Behind the $68 Billion Loss

Real stories from bankers on the front lines of fraud prevention.

THE TACTICS

Every day, criminals impersonate financial institutions via fake calls, texts, and emails to scam Americans out of an estimated $68 billion per year.

> *Our organization regularly receives calls from concerned customers about how they have received calls from our bank's 'fraud department'. These fraudsters regularly use our bank's name to try and convince victims they are legitimate and then attempt to steal thousands of dollars from them.*
>
> — **Brad W.,** Midwest Bank, NE

> *We have seen fraudsters impersonate banks through spoofed phone calls to customers, including calls that falsely appear to come from trusted financial institutions. As AI tools become more advanced, these scams will likely become more convincing . . . Stronger caller verification standards are needed now to help reduce this type of fraud, protect consumers, and preserve trust in the financial system.*
>
> — **Trevor D.,** Midwest Bank, NE

> *Wisconsin banks deal with fraud daily, and it is becoming increasingly common for criminals to commit fraud through illegal robocalls, particularly through schemes of impersonating Wisconsin banks and their staff.*
>
> — **Wisconsin Bankers Association,** WI

> *Often the fraudsters spoof our bank call center numbers to contact our customers directly to gain access to passwords and private individual information. Our customers often fall victim to the scam because they trust a call from our bank number is a valid call.*
>
> — **Scott S.,** United Bank Corp, GA

> *To create a sense of urgency, the [criminal] caller tells the customer that immediate action is required to prevent additional losses [and] then asks the customer to . . . [t]ransfer funds to a 'safe' account that the fraudster claims is controlled by the bank.*
>
> — **Kathy M.,** BOM Bank, LA

> *I have been inundated with...up to six calls per day from various numbers, all with computer generated voices... The company making the call is never identified.*
>
> — **Martha B.,** GA

> *Our customers have received calls in which our bank's main telephone number appeared on the caller ID, making the calls appear to be legitimate. During these calls, fraudsters impersonate bank employees, claiming to be from our fraud department and stating they need to verify potentially fraudulent transactions on the customer's account. They create a false sense of urgency by advising customers that immediate action is necessary to prevent additional fraudulent activity . . .*
>
> — **Concordia Bank and Trust Co.,** LA

> *The caller [purporting to be from the bank] convinced our customer that their account had been compromised by a bank employee and to keep their funds secure, they needed to withdraw it and purchase cryptocurrency, which they followed through with on multiple occasions... The lost funds have never been recovered.*
>
> — **Kim A.,** Tensas State Bank, LA

THE COST

The losses are real: fraudulent wires topping $1 million, six-figure withdrawals authorized under pressure, and customers watching a lifetime of savings disappear.

> *We have seen several instances where spoofed calls have led to bank customers disclosing personal information, having their online banking compromised, accounts taken over and financial losses due to unauthorized transactions.*
>
> — **Julie L.,** PA

> *Recently, a client of my financial institution was duped into thinking he was talking to a member of the bank's fraud team. The client ended up providing all his online banking credentials and personal information, with fraudulent wires being initiated for over 1 million dollars.*
>
> — **William S. B.,** First Federal Bank, FL

> *We speak to customers daily that are misled by fraudulent callers, most have lost funds as a result. Customers are upset and do not understand why this is allowed to happen. They are looking for protection from the predators. These fraudsters are stealing massive amounts and directly impacting the financial well being of our citizens.*
>
> — **Greta W.,** United Bank, GA

> *Almost without exception, the actual financial losses that our customers are experiencing originate through a fake call or text message. Something needs to be done.*
>
> — **Troy Q. R.,** Guaranty Bank and Trust Company of Delhi, LABank, LA

> *Recently, a consumer customer of ours lost nearly her entire life savings because of these spoof tactics.*
>
> — **Jamie M.,** Midwest Bank, NE

The caller represented himself as an employee of the bank's fraud department. The caller told the customer that there were suspected fraudulent transactions on the account and needed their information in order to verify the transactions. Unfortunately, the customer provided the information requested which resulted in $750,000.00 fraudulent ACH transactions being debited from the account. The bank was able to recover almost half the funds; however, the customer took a significant loss.

— **Austin B.,** Texas NA, TX

I have had customers come to withdraw their life savings because 'corporate security' from our bank is advising they need to do that to keep their money safe.

— **Deb B.,** First Citizen's Bank, WI

THE VICTIMS

3 in 4 Americans have experienced a scam or fraud attempt, and adults 65+ report the highest fraud losses. Scammers often threaten elderly victims until they hand over their savings.

We have witnessed our customers, the victims, on the phone with these criminals, being verbally abused, berated, degraded, and threatened with physical violence. We have witnessed these criminals threatening to come to the homes of the victim if the victim refuses to continue sending funds.

— **First Community Bank of Tennessee,** TN

I know of many banks that have had customers suffer from 'elder abuse' via these types of phone calls. The bad actors are very convincing. In many cases, [the customers] lose their entire savings.

— **Troy A.,** The Bankers Bank, OK

Just recently, an elderly customer was contacted by phone by a fraudster posing as another financial institution claiming there was a serious issue with his account that required immediate attention. Frightened, the elderly customer disclosed information (routing and account numbers) on several accounts, which the fraudster used very quickly to steal funds from.

— **Fifth District Savings Bank,** LA

This type of fraud is not a monthly occurrence, it's a daily issue. Regardless of whether the fraud begins via a text message, voice message, or some combination, it is pervasive and results in the loss of hundreds of thousands of dollars, frequently impacting the elderly in our community.

— **John L.,** Metairie Bank & Trust Company, LA