The New York Times https://www.nytimes.com/2025/09/18/nyregion/zelle-chase-banking-scam.html

I've Written About Loads of Scams. This One Almost Got Me.

The caller ID said "Chase Bank," and the man on the line said I might be a victim of fraud. His supervisor would explain.

By Michael Wilson

Published Sept. 18, 2025 Updated Sept. 20, 2025

"Please hold," the caller said, "while I transfer you to my supervisor."

It was a Wednesday in August, a little before lunch. The call came from a 212 number, which for a New Yorker could be almost anything — the school, the pharmacy, the roof guy — so I answered.

The caller asked for me by name and stated in measured tones that he was from Chase Bank and he wanted to verify transfers being made from my account to someone in Texas.

Wrong number, I said. I don't have a Chase account.

But one was recently opened in your name, he replied, with two Zelle transfers. And minutes ago, someone tried to transfer those funds, $2,100, to San Antonio.

Now, this carried the whiff of plausibility. I'm one of some 150 million people who have access to Zelle, the payments platform that lets you send and receive money from your phone. But my scam radar was also fully operational and pinging.

"How do I know this isn't a scam?" I asked, sounding like that guy in every movie who asks an undercover cop if he's a cop.

He had a quick answer. Look at the number showing on your phone and Google it, he replied. “Now look up the Chase branch at 3 Times Square,” he instructed. “See the office phone number?” I did, and it matched the one on my phone’s screen.

Then he added, “Here at Chase, we’ll never ask for your personal information or passwords.” On the contrary, he gave me more information — two “cancellation codes” and a long case number with four letters and 10 digits.

That’s when he offered to transfer me to his supervisor. That simple phrase, familiar from countless customer-service calls, draped a cloak of corporate competence over this unfolding drama. His *supervisor.* I mean, would a scammer have a supervisor?

The line went mute for a few seconds, and a second man greeted me with a voice of authority. “My name is Mike Wallace,” he said, and asked for my case number from the first guy. I dutifully read it back to him.

“Yes, yes, I see,” the man said, as if looking at a screen. He explained the situation — new account, Zelle transfers, Texas — and suggested we reverse the attempted withdrawal.

I’m not proud to report that by now, he had my full attention, and I was ready to proceed with whatever plan he had in mind.

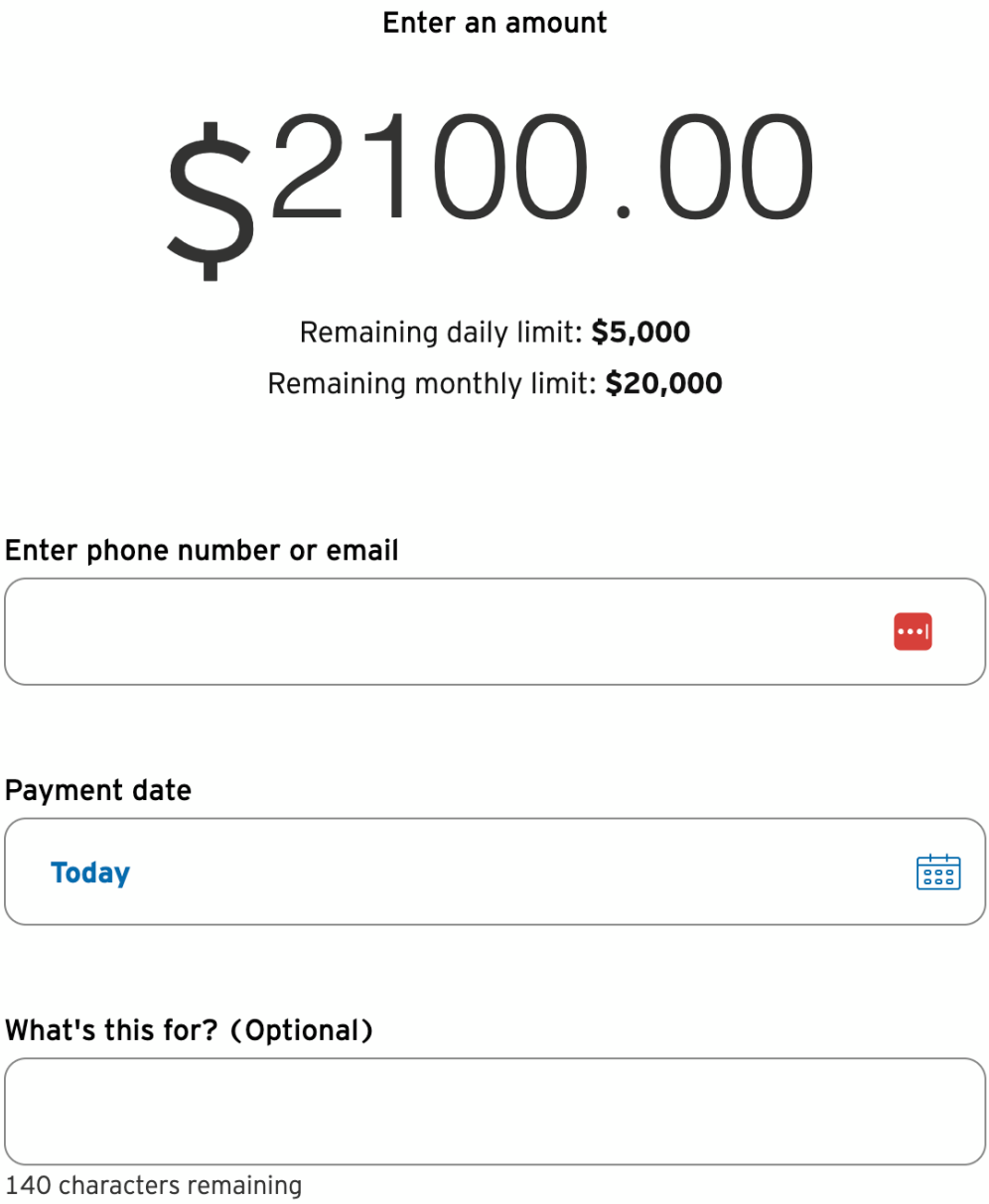
Internet fraud has grown steadily, with 2024 setting new record-high losses — “a staggering $16.6 billion,” the F.B.I.’s annual Internet Crime Complaint Center wrote in a recent report. These crimes include elaborate cryptocurrency schemes and ransomware attacks on entire cities, but phishing and spoofing — the cloning of an actual phone number — still lead the list of some 860,000 complaints last year.

Are these scams entering some sort of improved, 2.0 version of the old-school Nigerian-prince-type setup?

“I wouldn’t call it an improvement,” said Paul Roberts, an assistant special agent in charge of the New York offices of the F.B.I. “It’s an adaptation. As the public becomes more aware of schemes, they need to adjust.”

The man claiming to be a Chase supervisor asked me to open Zelle. Where it says, “Enter an amount,” he instructed me to type $2,100, the amount of the withdrawals he was going to help me reverse.

Then, in the “Enter phone number or email” window — where the other party in a Zelle transaction goes — he instructed me to type the case number the first caller had given me, but to leave out the four letters. Numbers only. I dutifully entered the 10 digits, but my skepticism was finally showing up.



The “supervisor” guided the author on what information to put into his Zelle account. The

parenthetical “optional” was the final detail that made him pause.

“Mr. Wallace,” I said, somewhat apologetically. “This case number sure looks like a phone number, and I’m about to send that number $2,100.”

No, he replied, because of this important next step. In the window that says “What’s this for? ” where you might add “babysitter” or “block party donation,” he told me to enter a unique code that would alert his team that this transaction should be reversed.

It was incredibly long, and he read it out slowly — “S, T, P, P, six, seven, one, two …” — and I typed along. Now and then he even threw in some military-style lingo: “… zero, zero, Charlie, X-ray, nine, eight …”

Once we were done, he had me read the whole 19-character code back to him.

Now, he said, press “Send.”

But one word above the “What’s this for?” box containing our special code with the X-ray and the Charlie kept bothering me: “Optional.”

Then I had an idea, and asked the supervisor if he was calling from 3 Times Square. Yes, he said.

I’ll come to you, I said, and we’ll fix this together.

By then it will probably be too late, he said.

“I’ll call you back,” I said, and he said that would be fine, and I hung up.

I called my bank and confirmed what I’d come to suspect. There had been no recent Zelle activity.

My jaw dropped when I went back and looked at my call history. Sixteen minutes — that’s how long they had me on the line.

In decades as a crime reporter, I’ve covered many, many scams — psychic scams, sweetheart swindles, real-estate scams, even the obscure “nanny scam,” where a fake mother reaches out to a young caregiver to try to rip her off.

I should be able to spot a scam in under 16 seconds, I thought — but *16 minutes*?

I wanted to know why this scam seemed to work so much better than others.

An online search for "Chase Zelle scam" turned up many posts on social media describing calls that were nearly identical to mine.

Kayleigh Coleman, who runs a trash removal company in Largo, Fla., wrote about the scam on Facebook; for her, the transfer to the supervisor "is when it got fishy."

Candance Lace, a boutique dog groomer in Lake Elsinore, Calif., was busy with a client's pet when she got the call and, distracted, all but volunteered her password. She caught herself just in time and hung up to call her bank.

Not everyone gets out before sending money. "Ugh," a Reddit user posted seven months ago. "I just had this happen to me but I fell for it. I'm an idiot." Another wrote, "I'm out $300."

I reached out to Zelle and was connected with Benjamin Chance, head of Identity and Payments Risk at Early Warning Services, the company that owns and operates the platform.

He said impersonation or impostor scams have grown since the pandemic, and he broke down what makes this particular scam work.

First, the callers express urgency.

"If you are that young mother who's taking their kids to soccer practice and is unloading the minivan, you might be in a rush and more likely to fall for this type of scam," Mr. Chance said.

And then there's that "supervisor."

"They are attempting to lend authenticity and legitimacy to the phone call," he explained. "You feel like you're actually in a real call center, and you feel like you're talking to a real person." In fact, it could just be two people sitting together, sharing the phone. Or one person changing his voice.

Main entrance to the Chase branch in Times Square. Erik McGregor/LightRocket, via Getty Images

Then there's all that information coming at you — in my experience, the "case number," two "cancellation codes" and that 19-character string at the end. Mr. Chance said the delivery of all that stuff creates a lulling effect on the would-be victim.

"As you started to type that long number and letter string, it's getting you to just do a task at the request of this criminal on the other side," he said. "As you do that, you've shifted as a critical thinker to someone performing a task."

He said people should be wary of answering calls from strange numbers; if it's someone claiming to be from a bank, hang up and call the bank's number on your debit card.

Agent Roberts had advice for those who do answer the call: "Take that breath, take a beat. Think about what's going on and what this call is about."

In the end, I had avoided the scam easily enough. But it nagged at me, and so I knew I had one more stop to make — 3 Times Square, on West 42nd Street in the heart of Times Square, once the nation's capital for old-school scams like three-card monte. Did the bank know what was going on, with fake calls seemingly coming from their office? Inside, there are ATMs in the small Chase lobby and an escalator up to a floor of cubicles and bankers in glass-enclosed rooms.

"I'm looking for a Mike Wallace?" I told an employee.

No such person here, she replied. I began to describe my call, and she smiled knowingly. The Zelle transfer, the supervisor — she'd heard it all before, many times, from people calling the branch for verification, she said.

Had anyone said they'd sent the money like the scammers requested?

She thought, and said, "Maybe two."

Finally, looking for more victims, I turned to Reddit and wrote a post in a thread of users swapping stories about this scam, asking anyone interested in sharing their story to reach out.

My post was rejected by moderators. Reaching out to people who have been victims of a scam, it turns out, is a classic maneuver at the start of a whole new scam.

Read by Michael Wilson

Audio produced by Jack D'Isidoro.

Michael Wilson, who covers New York City, has been a Times reporter for more than two decades.

A version of this article appears in print on , Section A, Page 1 of the New York edition with the headline: The Zelle Scam Is So Good, Even a Skeptical Crime Reporter Almost Got Reeled In