

SCAMS FRAUD WHAT TO LOOK FOR



Emails, Websites, Text Messages,
Phone Calls, Regular Mail...

How to Spot a Scam or Fraud Attempt

by Susan S. Teachey (aka Susie)*



May 1, 2026: **THIS TEXT SCAM SENDS TEXTS TO YOU AND CLAIM THAT YOU HAVE A TRAFFIC VIOLATION. IT IS A SCAM.**

If you receive a message like this, report it immediately by calling your county non-emergency police number and report it. Susie received two in the same day from different phone numbers. **Report, delete, and block these numbers.** Staying alert helps protect our community. More information inside.

AND REMEMBER THAT SAINT MARTIN'S MESSAGE GIFT CARD SCAM!

Remember that we, Saint Martin's and Father Lee, would never ask parishioners for gift cards. If you receive a text like this, please report these texts as spam, delete and block the number.

UPDATES MADE MAY 1, 2026 THIS IS A WORKING DOCUMENT

This document will be updated as new and pertinent information on this subject surfaces. If you have information you think should be included, please email me at designer@saintmartinschurch.org and put "Scams and Frauds" in the subject line.

A SHORT NOTE FROM THE AUTHOR:

***I AM NOT AN EXPERT.** But I've experienced serious scam and fraudulent activities that took months or longer to fully correct. I'm sharing this information from personal experiences and my knowledge from formerly worked in Cyber Security. The following pages have examples that I have pulled that came to me personally. I'm quite sure that these examples don't cover everything that could happen in the world today, but I feel obligated to share the knowledge that I do have of this subject with you. I am providing this information in the hopes that if something happens to you, this document can help you find ways to best navigate a solution.

IT IS AN UNFORTUNATE TIME WE LIVE IN...

FRAUDS AND SCAMS attack us through so many modes - some we don't even realize. It is overwhelming and only gaining speed. Many of these attacks are simply to take time away from each of us, causing a nuisance.

NOW WITH AI, it has increased even more and there is no end in sight for this. Sadly, the latest negative impact of AI concerns in hostage situations. Law enforcement is slowed down with fake ransom notes generated by AI. Investigators were once able to determine the authenticity of ransom calls through receiving photos of the hostage, but those same photos can now be generated with alarming accuracy using AI tools. (www.inc.com/ava-levinson/deepfakes-nancy-guthrie/91300426)

These are just a few examples of the possible thousands upon thousands of scams out there.

NOT ONLY ALL OF THAT, if someone wants to get your information they can. But you can take steps to make it more difficult to obtain your information.

Thieves through the dark web - **yes it's real** - and other avenues, will not stop trying to gain access to your identity. It's up to each of us to be vigilant in protecting ourselves. There is a time and money investment, but can save you from identity theft and wasting your time.

HERE ARE SOME TIPS TO LOOK AND LISTEN FOR:

EMAIL: Check the email address that it comes from first. If the information after the "@" is garbled letters, that's a **SCAM**.

TEXT MESSAGES: Don't recognize the number? No message left? **BLOCK THE NUMBER**.

OTP (ONE TIME PASSWORD) YOU DID NOT REQUEST. There is a major uptick in receiving OTP numbers, such as you would get from Amazon and other types of companies.

You've likely noticed that many websites these days text you a 6-digit number to confirm your identity. Now,

OTP's are being sent in an effort to get you to go to that website and put in the code.

A scammer may know your email or phone number and are using "forgot password" to gain entry into your account. **DO NOT VISIT THE WEBSITE THAT THE OTP IS COMING FROM. IT IS CRUCIAL THAT YOU CHANGE YOUR PASSWORD ASAP.**

MAIL: If you receive a check and the send asks you to send some of it back, **IT'S A SCAM**

UNKNOWN CALLER: Don't answer it. If a voicemail is not left, then it's likely a **SCAM**.

IF YOU RECEIVE A JOB OFFER in email, text, and social media platforms a communication. These type of Scams are to get you to talk to them, give them all your information (but most don't ask for your social security number) and then they ask for payment to process your application.

NEVER provide your social security number to an unknown party.

NEVER provide a credit card number or check over the phone to an unknown party. Even when they sound like a very nice person, if they ask for any financial or personal identifying information, **JUST HANG UP**.

IF YOU ARE THREATENED, HANG UP. Some are very abusive and will threaten you with being arrested!

IF YOU ARE NOT QUITE SURE that a communication that comes to you with a familiar company you use, contact the company that is in the message. Another time hog, but effective.

IN 2025 over 73% of U.S. adults report scam phone calls and text messages. In 2024 it was 68%.

Link to article online for deeper information.

bit.ly/3P45agD

WHAT CAN YOU DO TO PROTECT YOURSELF?

Lifelock, LastPass, and Norton are the most secure ways I have found to hold your information, passwords and provide virus protection on your computer. There are others, these are the three this writer uses.

LifeLock by Norton is by far the most robust identity protection there is, in my experience.

www.lifelock.norton.com (See next page for their pricing).

First year is 52% off.

lifelock.com or norton.com

CHANGE YOUR PASSWORDS!

While this is a big inconvenience, it has proven to be a good defense against scammers/fraudsters.

A solid website for storing passwords securely and also a robust password generator is from LastPass.

www.lastpass.com

SET UP TWO-STEP VERIFICATION (2SV).

Get Google Authenticator on your cell phone. This is an app on your phone. It's free and adds another layer of security.

Here is a website search link to Google Search Authenticator apps: <https://bit.ly/4uokZPu>

USING AUTHENTICATOR APPS

DOWNLOAD THE GOOGLE AUTHENTICATOR app to your phone device.

Link: Google Play Store <https://play.google.com/store/apps/details> (Android)

Link: Apple App Store <https://apps.apple.com/us/app/google-authenticator/id388497605> (Apple)

It is a free mobile app used to generate 2-step verification codes for online accounts.

EXAMPLE INSTALLATION: Search for "Google Authenticator" (published by Google LLC) in your device's app store.

SETUP: Open the app, click the plus sign (+) to add an account, and choose to scan a QR code or enter a setup key provided by the service you want to secure.

INTEGRATION: For Google accounts, go to your Google Account settings, select "Security," then "2-Step Verification," and choose "Authenticator app" to link it.

It is recommended to use a personal Google account to sync your codes, ensuring they are not lost if you switch devices.

It detects which web pages you have open and provides a 6-digit number to provide. This is a one time password (OTP) in a more secured set up.

LOG OUT OF ALL YOUR PROGRAMS, WEB PAGES, OR EMAIL ON THE DEVICES YOU USE TO ACCESS THEM. Then you can log back in and change the password.

WHEN YOU RECEIVE PHONE CALLS

from unknown numbers and they ask if they are speaking to you, **NEVER** say yes. Your responses can be recorded and then used for further attempts on your identity. Ask who is calling before you respond in any other way. Likely it will be some company that is made up...if it sounds weird, it probably is.

JUST HANG UP.

REPORT ATTEMPTS TO AUTHORITIES!

It can seem like this is just a drop in the bucket against the magnitude of cybersecurity, but every drop really does help.

THESE TIPS SCRATCH THE SURFACE AND ONLY ENCOUNTERS I HAVE PERSONALLY HAD.

This "fraud/scam industry" is growing by the day, and AI is a major player in this now. Meaning it will become faster, more legitimate looking, and a bigger waste of our time.

There are so many other ways that you can protect yourself other than the suggestions I have made. Lastpass, Lifelock, and Norton are what I use and have had EXCELLENT success with.

If you want to take it a step further, take the time to

HANDWRITE your passwords in a password book and put it in your safe or other safe and secure place in your home. DO NOT take that password book out of your home. This is a safety net for you to have your passwords and account numbers written down - NOT TYPED ON THE COMPUTER. If the digital world is attack on a large scale, it will interfere with being able to login into your accounts. This is an unlikely occurrence, at least today, so have that backup passcode book could turn out to be a vital help to you in the future.

If you ever run across something you just aren't sure about, REPORT, DELETE, AND BLOCK.

I am not an expert but have worked in Cyber Security and as a graphic designer I am online for hours and hours each day. **What I am providing to you are solely based on my experiences.**

Email me at ssteacheyrva@gmail.com with the subject line that says: **Scamming Help.**

I cannot promise that I can solve what you are experiencing, but I am here to help.

***I cannot stress enough
If you don't know it, Don't click it.***

LIFELOCK

There are a good set of choices to get precisely what you need. Easy to talk to and have always been very helpful. I have had 4 serious identity theft attempts and each time LifeLock got it straightened out with no cost to me.

FIRST MONTH FREE

STANDARD for Individual is \$11.99 paid monthly.
ULTIMATE PLUS for Individual is \$34.99 per month.
There are deep discounts if you pay for the entire year.

www.lifelock.com or www.norton.com

LASTPASS

There are a good set of choices suited to what you need. Generator complex passwords on sites you log into. Reset your password and then allow LastPass to store your username and password. I have found that this is a solid way to handle and save passwords.

LastPass Why LastPass? Personal Business Pricing Partners Get LastPass free Cont

Plans and pricing

Try it for free, no credit card required.

Plan	Price	Free Trial	Best For
Premium	\$3.00 /month billed annually*	30 days	Best value for personal use
Families	\$4.00 /month billed annually*	30 days	Best value for personal use
Teams	\$4.25 user/month billed annually*	14 days	Best value for personal use
Business	\$7.00 user/month billed annually*	14 days	Most admin controls
Business Max	\$9.00 user/month billed annually*	14 days	Most admin controls

Premium
Individual plan that ensures secure password management across all your devices

Families
Keep your household's logins secure and always within reach at home or on-the-go

Teams
Simple credential management for small teams and startups

Business
Effortless password and access management for small and medium-size businesses

Business Max
Advanced protection and secure access for any business with more admin control

For personal use across devices:

- Save unlimited passwords
- Access on all devices
- Save and autofill

Everything in Premium, plus:

- 6 Premium accounts for yourself and your parents, kids, roommates, friends, and whoever else you call family

For your small business or team:

- Admin console to manage users
- Shared folders
- 25 security policies

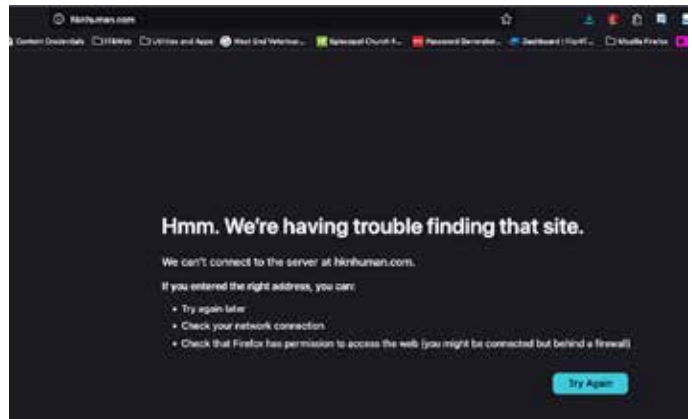
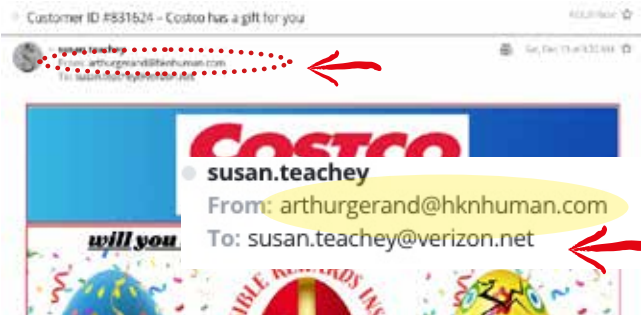
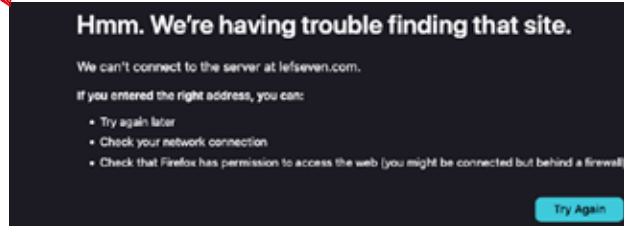
Everything in Teams, plus:

- 100+ security policies
- LastPass Families for employees
- Group user management

Everything in Business, plus:

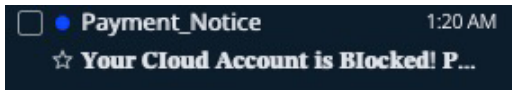
- SaaS Monitoring
- SaaS Protect
- Unlimited number of SSO apps
- Advanced MFA capabilities

↓ If an email comes through such as this, it is a **SCAM**. Remember to look at the "From" name. **Not sure?** Search for the website online. This one is "lefseven.com" as shown in the email. The result is



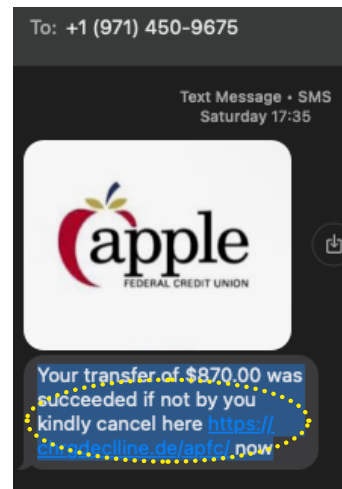
Emails such as this are a scam. Look at the "from line" in the email. If the "@" is like alphabet soup, that's a flag. Don't Click Anything. **DELETE IT.**

NOT CERTAIN? Type in the text after the "@" in your browser and see if anything comes up.



If an email shows up your email list in a different typeface. **DELETE IT.**

Pay close attention to the typeface in an email to see if looks different than your regular emails.



DON'T CLICK IT!
Delete It & Block the Number.

As you can see, the attempts are becoming more and more "legitimate and sophisticated looking." This is only going to increase as time goes on, particularly with AI generating hacks, fake communications, fake photos, and even fake voices that sound like someone you know, or your voice.

Your AntivirusSystem StillPending

From:  Payment/Declined*susan.teachey (arthursavoy@elxlight.com)

To: susan.teachey@verizon.net

Date: Saturday, January 3, 2026 at 12:07 AM EST

DON'T CLICK IT AND DELETE IT!

susan.teachey

Your Device Under Attack Your Data Could Be Stolen

Subscription Details
! Subscription: **Expired**

Your Antivirus Protection Has Expired

Account ID :	qp1nw
User :	*****37
Safe status :	Suspended
Discount :	83% Renewal discount

Your Antivirus subscription expires Today **02/01/2026**
subscriptions are recommended to protect your device. is activated to use a special discount
Once the expiration date has passed, the computer is exposed to many different virus threats.

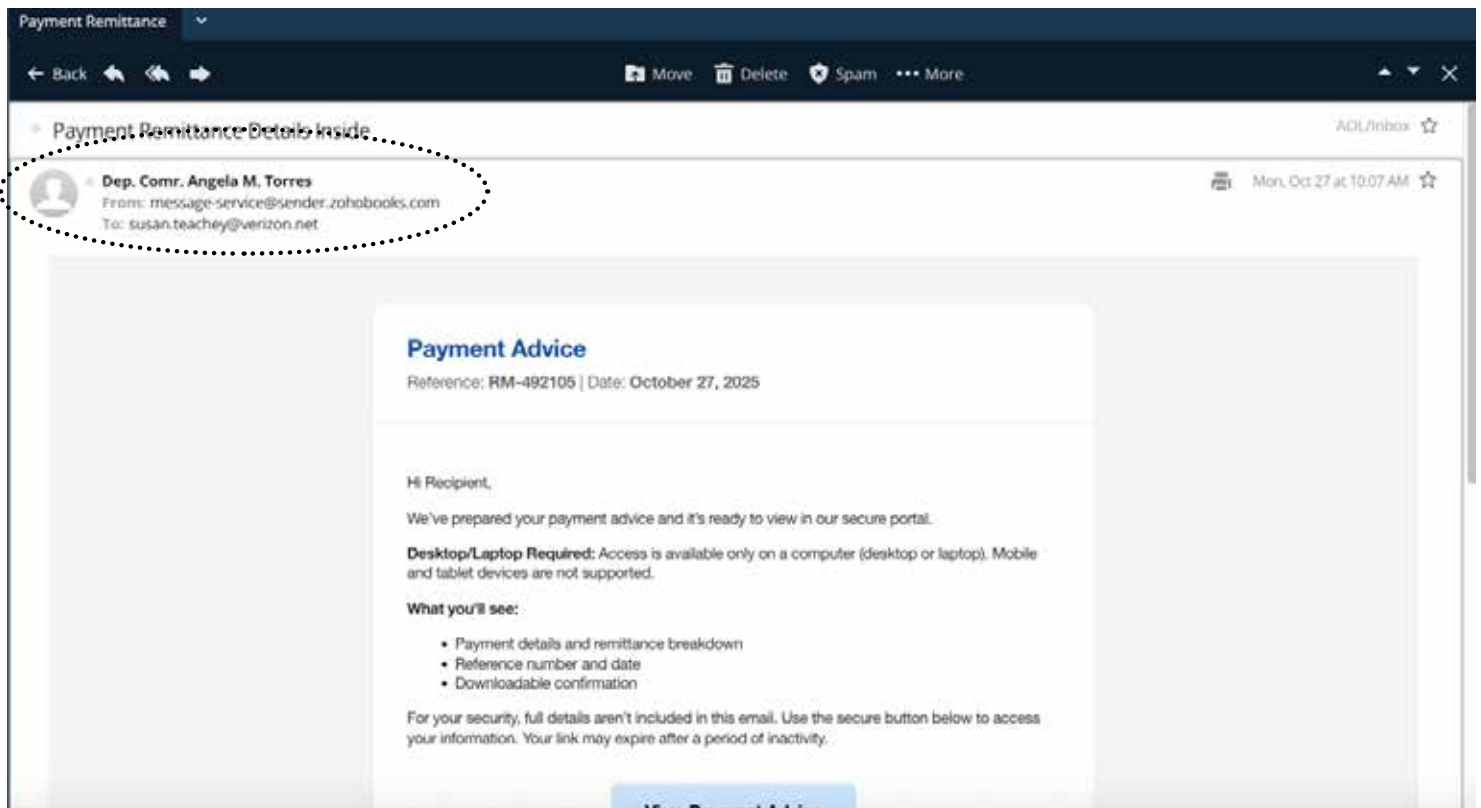
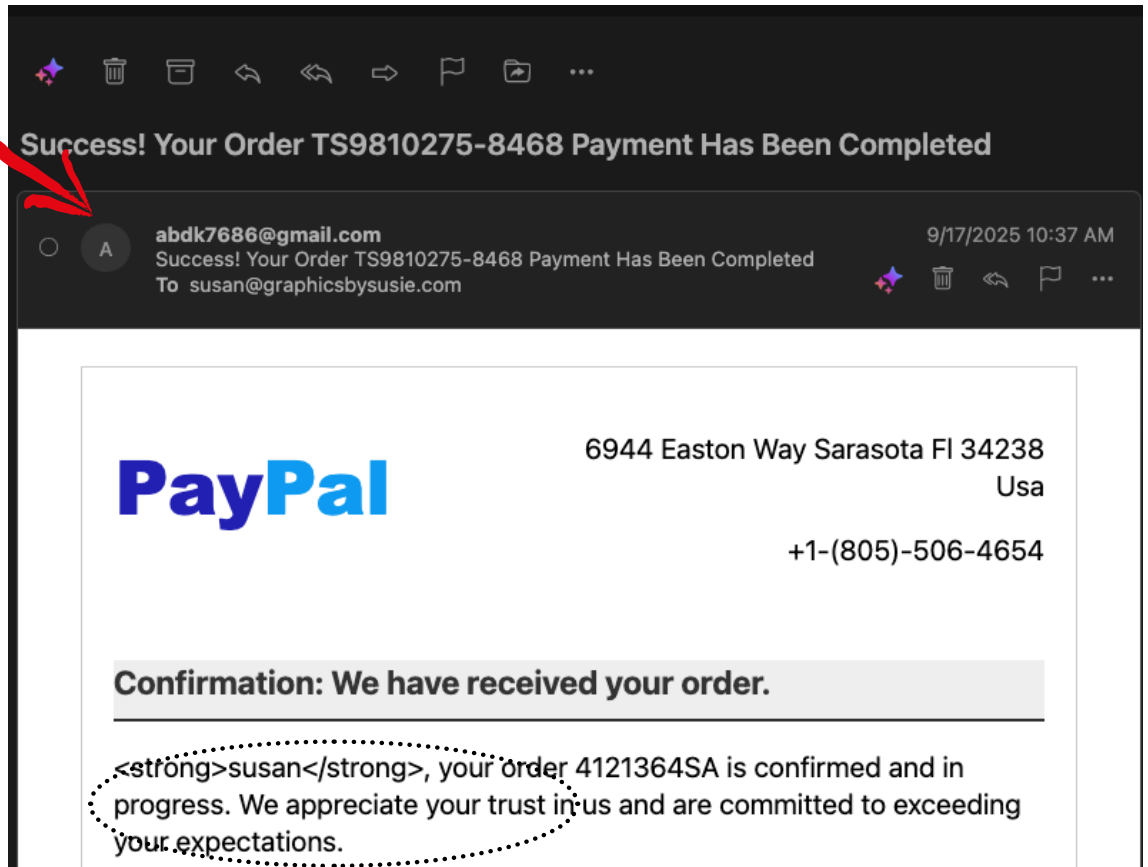
It cannot be protected, it can be exposed to viruses and other software?

You are entitled to the discount: **83% discount on renewal for 1 year**

Renew Membership

This ad is sent on behalf of NewMarket Health Publishing, LLC. P.O. Box 913, Frederick, MD 21703, USA. If you would like to unsubscribe from receiving offers from NewMarket Health Publishing, LLC, please click [here](#)

**DON'T CLICK
IT, DELETE IT
AND CONTACT
THE COMPANY
TO SEE IF ANY
CHARGES ON
YOUR ACCOUNT
HAVE BEEN
MADE.**



Confirmation of Recent Bitcoin Purchase – signature requested by Jeff S. Franklin

From: Jeff S. Franklin (noreply@mail.hellosign.com)

To: jackie.davis@reecebrooks15.onmicrosoft.com

Date: Friday, January 24, 2025 at 11:28 AM EST



ACTION REQUESTED

Jeff S. Franklin (dropboxal@fastmail.net) has requested a signature

Review & sign

Document

Confirmation of Recent Bitcoin Purchase

Message from Jeff S. Franklin (dropboxal@fastmail.net)

Dear Customer,

We would like to notify you about a recent transaction made through your PayPal account. The purchase involved 0.045 Bitcoin, totaling \$485.50 USD. This transaction has been successfully processed and will reflect in your account within 24 hours. Customer Support Hotline: +1 (858) 379-2994

Transaction Details:

Product Purchased: Bitcoin via Coinbase

Transaction Amount: \$485.50 USD

Invoice Number: #XT567923

Payment Status: Completed

If you did not authorize this transaction or believe it was made in error, please contact our support team immediately for assistance.

Customer Support Hotline: +1 (858) 379-2994

To: charlie88@spvpasadena.appleaccount.com



iMessage
Today 09:23

**USPS® Ground
Rearrange Your Delivery**

We attempted to deliver your USPS package; however, we were unable to complete the handover successfully. This package necessitates a personal signature upon receipt. Please follow the instructions provided below to set up a new delivery time.
Reschedule Now:

[https://
www.usps.com@servicehcva.sbs/
TrackConfirm/](https://www.usps.com@servicehcva.sbs/TrackConfirm/)

You have the following choices:

- Choose a new date and time for your delivery

Simply respond with "Y" and then close and reopen this email for the link to activate. If the link does not work, kindly copy it and paste it directly into your Safari browser.

Important Notice:

- Your package will be stored at our local facility for three days starting from the date of this notice.
- If you do not reschedule within this timeframe, your item will be returned to the sender.



David Terry ✓

Experienced Office Executive | Administrative Leadership | Contract & Operations Management

MONDAY



David Terry ✓ · 9:24 AM

I've been asked to reach out to you in regards to paid board and advisory positions. Your back ground matches a few positions that may be a great fit. We would love to have a discussion with you. Please schedule a call at your earliest convenience. See calendar below.

<https://calendly.com/boardsi/board-seat-inquiry-l34?month=2025-06>

Schedule

Not interested

LINKEDIN SCAM: This type of message received in messages in a LinkedIn account is a scam. The entice you to schedule a meeting by clicking the link and does not have a way to contact them.

These scams are designed to harvest personal data and get you to click malicious links which can cause problems within your computer.

Do not click any links, including the Not Interested button. Just delete the message by clicking the three dots in the upper right hand corner of the message and select delete message.



COMMONWEALTH OF VIRGINIA
 IN THE DISTRICT COURT OF VIRGINIA
 FOR RICHMOND
 TRAFFIC DIVISION

**ENFORCEMENT
 ACTIVE**
 NON-COMPLIANCE
 CONFIRMED

CASE NO.: VA-26-TR-273196

DATE: May 4, 2026

FINAL ENFORCEMENT NOTICE — COURT-ORDERED COMPLIANCE REQUIRED

SCAM!

FINAL LEGAL NOTICE OF DEFAULT AND ENFORCEMENT ACTION
 Your traffic violation account has been FORMALLY DECLARED DELINQUENT AND IN DEFAULT pursuant to applicable provisions of the Virginia Code.

All prior notices, compliance deadlines, and opportunities to resolve this matter voluntarily have been EXHAUSTED AND TERMINATED.

THIS MATTER HAS BEEN ESCALATED TO ACTIVE ENFORCEMENT STATUS.

VIOLATION:	AUTHORITY:	RELATED AUTHORITY:
<ul style="list-style-type: none"> • Failure to Pay Electronic Toll/Toll Evasion • Parking Violation • Speeding Violation 	<ul style="list-style-type: none"> • Va. Code, Transportation § 96.2-1229 	<ul style="list-style-type: none"> • Va. Code, Transportation § 46.2-662 • Va. Code, Transportation § 46.2-682 • and other applicable provisions of the Virginia Code

MANDATORY COMPLIANCE ORDER
 You are hereby required to take IMMEDIATE AND COMPLETE ACTION to resolve this matter:

1. Remit FULL PAYMENT IN TOTAL of all outstanding fines, penalties, court costs, and applicable enforcement fees, OR
2. Appear before the Court at the scheduled hearing date to respond to this matter.

FAILURE TO COMPLY WILL RESULT IN ENFORCEMENT ACTIONS INCLUDING, BUT NOT LIMITED TO:

- Entry of a FINAL DEFAULT JUDGMENT without further notice
- Assessment of MAXIMUM STATUTORY PENALTIES, late fees, and court costs
- SUSPENSION OF DRIVING PRIVILEGES within the Commonwealth of Virginia
- STATEWIDE VEHICLE REGISTRATION HOLD, including denial of renewal or transfer
- Referral to authorized COLLECTIONS AND RECOVERY PROCEDURES
- Issuance of authorized COURT-ORDERED ENFORCEMENT MEASURES, as permitted by law
- Permanent adverse entry on your driving and compliance record

FINAL LEGAL NOTICE
 NO FURTHER NOTICE WILL BE ISSUED.
 THIS MATTER WILL PROCEED WITHOUT ADDITIONAL WARNING.
 Failure to act will result in CONTINUED ESCALATION OF ENFORCEMENT ACTIONS until full compliance is verified.

<p>COURT HEARING INFORMATION</p> <p>Date: May 4, 2026 Time: 9:00 AM Location: District Court of Virginia Traffic Division 402 S. 9th Street Richmond, VA 23299</p>	<p>PAYMENT INSTRUCTIONS</p> <p>To resolve this matter please create hearing date, submit payment through the official court payment system.</p> <p>Failure to complete payment prior to the scheduled hearing may require mandatory court appearances.</p>	<p>SCAN TO PAY</p>  <p>Official Payment Portal</p>
---	---	--

BY ORDER OF THE COURT
 Clerk of the Court
 District Court of Virginia
 Commonwealth of Virginia



VA-26-TR-273196

May 1, 2026: **THIS TEXT SCAM SENDS TEXTS TO YOU AND CLAIM THAT YOU HAVE A TRAFFIC VIOLATION. IT IS A SCAM.**

If you receive a message like this, report it immediately by calling your county non-emergency police number and report it. Susie received two in the same day from different phone numbers.

Report, delete, and block these numbers.

The Richmond Police Department and the Commonwealth Attorney's Office are aware of fraudulent messages circulating that appear to be official court or traffic violation notices. These messages are not legitimate. Do not respond, click links, scan QR codes, or share personal or payment information. If you are unsure whether you have any pending violations, please contact the Richmond General District Court Clerk's Office at (804) 646-6431 for assistance.

If you receive a message like this, report it immediately by calling the non-emergency police department in your county. It only takes a few minutes. Staying alert helps protect our community.