



PROTECT YOURSELF FROM SWEEPSTAKES SCAMS & FRAUD

If it seems too good to be true, it probably is. Sweepstakes scams are one of the most common ways fraudsters target individuals. Scammers use excitement, pressure, and false promises to trick victims into giving money or personal information. Stay alert and know the warning signs.

HOW SWEEPSTAKES SCAMS WORK

- You receive notice that you've won a contest you never entered.
- You're asked to pay shipping fees, taxes, or upfront costs to receive a "free" prize.
- You face high-pressure sales tactics or claims of a "once-in-a-lifetime opportunity."
- The prize requires you to share bank details, Social Security numbers, or other personal information.
- Money is requested via overnight mail, wire transfer, or courier to "speed up" your winnings.
- You're told to keep your prize a secret from family or friends.
- The caller often pretends to be from a real organization to appear credible.

HOW TO PROTECT YOURSELF

- **Never pay** to receive winnings as real sweepstakes don't require upfront fees.
- **Verify the caller** by contacting the organization using official phone numbers, not the one provided in the message.
- **Get it in writing.** Ask for mailed documentation before sharing anything.
- **Hang up on telemarketers** who claim they can help recover losses.
- **Be cautious** of anyone claiming you have unclaimed property as only the State Treasurer handles this.

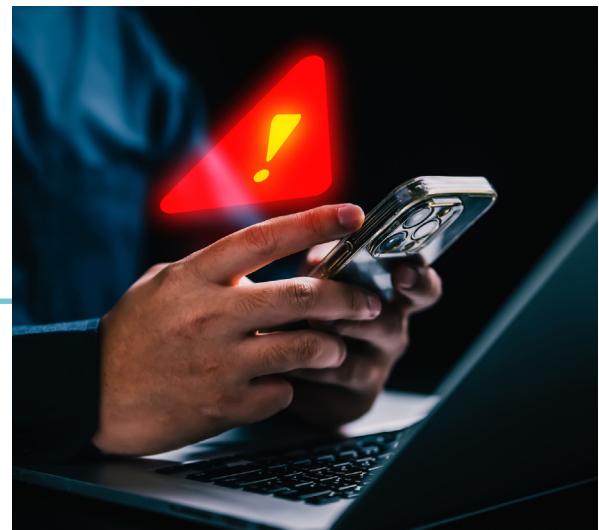
IF YOU SUSPECT A FRAUD ATTEMPT

- Stop all contact with the scammer.
- Do not send money or provide information.
- Immediately notify us and report the incident to the following consumer protection authorities:

Security First Bank Fraud Resolution Department	605-718-8057 Fraud@Security1stBank.com Security1stBank.com/Fraud-Protection	Credit Bureaus to place an identity theft alert or credit freeze.	TransUnion 800-680-7289 TransUnion.com	Experian 888-397-3742 Experian.com	Equifax 888-378-4329 Equifax.com
Federal Trade Commission (FTC) to report fraud and take preventative steps.	Report Fraud ReportFraud.FTC.gov				
Local Police Department to file a police report.	<ul style="list-style-type: none">• Call the local non-emergency number• Go to their website to file a report online• Visit the station in-person				

ESSENTIAL FRAUD PREVENTION TIPS

Reduce your fraud risk by up to 90% with these daily best practices:



ONLINE ACCOUNTS

- Use strong, unique passwords and update regularly.
- Enable 2-factor authentication (2FA/MFA).
- Review bank statements & credit reports frequently.
- Avoid banking on public Wi-Fi; use a VPN if needed.

PROTECT YOUR IDENTITY

- Freeze your credit when not applying for loans.
- Keep sensitive documents locked or encrypted.
- Avoid oversharing on social media.

SAFE COMMUNICATIONS

- Verify unexpected contacts using official numbers.
- Be cautious of emails, calls, and texts asking for money or information.
- Restart your phone every few days to reduce malware risk.
- Never click unknown links or attachments.
- Confirm identity if a caller's voice or video seems "off" as deepfakes are increasing.

SAFEGUARD YOUR MONEY

- Don't send money to anyone you haven't met in-person.
- Slow down as scammers use urgency to force fast decisions.
- Use caution with mobile payments and remote deposits.
- Verify business licenses and legitimacy before paying.
- Use tap-to-pay to reduce card-skimming risk.
- Enable transaction alerts on all accounts.
- Be skeptical of "too good to be true" jobs, investments, sweepstakes, and more.

SECURITY FIRST BANK

Fraud Resolution Department

 605-718-8057

 Fraud@Security1stBank.com

 Security1stBank.com/Fraud-Protection

