How to Spot a Scam or Fraud Attempts In Emails, Websites, Text Messages, Phone Calls, Regular Mail and WHAT YOU CAN DO TO PROTECT YOURSELF.

*by Susan S. Teachey (aka Susie)**

A SHORT NOTE:

I AM NOT AN EXPERT. But I've experienced serious scam and fraudulent activites that took months or longer to fully correct. I'm sharing this information from personal experiences and my knowledge from formerly worked in Cybersecurity. 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.

IMPORTANT SAINT MARTIN'S MESSAGE: GIFT CARD SCAM!

A few times a year texts have circulated claiming to be a parishioner of our church asking for gift cards; these texts are scams! We, Saint Martin's and Father Lee, would never ask parishioners for gift cards. Please report these texts as spam & delete.

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.

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, contant 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?

THINGS YOU CAN DO TODAY to fight against scams and frauds:

Change your passwords at least every 3 months. It's a cumbersome thing to do, but an effective one.

LastPass is a terrific and affordable tool to generate high security passwords and to keep your passwords secured. (More info in this document.)

Lifelock is maverick in protecting your identity and restoring credit.

CHECK YOUR CREDIT REPORT, CREDIT CARD STATEMENTS FOR CHARGES NOT MADE BY YOU AND BANK STATEMENTS! 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.

www.ReportFraud.ftc.gov
FTC's primary reporting platform
www.IdentityTheft.gov
FTC for reporting your identity theft
IC3.gov (FBI)
For internet, email, and online attempts to get your information
www.bbb.org/scamtracker/lookupscam (Better Business Bureau)
www.oag.state.va.us
Virginia Attorney General's Office

LOCAL COUNTY AUTHORITIES

804-501-5000 Henrico County Police
804-556-5300 Goochland County Police
Call the non-emergency department in your county to file a report an attempt of fraud.
In Henrico you can also file a report online: **www.henrico.gov/services/duty-officer-reporting-system/**

In Goochland County you can report an identity fraud attempt or success. Contact the Goochland County Sheriff's Office at 2938 River Rd W, Building C, to file a criminal complaint.

LIFELOCK

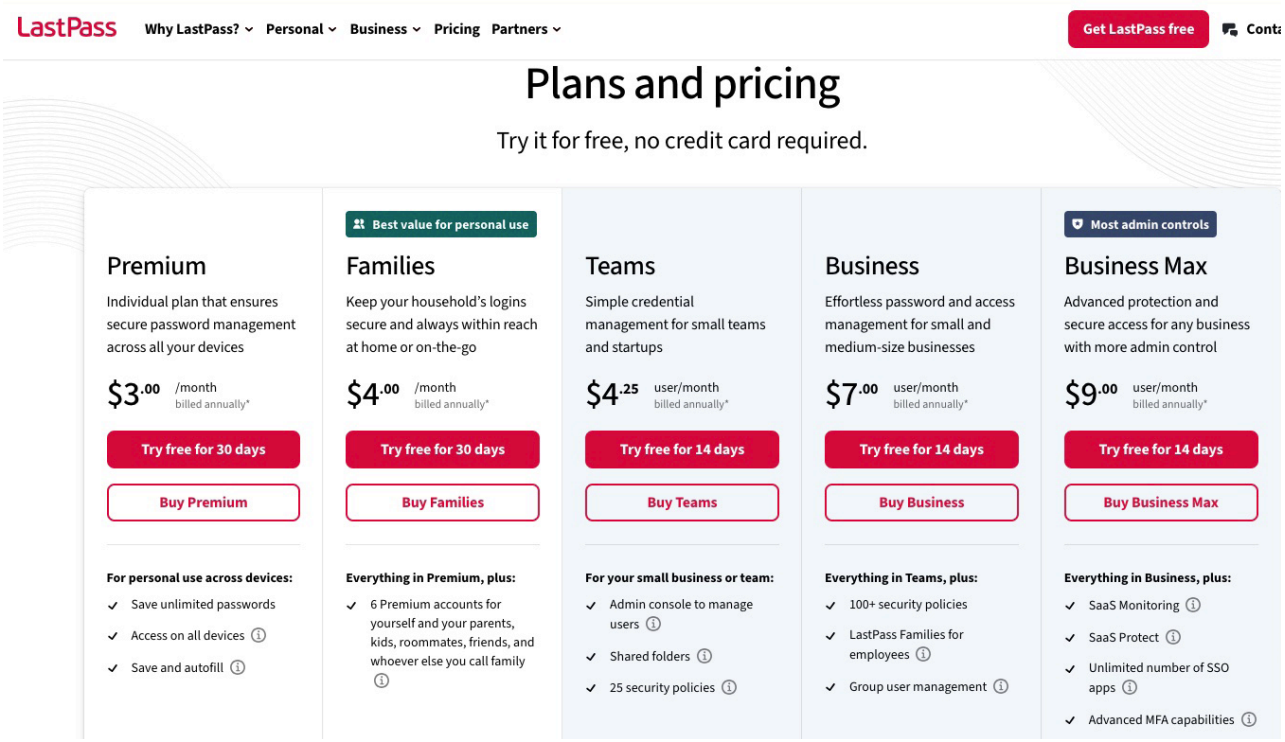
There are plenty of choices to get precisely what you need. Easy to talk to and have always been very helpful. I have had 4 serious identity theft attempts and each time LifeLock got it straightened out with no cost to me.

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.



CONTACT CREDIT BUREAUS

EQUIFAX
1-888-298-0045
equifax.com

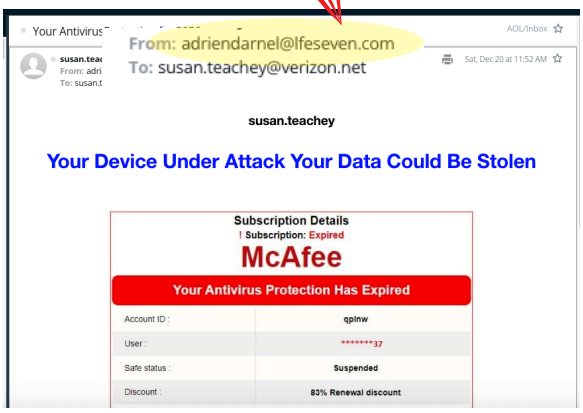
EXPERIAN
1-888-397-3742
experian.com

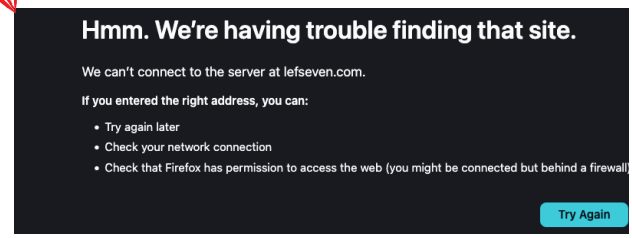
TRANSUNION
1-800-916-8000
transunion.com

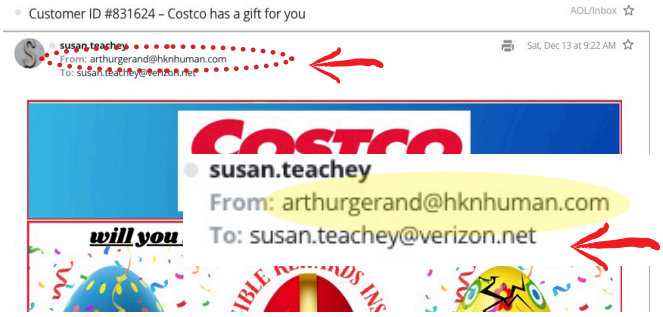
For an even deeper dive into Scams and Frauds can be found in this link:
https://www.pewresearch.org/internet/2025/07/31/online-scams-and-attacks-in-america-today/

The following pages have screenshots and notes of where to look in an email, text, or phone call.

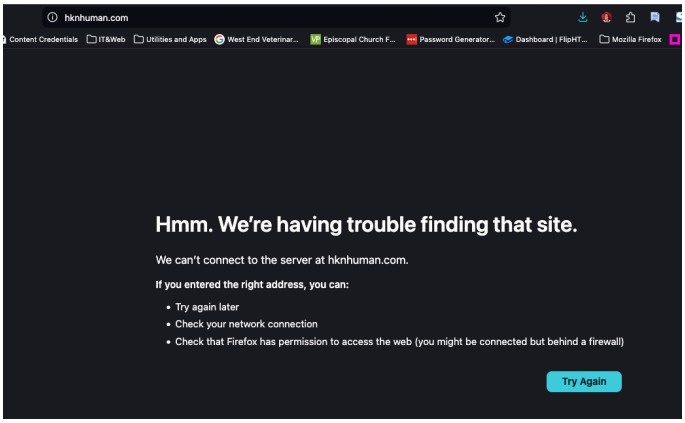
If an email comes through such as this, it is a **SCAM**. Remember to look at the "From" name. ***Not sure?*** Search for the website online. This one is "lefseven.com" as shown in the email. The result is



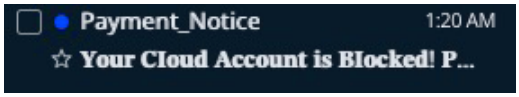




Emails such as this are a scam. Look at the "from line" in the email. If the "@" is like alphabet soup, that's a flag. Don't Click Anything. **DELETE IT.**

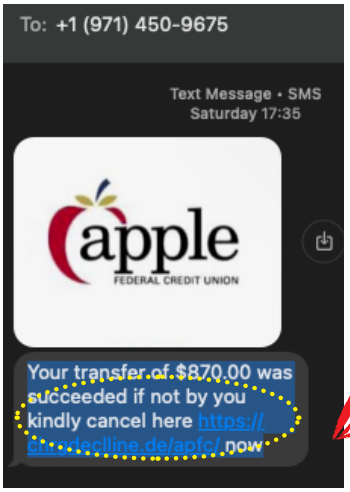


NOT CERTAIN? Type in the text after the "@" in your browser and see if anything comes up.



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

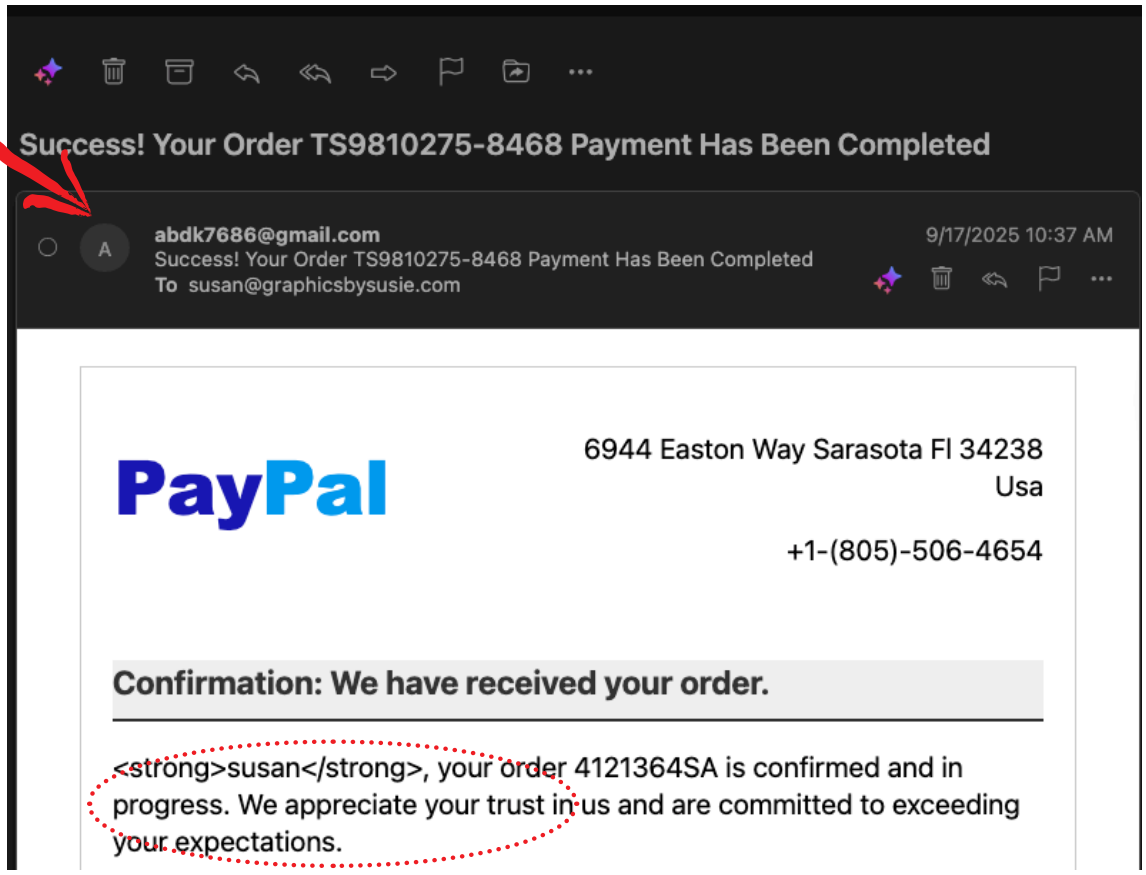
Pay close attention to the typeface in an email to see if looks different than your regular emails.

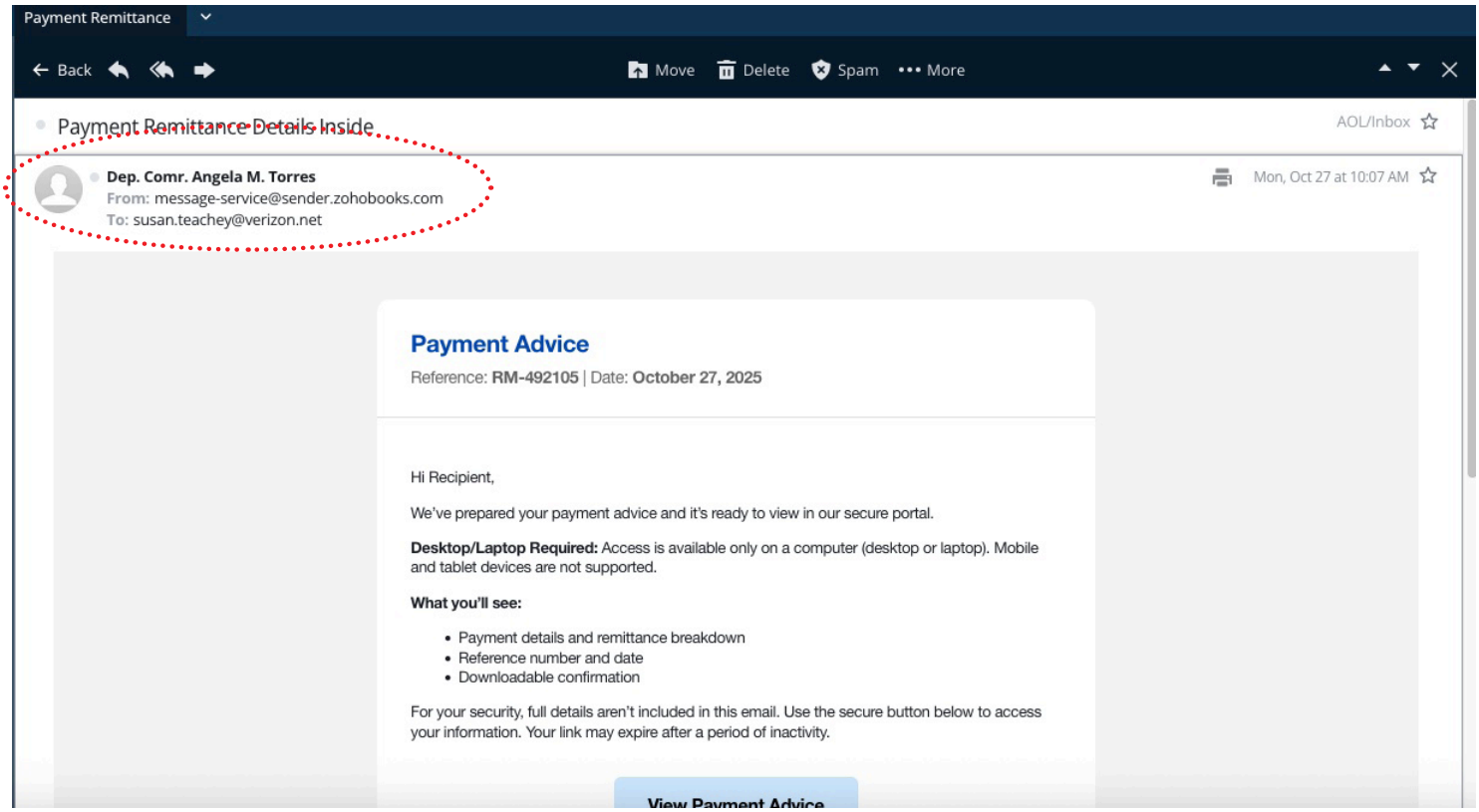


DON'T CLICK IT!
Delete It & Block the Number.

As you can see, the attempts are becoming more and more “legitimate and sophisticating 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.

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

Dropbox Sign

ACTION REQUESTED

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

Review & sign

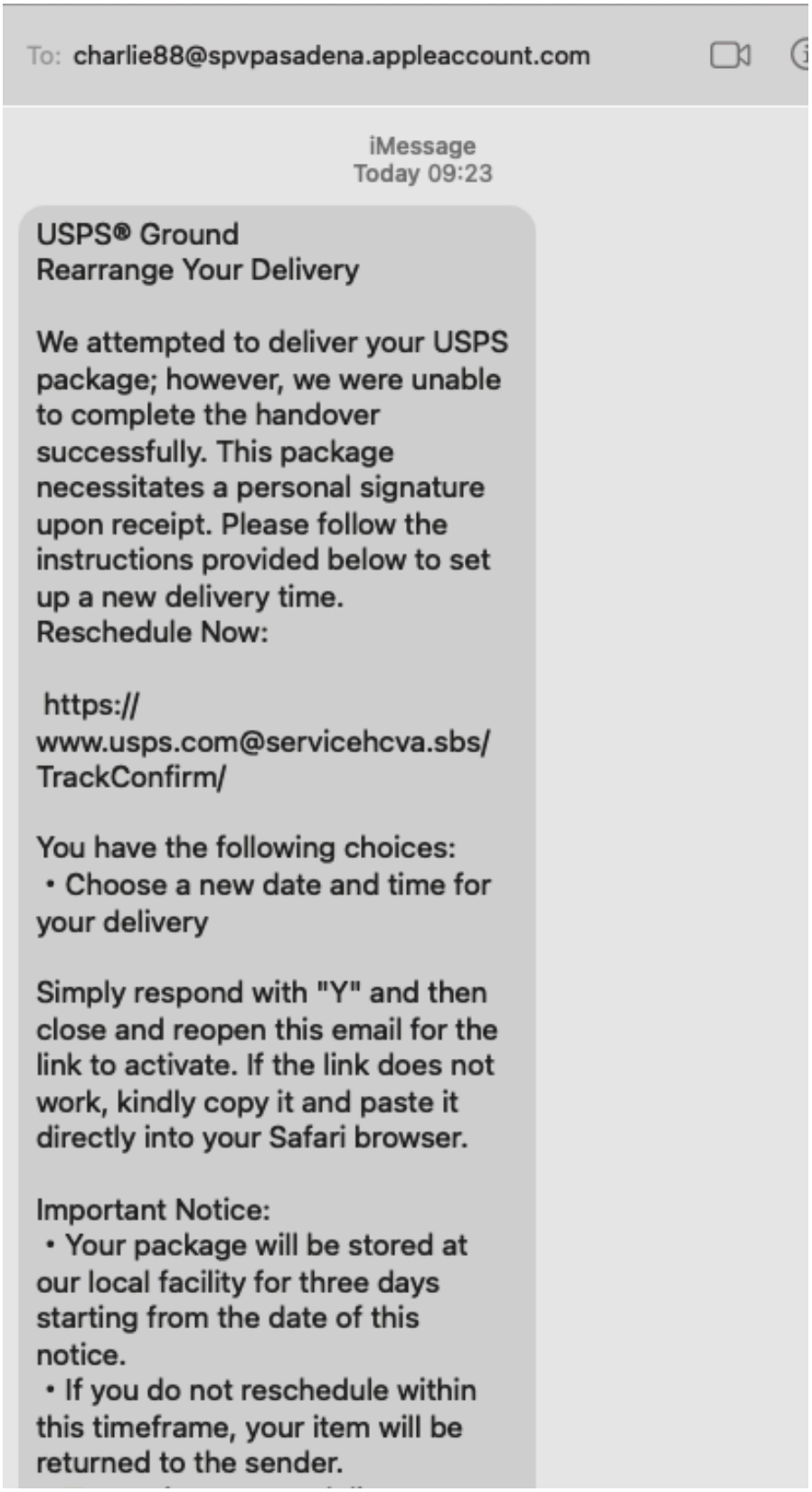
Document
Confirmation of Recent Bitcoin Purchase

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/
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.

NOTES