REFINE
INTELLIGENCE

A Guide to Effective Fraud Banners in Online Banking

Introduction

In today's digital banking environment, financial institutions are working harder than ever to protect their customers from increasingly sophisticated attacks. A quick glance at most financial institution's homepage or mobile app today will reveal a "Be Aware of Fraud" section and, in many cases, a pop-up banner that takes a very central stage - essentially the first thing a customer sees as they enter the site or app.

These banners serve a positive purpose: raising awareness. Any step taken to educate the public is a step in the right direction, and no alert is a wasted effort. However, communication is a constantly evolving practice, and there are always ways to optimize our messaging to ensure it is as helpful and empowering as possible.

To discover the best ways to guide customers, we conducted a comprehensive review of the current landscape. We analyzed exactly 88 different bank fraud alert banners actively deployed across various US-based financial institutions to understand the different approaches to customer education.

In this post, we will explore the top tactics banks are currently warning their customers about, introduce a positive framework for evaluating and refining alert messaging, and provide a helpful blueprint to ensure your institution's alerts are delivering maximum value.

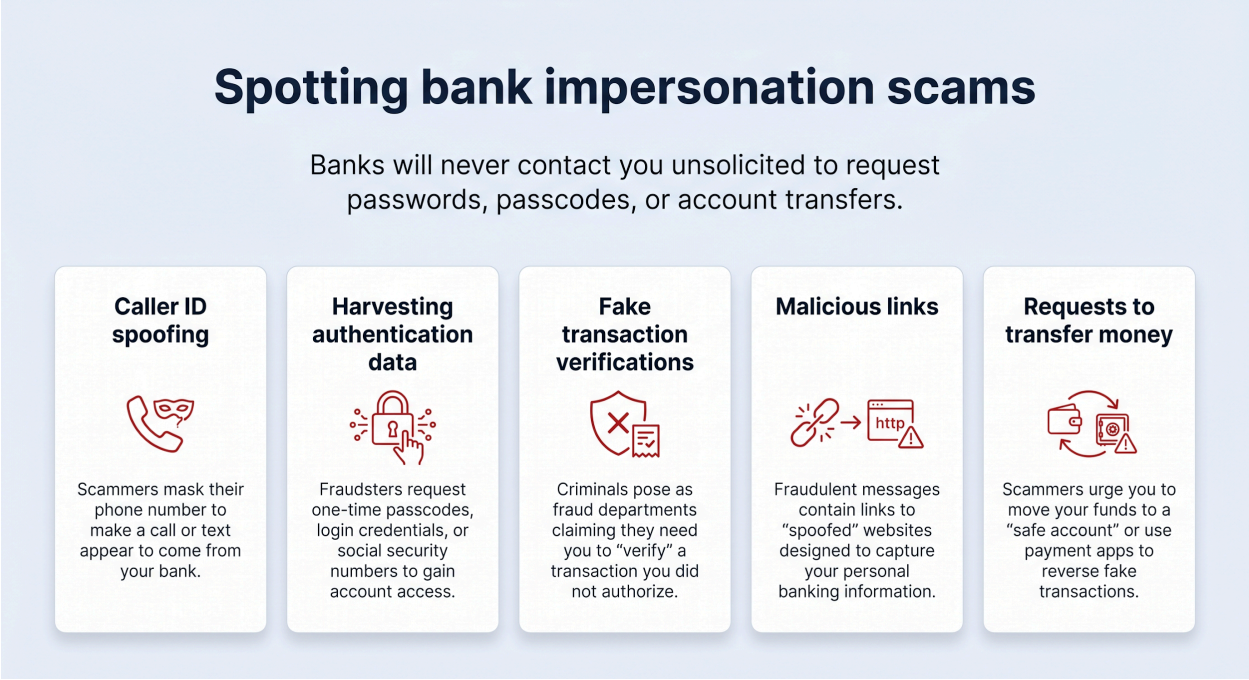
The Threat Landscape: 5 Main Tactics

Before looking at how we communicate, it is helpful to look at what banks are currently communicating about. Across the 88 alerts we analyzed, institutions are doing a great job of highlighting five primary tactics utilized by modern fraudsters:

1. **Caller ID Spoofing & Impersonation:** Scammers are successfully manipulating telecommunications networks to make the bank's actual, legitimate phone number appear on the customer's caller ID. Alerting customers to this helps bypass their natural trust in caller ID.
2. **The Hunt for Authentication Data:** Scammers often have a customer's phone number, but they need the "keys to the kingdom." The best alerts remind customers that a legitimate bank representative will *never* ask for online banking

passwords, PINs, full debit card numbers, Social Security Numbers, or One-Time Passcodes (OTPs) sent via text.

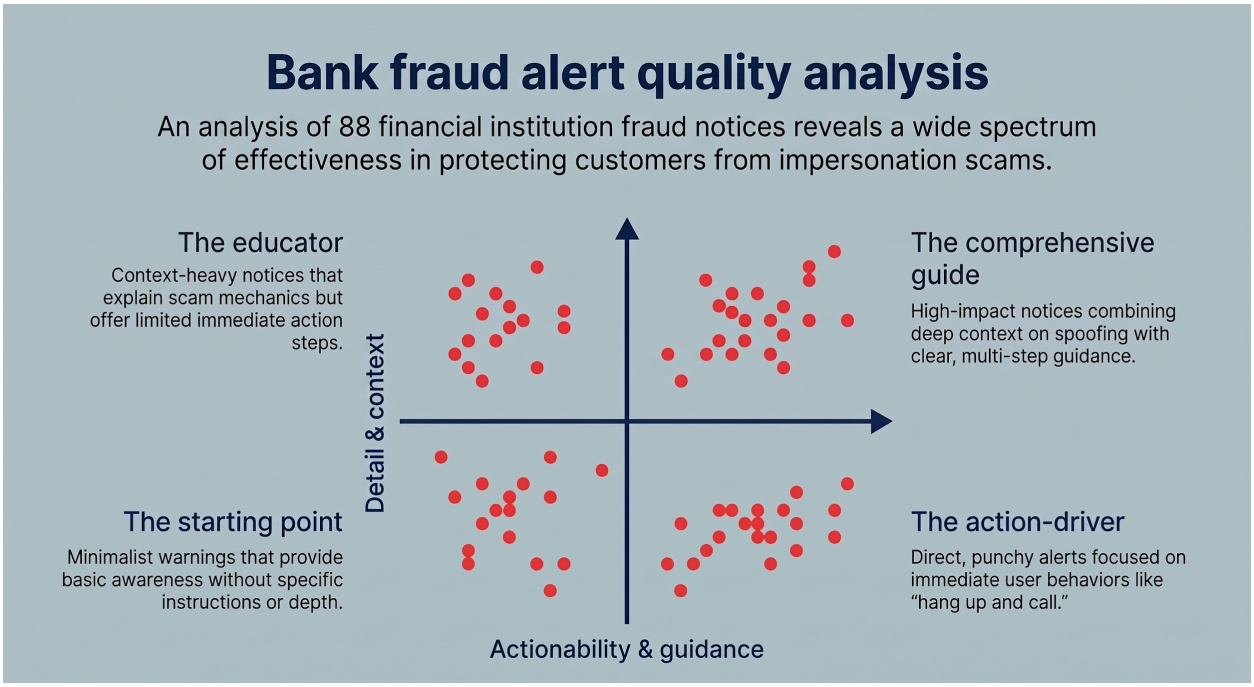
3. **Fake Transaction Verifications:** Fraudsters are contacting customers claiming there is "suspicious activity" to create a false sense of urgency. They ask the customer to verify fake ACH transactions, wire transfers, or even Paycheck Protection Program (PPP) loans.
4. **Malicious Links (Phishing):** Unsolicited text messages and emails are frequently sent containing hyperlinks. Customers are instructed to click these links to verify their accounts, which leads to a fake login page.
5. **Requests to Send or Transfer Money:** Fraudsters are using social engineering to convince customers to send money directly via Peer-to-Peer (P2P) payment apps to "reverse a transaction," or they pretend to represent well-known brands demanding payment.



A Framework for Growth: The 2x2 Matrix

To help institutions evaluate their current messaging and spot opportunities for enhancement, we developed a 2x2 evaluation matrix based on two helpful dimensions:

- **Y-Axis: Detail & Context (High vs. Low).** Does the message explain *how* the scam works so the customer can recognize it? Does it list what sensitive information is targeted?
- **X-Axis: Actionability & Guidance (High vs. Low).** Does the message provide immediate, frictionless instructions on what the customer should do next, like providing a direct phone number?



Exploring the Quadrants: Opportunities to Level Up

By plotting the 88 analyzed alerts onto our matrix, four distinct styles of messaging emerged. Every style provides value, but analyzing them helps us understand how to combine the best elements of each. Let's look at the characteristics of each quadrant using aggregated, anonymous examples.

The Starting Point (Low Detail, Low Actionability)

The Example: *"Fraud is on the rise in our area. Please stay vigilant and be aware of the latest scams targeting banking customers."*
The Takeaway: While raising general awareness, this type of banner is not very effective. It lets the customer know that the institution is paying attention to the community's safety. To level this message up, an institution can easily add a brief description of what the "latest scams" actually look like, and provide a phone number for the customer to call if they have questions.

The Educator (High Detail, Low Actionability)

The Example: *"Beware of bank imposter scams! Criminals are calling customers using a number that looks like our own. Remember: we will never ask you to send money to reverse a transaction. If you suspect fraud, reach out to your local branch."*
The Takeaway: Alerts in this quadrant are incredibly specific and serve as a good source of education. A customer reading this knows exactly what red flags to look out for. They are good for a specific high-scale attack hitting the bank. They are, however, not very actionable. To make this message even stronger, the institution simply needs to replace the general "reach out to your local branch" instruction with a specific, direct phone number. This removes any friction for a customer who might need immediate help.

The Action-Driver (Low Detail, High Actionability)

The Example: *"Please remember that your security is important to us. If you ever feel suspicious about a phone call or text message, please hang up and call customer service at-800-XXX-XXXX."*
The Takeaway: These messages are operationally superb. They give the customer a clear, comforting instruction and a direct lifeline to the bank. They are broad enough to cover any type of attack. The downside: they do not relate to any specific attack the bank might be experiencing. The opportunity for growth here is to add more context. Adding a quick sentence about *why* a customer might feel suspicious - such as mentioning caller ID spoofing - helps train the customer on when they should use that phone number.

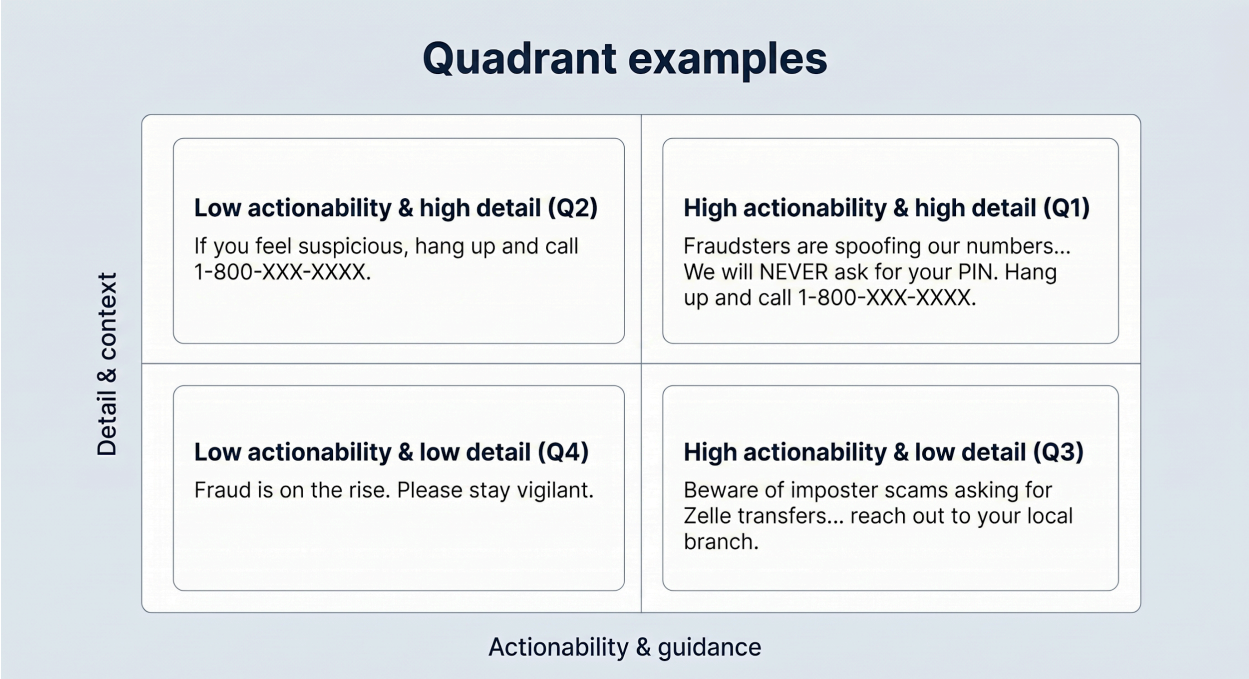
The Comprehensive Guide (High Detail, High Actionability)

The Example: *"Fraudsters are currently spoofing our phone numbers and claiming to be from our Fraud Department to alert you of 'suspicious activity.' We will NEVER call or text*

you to ask for your online banking passwords, one-time passcodes, or PINs. If you receive a call asking for this information, hang up immediately and call us directly at-800-XXX-XXXX."

The Takeaway: This represents a wonderfully balanced approach, combining great education with empowering action.

- **It provides context:** It names the tactic (spoofing) and the scenario ("suspicious activity" claims).
- **It sets a helpful boundary:** It definitively lists the data points the institution will never ask for (passwords, OTPs, PINs) 2.
- **It offers a frictionless next step:** It gives a clear instruction followed by the exact phone number the customer needs.



Conclusion: The 3-Question Audit for Customer Empowerment

Helping customers navigate the digital world is an ongoing, collaborative process. The goal is always to equip them with the detailed context and direct guidance they need to feel confident and secure.

To ensure your institution's alerts are as helpful as possible, try running your next message through this simple, three-question audit:

1. **Does it explain the mechanism?** (e.g., spoofing, fake links) so the customer can recognize it.
2. **Does it set a hard boundary?** (Clearly stating what the bank will *never* ask for).
3. **Does it provide a frictionless contact method?** (A direct, clickable phone number to a verified support line).

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.