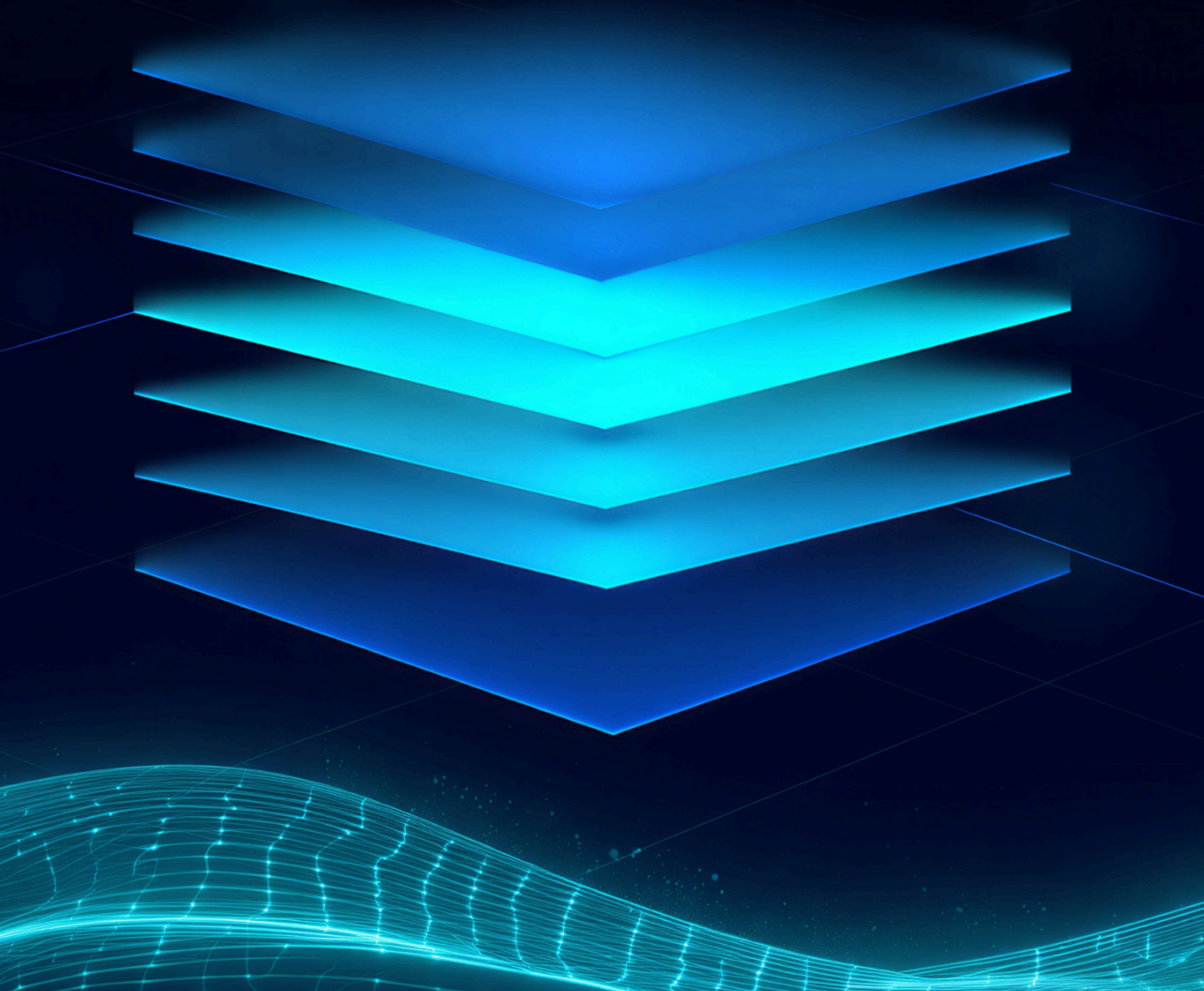
REFINE
INTELLIGENCE

How to Prepare for an

# AI-Powered Bank Impersonation Attack

A 7-Step Playbook



## Bank Impersonation Attacks: Fighting an Avalanche

Bank Impersonation attacks aren’t new, but recent developments in AI have made them an extremely severe threat - especially if you’re a small FI.

Criminals now view midsize banks, regional banks and especially community banks and credit unions as soft targets, knowing they possess limited operational capacity and smaller manual review teams. By using AI to automate spoofed phone calls, attackers can bombard hundreds of your customers simultaneously.

Once trust is established via a spoofed caller ID, victims are engaged by completely autonomous AI agents or, in some cases, criminals using deepfake tech. Once credibility is established, the victim is directed to fake sites where their credentials are stolen, including one-time-codes. Once inside, the criminals engage in transferring funds, often preceded by changing the account's password, email, and/or phone number. They would frequently add a new party to the account so they can easily answer callbacks or OTP checks, and disable notifications for other parties. The transfer itself will be a high-value wire, ACH, RTP or Zelle to new beneficiaries
By the time your operations team realizes you are under attack, you are already drowning in an avalanche of alerts.

## Prepare for a Massive Attack: The 7-Step Prep Playbook

Since you cannot build your defenses in the middle of a crisis while money is actively leaving the bank, it’s best to prepare. To safeguard against mechanized Account Takeover (ATO) bank impersonation call spoofing campaigns, risk and fraud leaders should consider implementing these seven operational priorities immediately.

| Steps 1-4 | Beef up your detection to make sure you minimize alerts during a full-scale attack |
|---|---|

### 1. Align Closely with Processors and Digital Vendors

Community banks rely heavily on third-party online banking providers and core processors. Your vendors are your first line of defense, but their controls won’t work if they aren't properly configured before an attack hits. Your best course of action is to engage with them proactively to understand exactly what fraud controls are available.

**Actionable Steps & Questions to Ask Your Vendors:**

- Surge Capacity: "What is your Service Level Agreement (SLA) and surge-capacity support if we experience a 1,000% increase in alerts in a 24-hour window?"
- Control Activation: "Which device, behavioral, and account-monitoring tools are currently enabled, and which ones require an additional license or setup time?"
- Remote Access Detection: "Do you have the capability to detect if a session is being driven by remote desktop software or screen-sharing applications?"
- Data Visibility: "Can we access real-time data feeds of post-login customer behavior to feed into our own internal fraud models?"
- Some providers may offer tech that safeguards the main bank number against spoofing. These services add the bank’s name in the beginning of calls coming out of the real phone number, and a warning about possible scam for calls coming out of other numbers that masquerade as the real number. It cannot protect against a spoofing attack where one of the digits was changed to evade the check - but it can limit the impact of call spoofing. Other services look for copycat bank websites and protect the bank’s brand.

## 2. Tighten Alerting Rules

During an automated attack, your fraud queue will explode - regardless of what monitoring system you use. You cannot manually review every transaction, so your alerting rules must be hyper-focused to filter the flood and isolate the highest-risk activity. Many regional and community banks use a combination of stand-alone transaction monitoring systems and controls offered by their processor or app provider. It’s important to align both - for example, make sure device information is passed on to your transaction monitoring system.

**Actionable Steps & Questions to Ask Your Team:**

- Rule Intersection: Do not rely on single data points. Combine anomalies. For example, configure rules to flag a transaction only if it involves a new beneficiary AND a high dollar amount AND a new device.
- False Positive Management: "What is our current false positive rate on wire/ACH alerts? If the alert volume is 10x tomorrow, at what point does our manual review process physically break down?"

- Velocity Checks: Implement strict velocity rules. Flag accounts that attempt multiple payment transfers in an unusually short time frame.

### 3. Monitor Account Maintenance Activity

Attackers almost always alter account details before they initiate a money transfer. They do this to intercept one-time passcodes and lock the legitimate customer out of the account. You must treat rapid changes to account maintenance data as giant red flags indicating a potential ATO.

**Actionable Steps & Questions to Ask Your Team:**

- Precursor Tracking: "Are we alerting on password resets, phone number changes, and email updates before a transaction is even initiated?"
- Cooling-Off Periods: "Do we enforce a mandatory cooling-off period (e.g., 24 to 48 hours) for high-value transfers immediately following a change to a customer's primary phone number or email address?"
- Authorized Users: Flag the sudden addition of new authorized users or joint account holders, particularly if followed quickly by a transfer request.

### 4. Implement Behavioral Biometrics and Device Intelligence

If your app provider supports it, behavioral biometrics and advanced device intelligence are another way to reduce false positives. Because attackers use stolen credentials, the login may look legitimate, but *how* they interact with the digital banking app will expose them. They'll also use MVNO, rent-a-phone, SIM Swap, or operating an eSIM farm - and there's tech to detect that. Note that the signal must come from the app provider, so you need to ask them whether they provide this data.

**Actionable Steps & Questions to Ask Your Team:**

- Behavioral Deviations: "Can our systems detect uncharacteristic typing speeds, pasting of credentials, or abnormal navigation patterns?"
- Can the app provider pass on indications of remote access (where the criminal asks the victim to install a tool allowing remote support)? This would bypass device controls, so if available can spot fraud cases that circumvent device intelligence.
- Can the app provider spot MVNO, rent-a-phone, eSIM or SIM swaps

| Steps 5-6 | Automate alert resolution so you don't rely on frontline or operational teams during a full-scale attack |
|---|---|

## 5. Establish Payment-Slowdown Protocols

Time is your best weapon against an automated attack. Because criminals are using AI to move funds in seconds, you must build intentional friction into your payment flows to buy your operations team time to verify the transaction digitally. It's much better to slow down a fraction of the transfers and verify them automatically, than rely on the limited capacity and human speed of your relationship managers, call center or operations teams.

**Actionable Steps & Questions to Ask Your Team:**

- Manual Review Routing: "What are the exact criteria for routing suspect wire and ACH transfers out of the automated queue and into a manual review path? How is that routing technically handled by your payment and monitoring stack?"
- Hold Authority: "Who has the authority to place temporary holds on high-risk outgoing payments, and is that authority delegated properly to avoid bottlenecks during a crisis?"
- Message to Customer: "Can we present a real-time message to the customer in the digital app if their transfer has been slowed down for inspection"?
- Regulatory Balance: Ensure your slowdown protocols comply with regulations. Slowing down a payment for 24-48 hours to prevent severe fraud is generally acceptable, but your compliance team must document the justification to avoid regulatory scrutiny.

## 6. Build Automated, Multi-Channel Verification

This is the most critical step: You must stop calling customers over fraud. Human outreach is too slow, and it puts customers in a low-signal environment where criminals have the advantage. You should move your fraud verification into automated, multi-channel digital outreach. Companies such as Refine Intelligence are offering such capability and banks report 84% response rates and virtually unlimited capacity, far exceeding any performance by frontline or ops.

**Actionable Steps & Questions to Ask Your Team:**

- Automate verification: “Can we set up automated verification that triggers when a suspect transfer is slowed down for review, releasing it when verification is completed?”
- Adopt branded messaging: “Can we engage customers through branded messaging with verified sender identities, giving customers visual proof that the message is real - something criminals cannot fake?”
- Multi-Party Outreach: "Are we reaching out to all valid parties on the account simultaneously?" Attackers cannot intercept multiple channels across multiple users unless they have compromised everything.
- Avoid contacting the wrong parties: "Does the program automatically prevent outreach from newly added parties or recently changed phones/emails, and what control do we have over the cooldown period?”.

| Step 7 | While prior steps are practical controls, this one is perhaps the most important. |
|---|---|

## 7. Secure Executive Support & Cross-Functional Alignment

A massive spoofing attack is not just a "fraud department problem" - it is an enterprise-wide crisis. When an attack hits, it triggers a chain reaction across the entire institution. Without executive mandate and cross-functional alignment, your response will be paralyzed by organizational silos, and your only remedy might be draconic controls that severely limit the normal course of business.

**Actionable Steps to Drive Alignment:**

- The Executive Mandate: The C-Suite should be provided with clear analysis of the potential impact of mass-scale bank impersonation attacks, presented with potential impact analysis, and asked for a budget to handle preparations. They should also mandate cross-team alignment.
- Call Center: Your call center will be the first to drown in angry, confused customers reporting fake alerts. They may need capacity increase through AI agents capable of verifying transfers automatically, otherwise they may not be able to handle volumes.
- Retail & Treasury: These teams oversee the actual movement of money. They must be aligned with Fraud Operations to instantly execute the

payment-slowdown protocols without getting bogged down in internal approvals.

- Digital Teams: The digital and IT teams own the online banking app and mobile communication channels. They need to be looped in during any conversations with the app providers and setting up automated customer-facing verification.

## Scale Your Operations with Refine Intelligence

When an AI-powered spoofing campaign hits, your traditional manual controls will be instantly overwhelmed. You need technology that matches the speed and scale of the attack. Many banks use Refine Intelligence to automate their alert resolution process. By utilizing automated, user-friendly digital inquiries across secure, branded communication channels, Refine helps institutions shift the focus away from ineffective phone calls.

Refine's adaptive, AI-driven digital questionnaires are highly effective for stopping Account Takeovers, Check Fraud, and Scams.

Banks leveraging the Refine automated outreach achieve an **84% customer response rate**. They turn 10-minute manual investigations into 1-minute alert resolutions, giving critical time back to their frontline team and stopping fraud before the money leaves the bank.

**Stop calling customers. Start automating.**
**Get a Demo of Refine Intelligence Today.**