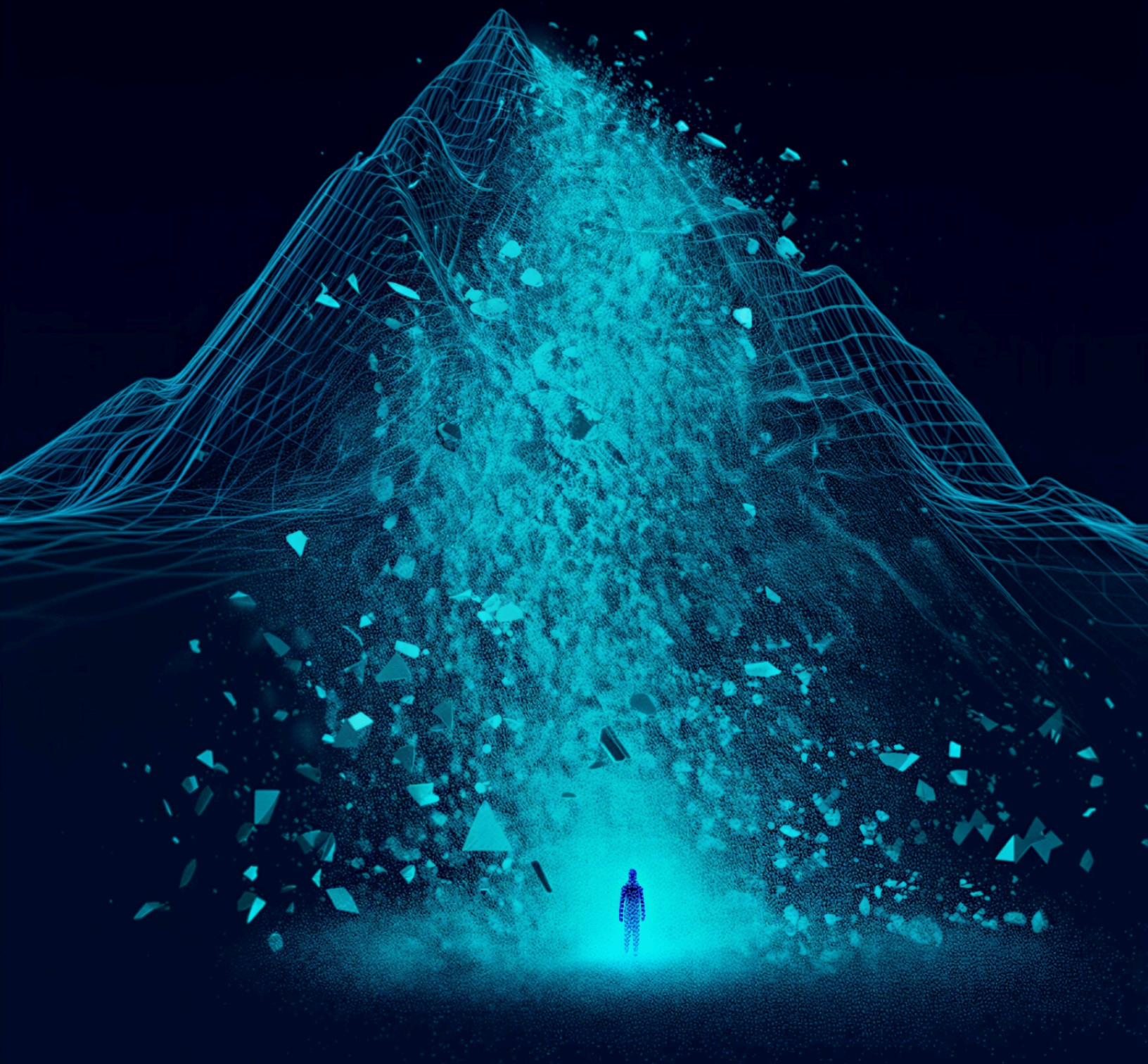
REFINE
INTELLIGENCE

AI-Powered Bank Impersonation

Emergency Response Playbook



The Situation

If your call center is suddenly flooded with panicked customers reporting fake fraud alerts, and your alert queue is spiking with high-value transfers, take a deep breath.

You're under a state of the art AI-driven Account Takeover (ATO) campaign known as Bank Impersonation or Call Spoofing Attack.

You need to respond fast.

Your traditional defenses rely on relationship managers, the operations team or your fraud investigators calling customers to verify suspect transfers. This won't work here - the attack is deliberately designed to saturate these defenses by attacking hundreds of customers at once. You simply don't have the capacity to use your routine operational cadence, and meanwhile money is leaving the bank at an alarming speed straight into criminal hands.

Instead, immediately slow down high-risk transfers, contact your digital app provider for an urgent conversation about controls they might offer, and rapidly deploy automated digital verification so your customers, rather than your team, will be able to clear the alert backlog.

Here is your step-by-step operational guide to surviving a bank impersonation attack, even if it caught you completely unprepared.

You Are in an "Avalanche"

Let's quickly understand what's happening:

- Bank impersonation attacks are no longer simple, isolated scams; they are massive, mechanized ATO campaigns. Fraudsters simultaneously attack hundreds of your customers using spoofed phone numbers that match your bank's legitimate caller ID.
- Once trust is established over the spoofed call, criminals direct the victim to a fake website, harvest their credentials, log into the account, and execute high-value transfers to new beneficiaries. And nowadays they can automate the entire thing end-to-end using AI.

Pull this manual and execute the following steps.

Immediate Triage: Minutes 0 to 60

Your first goal is to stop the bleeding. You must create intentional friction into your payment flows to buy your operations team time.

Step 1: Throttle High-Risk Payments

While you set up additional controls, you must immediately limit high-amount transfers to new beneficiaries, especially if they are originating from a new device (assuming you have visibility into device data). You cannot manually review every transaction during a flood, so establish strict payment-slowdown protocols:

- Predefine criteria for routing suspect wire and ACH transfers out of the automated payment queue and into a mandatory manual review path.
- Ensure that your treasury and retail operations teams are aligned to execute these holds without getting bogged down in internal approvals.

Step 2: Contact Your App Provider Immediately

Your core processors and online banking vendors are your first line of defense. Call them immediately to execute the following emergency actions:

- Slow Down Suspect Payments: Work with them to ensure that the payment-slowdown routing discussed in Step 1 is technically enforced at the application level.
- Display an In-App Emergency Message: See if a message can be displayed to customers directly inside the mobile banking app. This message should advise them that their transfer has been slowed down, will need to go through a verification process, and that they must call their branch only from a verified number the bank has on record.
- Request Data Feeds: Ask the app provider what real-time data they can feed directly into your transaction monitoring tool, so you can tweak rules accordingly. Ideally they'll be able to give you visibility into post-login behavior, including events such as changes to passwords, emails, phone numbers, the addition of new parties, or alterations to the account's notification policy.
- Ask your provider about activating additional controls like advanced device intelligence or behavioral biometrics. However, be mindful that some of these controls require building a behavioral profile of the user over time, so they may not be able to help you immediately with this specific wave of attacks.

Filter the Avalanche: Hours 1 to 24

Once the immediate bleeding is slowed, you must start thinking about one thing only: what do you do with all the suspect transfers? How do you clear the queue? During a mechanized attack, your manual review capacity will physically break down, so you'll need to do two things: reduce the number of alerts as much as you can, and verify the suspect transfers using an automated tool.

Step 3: Hyper-Focus Your Alert Rules

Tighten your alerting rules to filter the flood. Do not rely on single data points; instead, combine anomalies to isolate the highest-risk activity.

- Rule Intersection: Configure rules to flag a transaction only if it involves a new beneficiary AND a high dollar amount AND a new device, if that is feasible.
- Velocity Checks: Implement strict velocity rules to flag accounts attempting multiple transfers in an unusually short timeframe.
- Account Maintenance Precursors: Attackers often alter account details before moving money to lock the victim out. Treat rapid changes to contact info or the sudden addition of a joint account holder as a giant red flag.

Step 4: Start Clearing the Queue

It's going to be tough, and you'll need full cooperation across the bank, but now that you've narrowed down the alerts to a minimum, you need to start clearing the queue. Start by releasing payments that have been slowed and do not trigger your narrow-down rules. Those are safe to release.

Now comes the hard bit: you can't call all these customers to verify suspect transfers. There are so many reasons why this won't work: The entire attack is based on 'the bank is calling to verify a possible fraud' scenario; response rate for phone calls is at an all-time low, yielding 25% verification rate in a good day; your relationship managers and operations team don't have the capacity to go through the entire queue manually; and attackers might use line saturation tactics to make sure you can't really talk to your customers while their accounts are being emptied.

It will create more friction, but the best strategy for day 1 of the attack is to encourage customers whose transfers have been slowed down to contact the branch so their transfers can be checked and released - but this has to be done really carefully. A callback to a number on record that has NOT been recently altered is your best safeguard against calling the criminals.

Deploy Automated Defense: Days 2 to 5

The attack will continue - the fraudsters will still have a lot of potential targets. You can't keep your branch and operations team as your fraud department deputies - and you cannot hire enough staff to manually review hundreds of suspect transfers in a single day. You must scale your operations instantly to survive this avalanche of fraud.

Step 5: Set Up Automated Digital Verification

To clear the backlog of slowed payments, you should bypass the phone network entirely. Set up automated verification - technology such as Refine Intelligence can do that. Banks that switch from manual phone calls to automated customer outreach see their response rates jump from a dismal 25% to an incredible 84%.

This means automatically verifying suspect transfers using multi-channel, secure digital outreach.
If the right resources are aligned, setup time can be very quick, as no core integration is needed.

By utilizing automated outreach you can orchestrate an intelligent response:

- Utilize Branded Messaging: Engage customers through next-gen branded messages, rather than regular text messages. Supported by Apple, Google and all major carriers, it's now possible to send branded messages featuring a "verified sender" identity and the bank's official logo. This gives the customer visual proof that the message is real - something criminals cannot easily fake.
- Execute Multi-Party Outreach: Contact all valid parties on the account simultaneously. Criminals cannot intercept multiple channels across multiple users unless they have compromised everything.
- Avoid the Attacker: Ensure the automated program actively prevents outreach to newly added parties or recently changed phone numbers and email addresses, cutting the attacker out of the verification loop.

Step 6: Remove Temporary Controls and Restore Operations

Once you have successfully set up automated verification of transfers, you will be able to remove rigid transaction controls. When an automated system is handling the verification, suspect wires can be cleared efficiently without requiring blanket hold policies.

About This Guide

This guide was prepared by Refine Intelligence. At Refine we understand that AI-powered attacks operate at machine speed; you can't defend against them using traditional processes.

If you're under attack, or would like to prepare for one, we're happy to provide more information. Get a briefing from one of our experts today.