routine or risky?

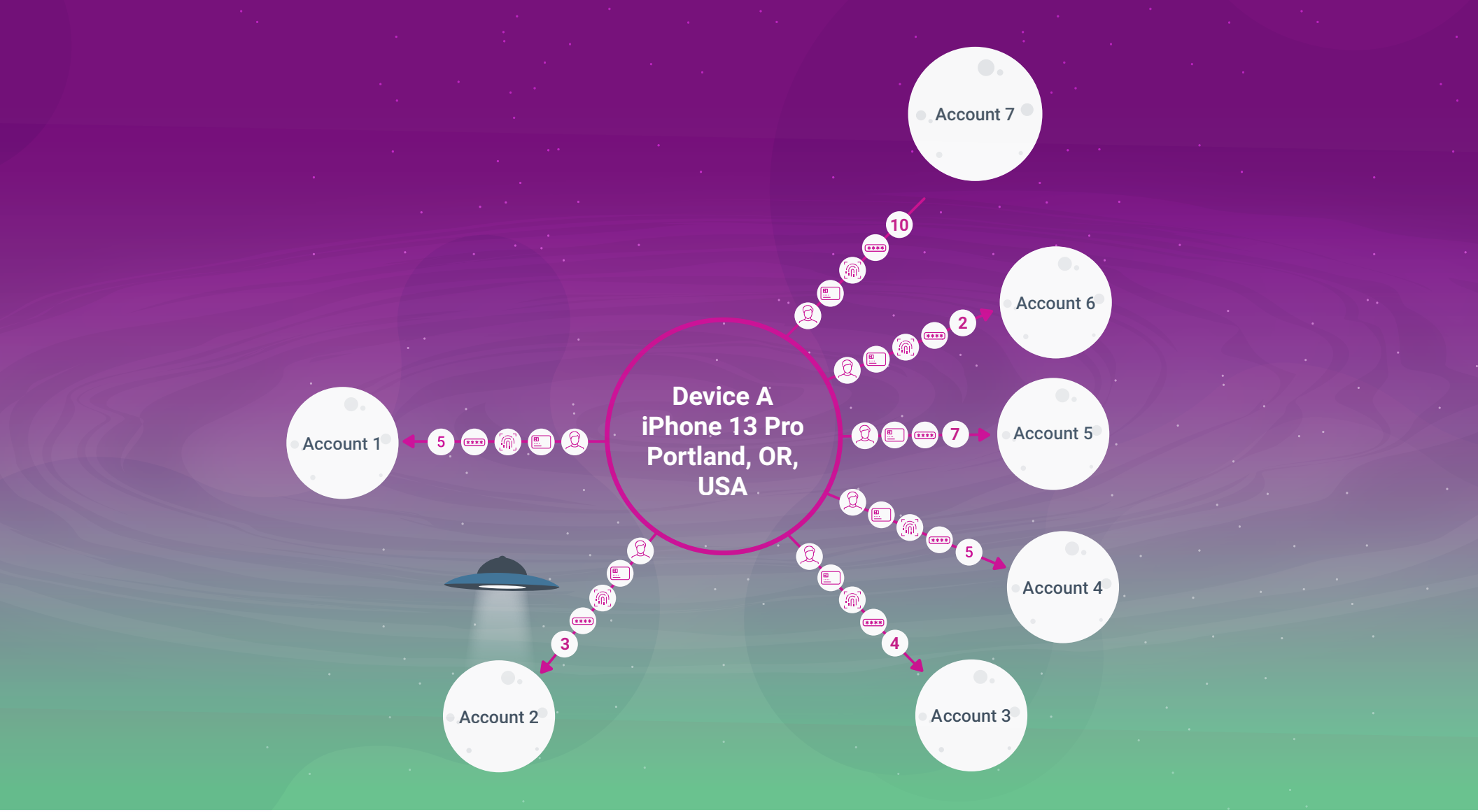
First, let's zero in on what looks like a typical login. **Device A** accessed **account 1** (shown right) using both password and biometric authentication — five successful logins during one billing cycle (30 days) without being flagged by any other tools in the payment provider's fraud stack. Within that billing cycle, they also added a new payment recipient and payment card. In isolation, these actions appeared legitimate; there was no reason for the payment provider to stop this user.

But device A wasn't the only one accessing account 1, and account 1 wasn't the only account they were logging into. Through behavioral analytics and device and network intelligence, NeuroID's Account Defense identified device A as highly risky immediately and began to trace its activity.

The picture shifted from a routine login to a highly coordinated attack. This login wasn't the start of the attack, but it was a critical pivot point — one that could have escalated into something far bigger if left unchecked.

$16 billion
account takeover losses in 2024

24%
year-over-year growth in ATO attacks



2. An imposter in action

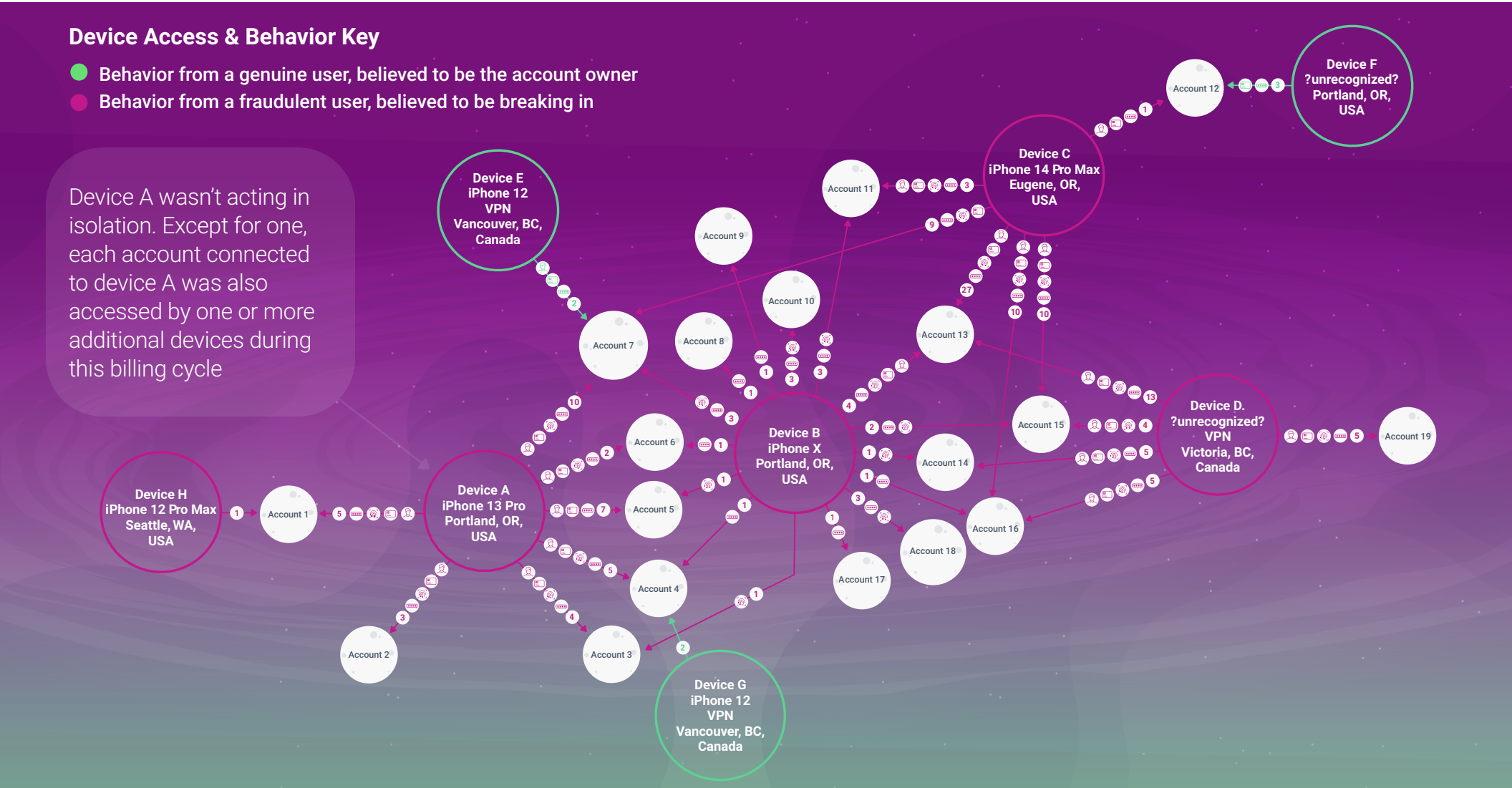
Device A kept coming back — and NeuroID kept recognizing it. We linked device A to six additional accounts over 30 days. When we did, its login to account 1 didn't look so harmless.

Across the seven accounts device A logged in to, its actions were consistent: multiple logins, successful authentication with both password and biometrics (a fingerprint, in this case), followed by adding a new payment recipient and card. What initially appeared to be a user returning to their account was, in reality, a fraudster systematically exploiting multiple profiles.

3. Revealing the ring

Device A wasn't acting in isolation. Except for one, each account connected to device A was also accessed by one or more additional devices during this billing cycle. Each device was located in the same area, Portland, Ore., signaling that this attack was carried out by a localized group that potentially knew each other outside of the digital world.

As we traced the connections, a clear hierarchy of an organized operation emerged:



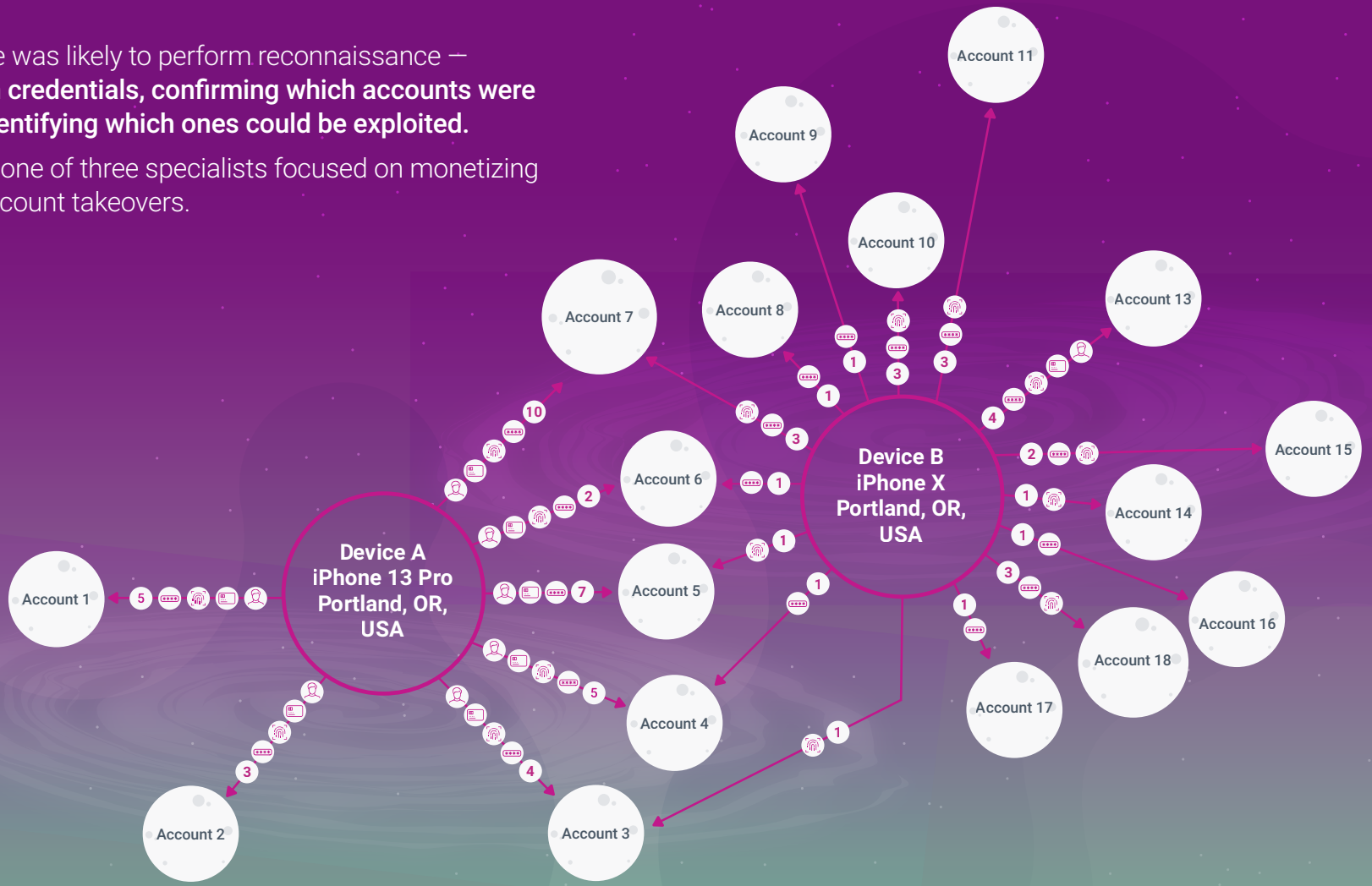
The Ring Leader: Device B

At the center of this ring was **device B**. Unlike device A, device B didn't linger in accounts or make changes. Its actions were minimal: one or two logins per account, typically using only a password. There were exceptions, but rarely did device B establish a biometric or alter account information.

Device B was the catalyst for the attack. It logged in to 14 accounts during the billing cycle, creating a web of connections that linked around a dozen compromised profiles back to this single hub. Based on its relatively light-touch interactions with its accounts, device B's role was likely to perform reconnaissance — testing stolen credentials, confirming which accounts were active and identifying which ones could be exploited. Once credentials were validated, device B passed them along to others, including device A, to carry out the rest of the attack.

Device B's role was likely to perform reconnaissance — **testing stolen credentials, confirming which accounts were active, and identifying which ones could be exploited.**

Device A was one of three specialists focused on monetizing successful account takeovers.



The monetization experts: devices A, C and D

The accounts tested by device B were distributed across three devices: **devices A, C and D**. These three devices appeared to be the execution arms of the operation. Their behavior was strikingly similar across different accounts, following the same procedural steps as device A:

Step 1: Multiple successful login with a password

Step 2: Successful biometric authentication

Step 3: Addition of new payment recipients and cards

These steps were deliberate actions designed to cement control over the account. Many fraud mitigation processes look at login history — how many times a device has accessed an account — to determine trust. By logging in repeatedly, devices A, C and D established themselves as the trusted device associated with the profiles they targeted. Adding biometric authentication was the next layer of entrenchment: Once the fraudsters' own biometrics were tied to an account (or bypassed in another manner), they could act as the account owner, accessing and changing profile information needed for monetizing the attack.

Each monetization expert tried to maximize their ATO efforts before the end of the billing cycle — when the accounts' true owners would be issued statements full of fraudulent transactions. On some accounts, the real owner did log in at some point during the billing cycle, but much less frequently than the fraudsters (see **account 4**). Most of the targeted accounts were only accessed by the fraud ring, though; their real owners never logged in to see what was happening to their accounts.

The monetization experts seemed to work on a distinct set of accounts, minimizing overlap and reducing the risk of detection. But nearly every account they touched began with device B's testing.

The monetization playbook

Step 1: Build a login history

Fraudsters start by logging in to the target account repeatedly — often more than the real owner. This creates history and trust between their device and the account.

Step 2: Take over biometric authentication

Once inside, the fraudster either sets up their own biometric authentication or bypasses it in another way (see page 8). With control over this step-up authentication, they're able to take further actions on the account.

Step 3: Add payment cards and recipients

Now able to edit profile information and complete transactions, the fraudster adds stolen cards and new payment recipients. These accounts become channels to move money to themselves or other members of the fraud ring.

The playbook behind the attack

While this fraud ring was only connected to 19 accounts, its highly coordinated effort likely made it highly profitable for the time investment. Defined roles allowed the ring to operate efficiently: **Device B** as the hub, validating credentials and distributing targets; **devices A, C and D** as specialists, focusing on a smaller batch of accounts to execute and monetize takeovers. It's likely that this small fraud ring's attack plan came from a much larger organization. Most of the accounts the ring accessed were established in Vancouver, Canada, with the ring members consistently using VPNs to place themselves in Canada rather than their true location (Portland).

These actions, combined with the structured nature of the attack and the consistent actions across the execution devices, suggest the use of a fraud attack playbook. This playbook would have contained instructions for verifying account credentials and login thresholds for triggering biometric enrollment. It's also possible that the playbook included a toolkit, complete with batches of stolen data and payment cards — in this case, from Canadian consumers — plus instructions for using VPNs, proxies or GPS spoofing to avoid detection.

Playbooks like this retail for as low as $50[6]. Even if they didn't use a playbook, valid credentials can be as low as $30[7] and MFA relay can be as low as $15.

Meanwhile, on average, each successful ATO costs this payment provider $300 in fraud losses. If this fraud ring managed to monetize all 19 accounts they touched, that could mean at least $7,500 in losses from this attack during a single billing cycle.

At an average cost of $45 per account and an average profit of $300, this menas an ROI of 566% per account. While we analyzed this behavior over a billing period, their total time investment could have been just a few days — a highly profitable scheme, and very likely to be repeated.

A dark web marketplace in action?

Because of this group's proximity to each other and coordinated efforts, we're inclined to believe this was a single fraud ring capitalizing on data they'd already purchased. But it's possible that the central hub — device B — was testing credentials with the intent of selling them, and devices A, C and D were individual buyers executing attacks with the small data batches they purchased.

It's nearly impossible to confirm exactly what happened. But it's clear that this was a group of bad actors accessing accounts they shouldn't have, and that letting it go unchecked could cause major losses and allow the attack to grow even larger.

How fraudsters beat biometrics

Biometric authentication is viewed as a reliable defense against ATOs. But in coordinated ATO attacks like this, fraudsters bypass it in multiple ways:

Establish, reset, or bypass: Once a fraudster's device is associated with an account, they can often establish new biometric authentication, reset the existing biometric authentication or bypass it entirely by switching to another form of step-up authentication, like MFA.

Social engineering: Attackers manipulate legitimate users into authorizing access — often through scams or phishing — and may use remote access tools to take control of legitimately authenticated sessions.[8]

AI: Fraudsters use AI to generate synthetic biometric data, like deepfake facial images or voice clones, that mimic legitimate users well enough to fool systems relying on facial recognition, voice ID or fingerprint matching.[9]

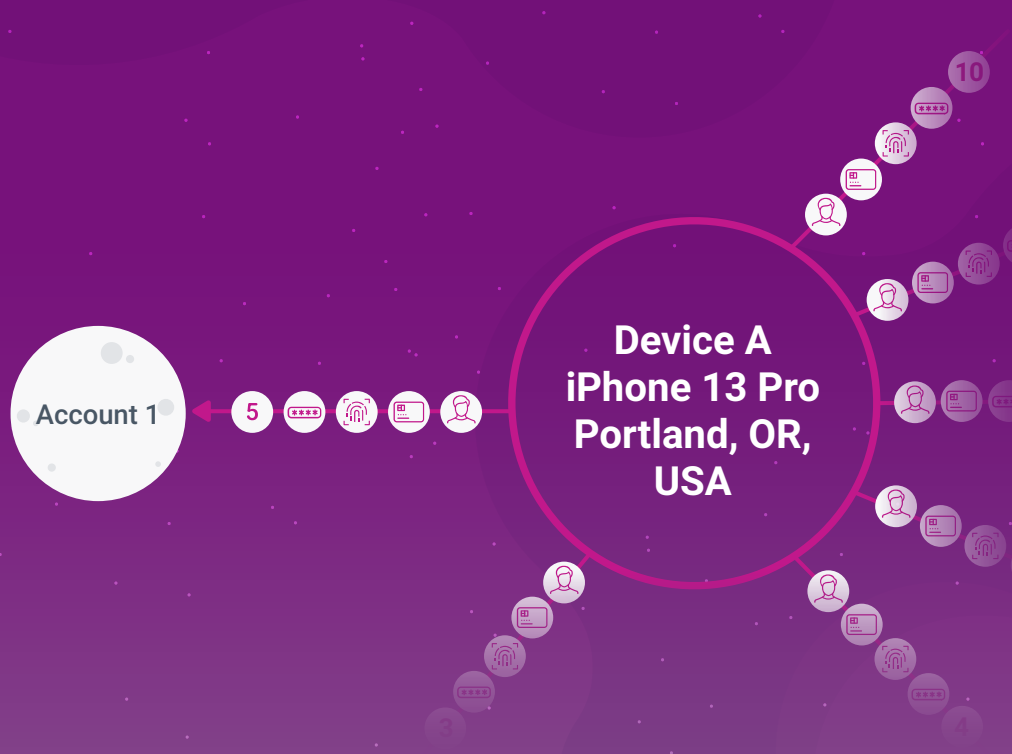
4. Unmasking the imposter: revisiting device A

At first glance, device A's login to account A looks routine. But by tracing device A's activity across accounts and connecting it to devices B, C and D, an organized fraud ring — and a coordinated effort to monetize compromised accounts — revealed itself.

Device A's actions (along with the other monetization experts, devices C and D) exposed weaknesses in the point solutions typically used to prevent ATOs. Many businesses use device and network data as their first line of defense to protect accounts. In this case, the fraudsters made a coordinated effort to establish trust with their devices. Once they did so, every other defense became vulnerable: The fraudsters could bind their identity to the account through biometric enrollment and likely establish their device as the MFA device, allowing them to bypass defenses as they modified account details.

Together, this ring executed a playbook that took advantage of specific point solutions and could scale rapidly if left unchecked. Blocklisting one execution device wouldn't have stopped the attack; the others would have continued without interruption. The only way to dismantle this ring — stopping this attack and preventing the ring from targeting another batch of accounts during a different billing cycle — was to trace it back to its source and blocklist all devices involved. For this payment provider, NeuroID's link analysis gave them the confidence to comfortably blocklist this fraud ring's devices.

If this attack hadn't been stopped, it could've grown exponentially. Account 1 was one of the few accounts device A accessed that wasn't connected to the hub of the attack. This may have been an example of device A testing credentials, on the verge of becoming a hub itself. Larger attacks often include multiple hubs; by stopping this one in real time, the payment provider potentially prevented this attack from growing into one such case.



The only way to dismantle this ring — stopping this attack and preventing the ring from targeting another batch of accounts during a different billing cycle — was to trace it back to its source and blocklist all devices involved.

5. Stopping attacks at their source

In attacks like this, MFA, biometrics and similar point solutions fail because they treat risky logins as individual events, not part of a coordinated effort. As scams grow more effective and ATO tools more accessible, we've seen an increase in incidents where step-up factors are compromised.

NeuroID looks at attacks differently. Through behavior-based fraud detection and link analysis based on best-in-class persistent device ID, NeuroID exposes and stops ATO attacks of all kinds. Whether it's an individual risky login or a coordinated fraud ring, we don't just stop a login — we shut down the infrastructure that makes attacks like this possible.

Want to see more fraud ring playbooks in action?
Stay tuned to your email for the next installment in this series, and visit neuroid.com to learn more about NeuroID's ATO protection.

With NeuroID, this payment provider saw:

2X
fraud detection at login

56X
lift in chargeback prediction

$1M+
in annualized savings

1. Fraud Ring Glossary, FraudNet
2. Alloy 2025 State of Fraud Report
3. Beyond the Breach: Account Takeover Data & Insights, Sift, 2024
4. How Hackers Bypass MFA, And What You Can Do About It, Forbes, 2024
5. MFA Fatigue Attacks, UChicago, 2024
6. What We Learned From Infiltrating 22 Credential Stuffing Crews, Kasada, 2025
7. Dark web price index, Privacy Affairs, 2023
8. Social Engineering, Carnegie Mellon University
9. How AI will disrupt fraud prevention & detection technologies, Thomson Reuters, 2024