
Scam Stories: Real Experiences. Real Lessons.

A consumer security resource from SSB Bank

Every story below reflects real scam experiences reported by people just like you. Scammers are sophisticated and relentless — no one is immune. Read how these scams unfolded and what the victims wish they had known, so you can recognize the warning signs before it is too late.

Remember: SSB Bank will never call, text, or email you to ask you to move money, share your password or one-time passcodes, or assist with a sting operation. If something feels off, hang up and call us directly using the number on the back of your card.

Bank Impersonation Scams: When the Caller Sounds Like Your Bank

Scammers can spoof caller ID, emails, and texts to appear as SSB Bank. They create urgent fraud alerts and pressure you to move money — something your real bank will never do.

"They knew my account balance to the penny"

How it can happen

My phone lit up showing SSB Bank. The caller said unusual charges had hit my account overnight and rattled off my exact balance. He said a fraud specialist was standing by and transferred me. She explained that to protect my funds, I needed to move everything to a temporary SSB holding account and gave me a routing number.

I drove to my nearest branch and wired the funds. That evening I logged into my real SSB app and found my account empty with no trace of any holding account. When I called the number on the back of my card, a real SSB representative confirmed the wire had gone to a stranger. The money was gone.

I wish I'd known

- SSB Bank will never ask you to wire money to a safe or holding account to resolve fraud.
- Scammers research their targets — knowing your balance does not mean the caller is your bank.
- Hang up on any unexpected fraud call and dial the number on the back of your card.
- Wires and account-to-account transfers are final. Once the money is sent, it rarely comes back.

"I was told a teller at my branch had been arrested"

How it can happen

A woman identifying herself as the SSB Bank fraud director called to say a teller at my branch had been arrested for skimming accounts, including mine. A detective joined the call, gave me his badge number, and told me to keep things confidential so I would not tip off any other insiders.

They sent a one-time code to my phone and asked me to read it aloud to verify my identity. I did. Within minutes, \$4,200 disappeared from my account. The code had authorized a transfer, not a verification — and no detective was ever involved.

I wish I'd known

- One-time passcodes authorize actions on your account. Never read them to anyone.
- Police and banks do not ask customers to keep investigations secret from branch staff.
- If a caller tells you to distrust your own bank employees, that is the scam.
- Caller ID can be faked. Always verify by calling the number on the back of your card.

Investment Scams: When the Returns Are Too Good to Be True

Investment scammers build credibility slowly through professional personas and polished websites before making their move.

"My old friend's crypto tip seemed like a sure thing"

How it can happen

An old college friend reconnected with me on social media. We caught up, talked about our families, and eventually he shared a screenshot showing a \$14,000 crypto gain in six weeks. The platform looked professional: live charts, a mobile app, customer support chat.

I started with \$2,000 and watched it grow daily. Encouraged, I added more. When I tried to withdraw \$38,000, support demanded a tax release fee. I paid it. Then came a compliance hold. I never received a dime. My friend's account had been hacked months earlier — I had been talking to a scammer the entire time.

I wish I'd known

- If you cannot withdraw without paying extra fees, the platform is fraudulent.
- Scammers hack real accounts — a familiar face online is not proof of identity.
- Verify any investment platform at [investor.gov](https://www.investor.gov) before depositing money.
- Guaranteed or unusually high returns are always red flags.

Impersonation Scams: When Scammers Pose as People You Trust

Beyond your bank, scammers impersonate government agencies, law enforcement, and even your own family to create fear and urgency.

"Social Security called — my number was linked to a drug bust"

How it can happen

My caller ID showed the Social Security Administration's real toll-free number. The caller said my SSN had been linked to a vehicle found at the border packed with drugs and cash, and a warrant was out for my arrest. Unless I cooperated and protected my assets immediately by converting them to gold coins for a government courier, I would be detained.

I was terrified. I withdrew \$9,000 in cash and bought gold coins. A courier arrived at my door and took them. When I called SSB Bank to explain, I learned that government agencies never confiscate assets by courier and never call with arrest threats.

I wish I'd known

- Government agencies do not demand immediate asset transfers to avoid arrest.
- Caller ID numbers can be spoofed, even official government numbers.
- Couriers collecting cash or valuables for the government are scammers.
- Hang up and call the agency directly using a number from their official website.

"My grandson's voice — asking for bail money"

How it can happen

My phone rang early on a Saturday. I heard my grandson's voice, shaken and whispering. He said he had been in a car accident and his lawyer needed \$5,500 in cash before the courthouse opened or he would be held over

the weekend. Please, Grandma, do not tell Mom and Dad yet.

A man claiming to be his attorney gave me a drop-off address. I delivered the cash. An hour later I called my grandson directly — he was at home, perfectly fine. The voice had been AI-generated from clips on his social media. Five thousand five hundred dollars was gone.

I wish I'd known

- AI can clone a loved one's voice from short public audio or video clips.
- Agree on a family safe word for emergencies and do not share it anywhere online.
- Always call your family member back on a known number before sending money.
- Real attorneys and courts never accept loose cash envelopes dropped at an address.

Romance Scams: When Love Becomes a Weapon

Romance scammers invest weeks or months building a genuine-feeling emotional connection before they ever ask for anything. By the time they do, the relationship feels completely real.

"We talked every night for four months"

How it can happen

After my divorce I joined an online dating app. A man named Marcus reached out — a widower and civil engineer on an overseas contract. His messages were thoughtful and we video-called a few times. After months of daily conversation I truly felt I knew him.

Then the emergencies began. A medical bill from a job-site accident. Then his project payment was frozen and he needed help releasing his contract funds. Every time I hesitated, he sent voice messages full of emotion. I sent money three times over six weeks. Then he disappeared. His photos had been stolen from a real person's public profile. Marcus had never existed.

I wish I'd known

- Romance scammers deliberately build trust over weeks or months before asking for anything.
- They almost always claim to be working or traveling abroad, making in-person meetings impossible.
- Brief, choppy, or frozen video calls are a warning sign — deepfake technology has limits.
- Reverse-image-search profile photos to check if they appear elsewhere under different names.
- Never wire money or send gift cards to someone you have not met in person.

"She said the investment was just for us"

How it can happen

I connected with a woman on a photography hobby forum. After weeks of chatting about cameras and travel, she casually mentioned a private crypto fund her uncle managed. She was not pushing it — she said most people could not get access, but she could get me in as a personal favor.

I invested \$6,000. My dashboard showed steady gains and she would check in: you are up 22%, I am so happy for you. When I tried to withdraw, the platform required a 15-percent tax prepayment. She urged me to pay it so we could finally meet in person with my profits in hand. I paid. The site went dark the next morning. She was gone too.

I wish I'd known

- This tactic is called pig butchering — scammers build you up emotionally and financially before vanishing.
- Exclusive investment access through a new romantic connection is a classic setup.
- Any platform that requires a fee to release your own withdrawal is fraudulent.
- The romantic relationship and the investment scam are the same scam, designed together.

Seasonal and Event Scams: When Timing Makes You Vulnerable

Scammers time their attacks around holidays, major events, and busy life moments when your guard is down and urgency feels natural.

"We pre-paid a vacation rental that did not exist"

How it can happen

My family found a lakefront cabin online with great reviews and a fair weekly rate. The owner asked us to move the conversation off the rental platform to email and requested a 50-percent wire deposit plus a copy of my driver's license for the rental agreement.

When we arrived, another family was already there. The listing had been cloned from a legitimate property. Within weeks, fraudulent accounts were opened in my name using the ID copy I had sent. What was meant to be a summer vacation became months of credit disputes and identity restoration.

I wish I'd known

- Never pay outside the official platform — doing so voids all fraud protection.
- A request to move communication off a trusted site is a major red flag.
- Do not send photos of your ID to someone you found through an online listing.

"Fake playoff tickets and a fake website"

How it can happen

I searched for playoff tickets and a result took me to what looked exactly like a well-known ticket reseller. I found great seats and went to check out but my card declined. A message said to call a support number to complete the purchase.

The agent said credit cards were having issues and suggested gift cards as a workaround. I bought \$480 in gift cards and called back. He took the codes and gave me a booking reference. No tickets ever arrived. The site URL had one extra letter. The real site had no record of my order.

I wish I'd known

- No legitimate ticketing company will ask you to pay with gift cards.
- Navigate directly to the ticketing site rather than clicking search ads.
- Check the full URL carefully before entering any payment information.

Social Media Shopping Scams: When That Ad Is Not What It Seems

Fraudulent ads and marketplace listings are engineered to win your trust and rush you into sending money before you think twice.

"The furniture sale looked completely legitimate"

How it can happen

An ad appeared in my feed for a boutique furniture sale at 70 percent off. The site had professional photos, customer reviews, and brand logos. I ordered a dining set for \$640 and received a polished confirmation email.

Three weeks passed with no shipping update. The customer service number was disconnected and the site had vanished. My bank statement showed two additional overseas charges I did not recognize. My card number had been captured and sold.

I wish I'd known

- Social media ads are not vetted — professional design does not mean a seller is legitimate.
- Search the store name plus reviews or scam before buying from an unfamiliar site.
- Pay with a credit card when possible — it provides chargeback rights that a debit card does not.

"I sold my lawnmower and lost \$300"

How it can happen

I posted my lawnmower for \$250 on a marketplace app. A buyer offered to pay immediately via Zelle. Minutes later I got an alert that \$550 had been sent by mistake and was asked to send back the \$300 overage right away. I did.

The original payment reversed two days later — it had come from a compromised account. I never received a dime for my lawnmower and lost another \$300 on top of it.

I wish I'd known

- Overpayments followed by a refund request are always a red flag.
- Zelle transfers can be reversed if they originate from a stolen account.
- For marketplace sales, accept exact amounts only and confirm funds have fully cleared.

Checks You Write: When Fraudsters Alter or Counterfeit Your Checks

Stolen checks can be chemically washed and rewritten within hours. Your name, address, and account number can also be used to print counterfeit checks.

"My rent check was rewritten for \$3,800 more"

How it can happen

I mailed my rent check from the blue USPS collection box on my street — the same one I had used for years. The next month my landlord emailed about overdue rent. I checked my account: the check had cleared, but the payee name was different and the amount was \$3,800 higher than what I had written.

Someone had intercepted the envelope, washed the ink, and rewritten the check. They also used the account number to print counterfeit checks. By the time I discovered it, multiple fake checks had cleared and I had to close the account, file a police report, and dispute each transaction individually.

I wish I'd known

- Use SSB Bank Online Bill Pay to pay bills without sharing your account number.
- Stolen checks can be washed and rewritten in a matter of hours.
- Mail theft from street collection boxes is far more common than most people realize.
- If you must write checks, follow these precautions:
 - 1 Use a gel pen — gel ink is much harder to chemically wash than ballpoint.
 - 2 Fill every blank space; draw a line through leftover space in payee and amount fields.
 - 3 Sign consistently so alterations are easier to detect.
 - 4 Drop checks at the post office counter, not street collection boxes.

Think you have been targeted? Contact SSB Bank right away using the number on the back of your card or visit your nearest branch. You can also report scams to the FTC at reportfraud.ftc.gov.