

How to Avoid Scams and Fraud

Carefull

October 2026

Americans are losing billions to fraud and scams

18 million
The number of identity fraud reports filed in 2024

$27 billion
The amount lost to identity fraud in 2025

$38 billion
Total annual fraud and scam losses to Americans

10.4 hours
The average amount of time victims spend resolving identity fraud

Sources: AARP, Javelin, FTC

If you know about it, you're 80% less likely to engage in the scam

Source: FBI Internet Crime Complaint Center

Common Scams

- Imposter scams
- Online shopping scams
- Investment scams
- Lottery and sweepstakes scams
- Job scams
- Romance scams
- Tech support scams
- Emergency/person-in-need scams



Newer Scams



- AI voice scams
- Text message scams
- Zelle and payment app scams
- Facebook Marketplace scams
- “Can you hear me?” scams
- Check washing

AI Voice Scams



- Scammers are using AI voice cloning technology to sound like family members in need and ask for money.
- Scammers often know what names and details to use because they've gathered that information through hacking or social media.
- Choose a code word to share with family that you can use to verify each other's identity.
- Use the Find My Friends app and send an invite to friends and family to find their locations.

Text Message Scams

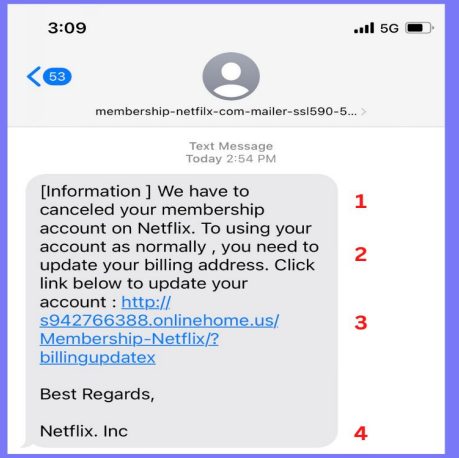
- Common text scams
  - Suspicious account activity scams
  - Relief and refund scams
  - Purchase and delivery scams
  - Retailer scams
  - Freebie scams

- What all of these scams have in common: They prompt you to take action by responding or clicking on a link.

- NEVER respond to or click on a link in an unsolicited text message.

Carefull

Can You Spot the Scam Red Flags?



1. Incorrect verb tense: have to canceled
2. Awkward grammar and unnecessary space before comma: To using your account as normally ,
3. Suspicious link
4. Incorrect punctuation: Netflix. Inc

Zelle and Payment App Scams



- Zelle and other payment apps such as Venmo, PayPal and CashApp appeal to scammers because they allow cash to be transferred almost instantly.

- Zelle scams typically begin with a text message that includes:
  - A claim there have been fraud attempts on your account;
  - A request to verify whether a payment was made; or
  - A request to verify your identity with your password

- The aim is to get victims to reveal their account login credentials or send thieves money.

Facebook Marketplace Scams

- These scams happen in a variety of ways, but the aim is to collect a payment without providing a good or to buy a good without making a payment.

- Signs of Facebook Marketplace scams:
  - Too-good-to-be-true price
  - Request for payment upfront, often through a payment app such as Venmo
  - Request to take communications off Facebook to keep them private
  - Overpayment for an item with a request to refund the difference
  - Newly created (fake) Facebook accounts

- How to avoid: Meet the seller or buyer in person, don’t pay upfront, don’t accept overpayments, don’t share personal information

“Can you hear me?” Scams

- Starts with a call from a number that appears to be local, and the caller asks “Can you hear me?” or a question to get you to answer “yes.”
- The caller records your response. The aim is to confirm that it is an active number, which can then be sold to scammers, or to use your “yes” to authorize purchases or sign you up for services you don’t want.
- Hang up if prompted to answer “Can you hear me?”
- Install a spam blocker and let calls go to voicemail.



Check Washing Scams



- Thieves are stealing checks from mailboxes and washing them in chemicals or altering them digitally to change names of recipients and amounts and depositing them.
- Victims often don’t realize their checks have been stolen until they get notices from companies that their bills weren’t paid.
- Set up automatic payments for as many bills as possible to eliminate the need to put checks in the mails.
- Use blue collection boxes inside the post office when mailing checks.
- Never leave mail in your mailbox overnight.

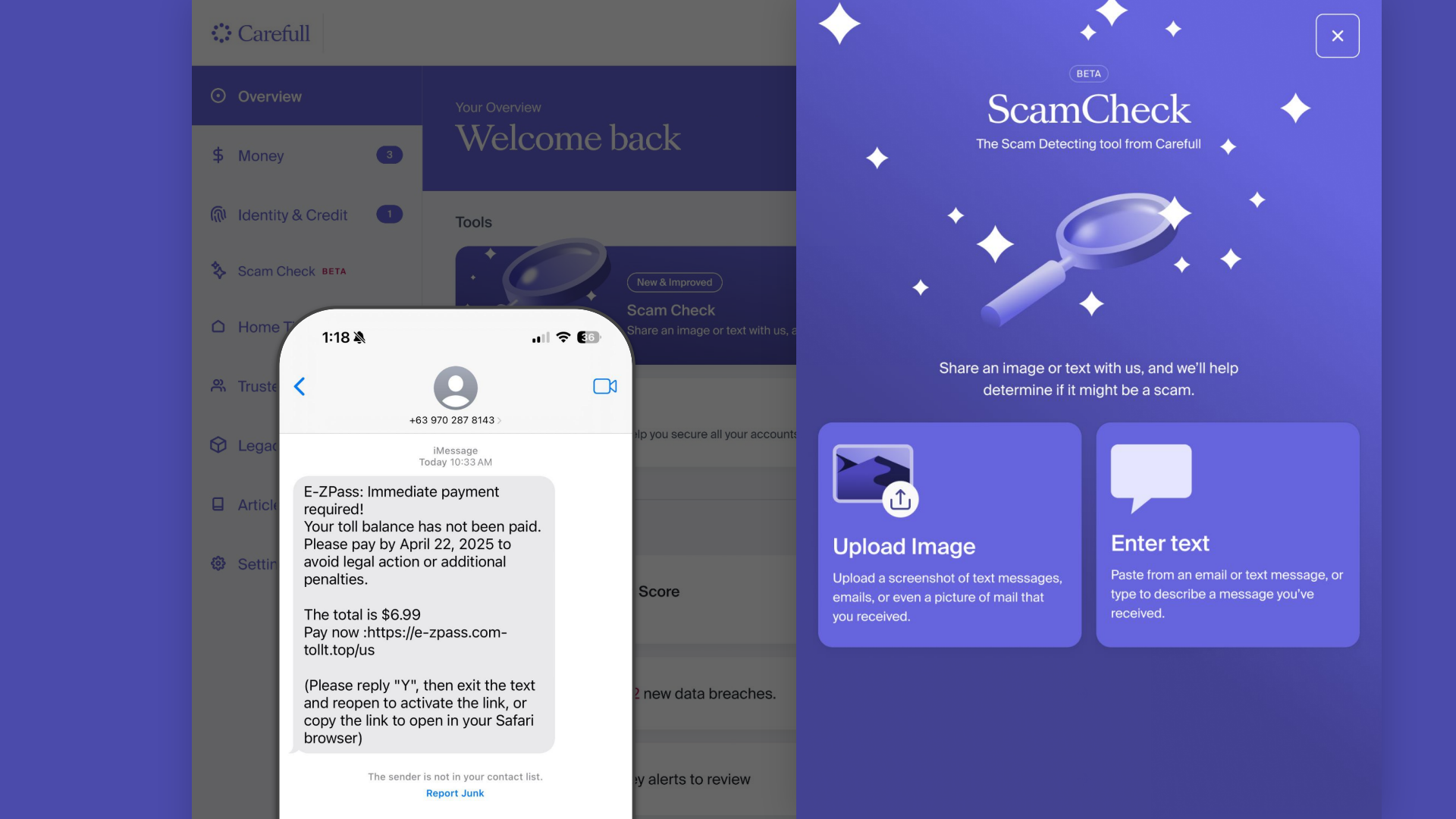
Scam Red Flags

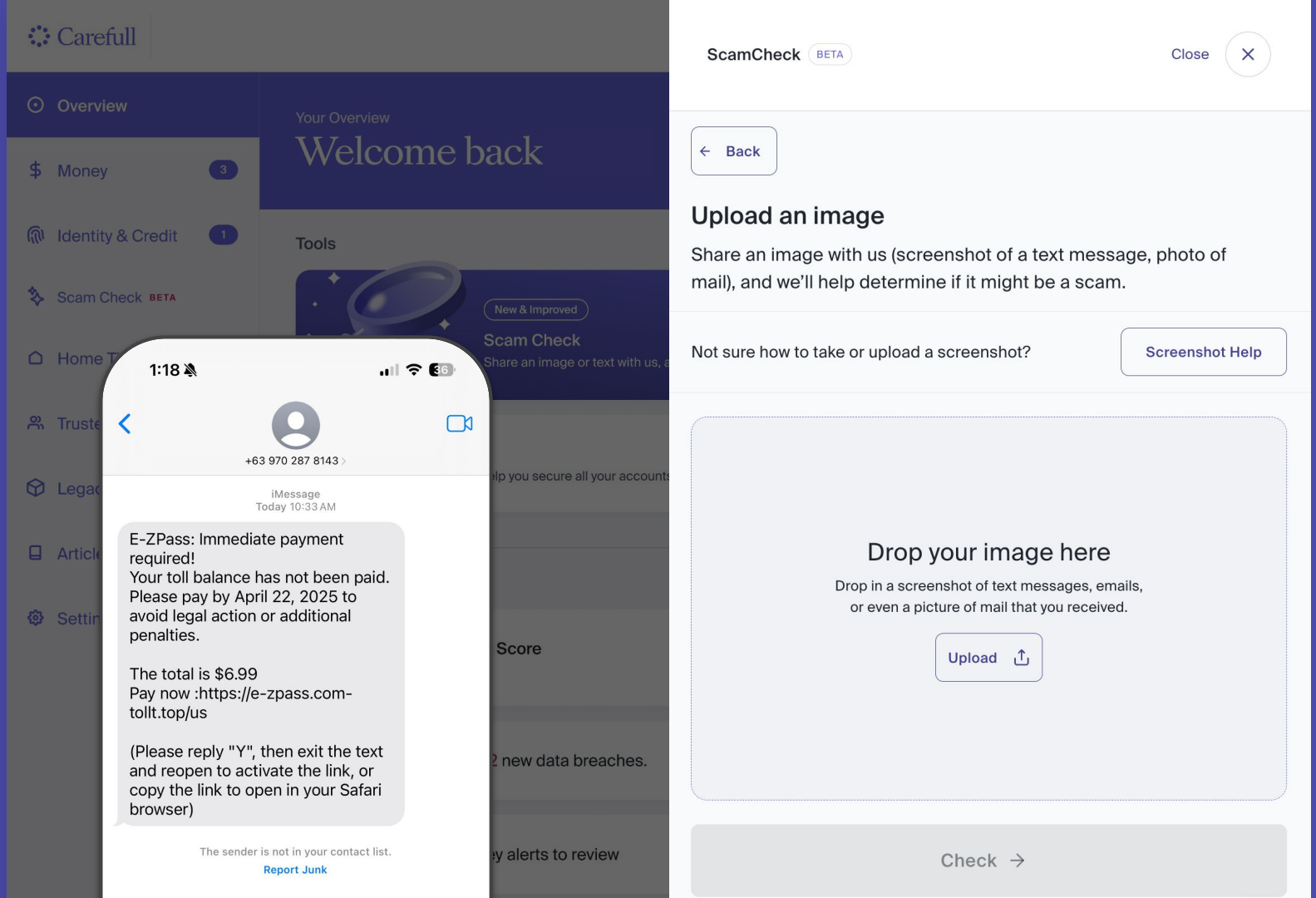
- ✓ Requests for specific payment type: wire transfer, gift card or payment app
- ✓ Unsolicited calls asking for personal information
- ✓ Calls from government agencies
- ✓ Emails or text messages with an urgent call to action
- ✓ Claim of overpayment and request for refund
- ✓ Limited-time offers and high-pressure sales tactics
- ✓ Offers of investments with high returns and no risk
- ✓ Requests to open a bank account for someone else
- ✓ Someone who initiates a relationship online, won't meet in-person then asks for money

How Carefull can help you to avoid these Scams



- **Carefull ScamCheck**
- Educational Content Library
- Smart Financial Account Protections
- 24/7 Dark Web Monitoring
- Spam Call Blocker


Carefull
Overview
Money
3
Identity & Credit
1
Scam Check
BETA
Your Overview
Welcome back
Tools
New & Improved
Scam Check
Share an image or text with us, a
1:18
+63 970 287 8143
iMessage
Today 10:33 AM
E-ZPass: Immediate payment required!
Your toll balance has not been paid. Please pay by April 22, 2025 to avoid legal action or additional penalties.
The total is $6.99
Pay now :https://e-zpass.com-tollt.top/us
(Please reply "Y", then exit the text and reopen to activate the link, or copy the link to open in your Safari browser)
The sender is not in your contact list.
Report Junk
BETA
ScamCheck
The Scam Detecting tool from Carefull
Share an image or text with us, and we'll help determine if it might be a scam.
Upload Image
Upload a screenshot of text messages, emails, or even a picture of mail that you received.
Enter text
Paste from an email or text message, or type to describe a message you've received.


Carefull
Overview
Money
3
Identity & Credit
1
Scam Check BETA
Your Overview
Welcome back
Tools
New & Improved
Scam Check
Share an image or text with us,
1:18
+63 970 287 8143
iMessage
Today 10:33 AM
E-ZPass: Immediate payment required!
Your toll balance has not been paid. Please pay by April 22, 2025 to avoid legal action or additional penalties.
The total is $6.99
Pay now :https://e-zpass.com-tollt.top/us
(Please reply "Y", then exit the text and reopen to activate the link, or copy the link to open in your Safari browser)
The sender is not in your contact list.
Report Junk
Score
new data breaches.
alerts to review
ScamCheck BETA
Close
Back
Upload an image
Share an image with us (screenshot of a text message, photo of mail), and we'll help determine if it might be a scam.
Not sure how to take or upload a screenshot?
Screenshot Help
Drop your image here
Drop in a screenshot of text messages, emails, or even a picture of mail that you received.
Upload
Check

Carefull

Overview

Money 3

Identity & Credit 1

Scam Check BETA

Home Title

Trusted Contacts

Legacy Kit

Articles

Settings

Your Overview

Welcome back

Tools

New & Improved

Scam Check

Share an image or text with us, a

Hack Recovery

Been hacked? We'll help you secure all your accounts

3 For your attention

70 Your Protection Score

3 tasks to 100

We've detected 2 new data breaches.

You have 3 money alerts to review

ScamCheck BETA

Close

Back

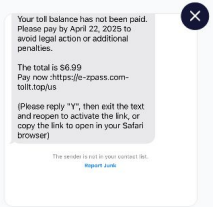
Upload an image

Share an image with us (screenshot of a text message, photo of mail), and we'll help determine if it might be a scam.

Not sure how to take or upload a screenshot?

Screenshot Help

We will analyze this image:



Check →

Carefull

Overview

Money 3

Identity & Credit 1

Scam Check BETA

Home Title

Trusted Contacts

Legacy Kit

Articles

Settings

Your Overview

Welcome back

Tools

New & Improved

Scam Check

Share an image or text with us, a

Hack Recovery

Been hacked? We'll help you secure all your accounts

3 For your attention

70 Your Protection Score

3 tasks to 100

We've detected 2 new data breaches.

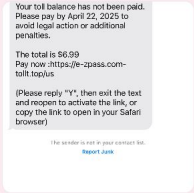
You have 3 money alerts to review

ScamCheck BETA

Close

High Risk

Likely a scam



This looks like a Unpaid Toll Scam. You should block this number and don't respond.

Save results as PDF

Was this answer helpful? Yes No

What you should do

1 **Do Not Click the Link**

Avoid clicking on any links in the message as they may lead to phishing sites.

2 **Report the Message**

Report the message as spam to your mobile carrier and block the sender.



What is Identity Theft

- Identity theft is the unauthorized use of someone's personal information for financial gain.
- Thieves can make purchases with your credit card, drain your bank account, open new accounts in your name, steal tax refunds or Social Security benefits, use your insurance for medical care.
- Information Identity Thieves are after:
  - Names
  - Addresses
  - Birthdates
  - Social Security Numbers
  - Health insurance or Medicare account numbers
  - Bank and credit card account numbers.

Avoiding Identity Theft

- Keep personal documents and information safe
- Set up online access to financial accounts, and create a SSA.gov account
- Use strong, unique passwords for each account and multi-factor authentication
- Be careful about sharing your SSN; don't carry your SSN card with you
- Install antivirus software on your computer, and run operating system updates on mobile devices
- Visit annualcreditreport.com to check your credit report for accounts you don't recognize
- Sign up for **Carefull**



Signs You’re a Victim of ID Theft

✓ Unusual activity in your bank or credit card account

✓ Collection notices or bills from unknown lenders

✓ Missing bills

✓ Missing Social Security payments

✓ Strange medical bills or insurance statements

✓ Unfamiliar account login alerts

✓ Unusual changes to your credit score or credit report

✓ Unreasonable denial of credit

✓ Rejected tax return or missing refund

✓ A warrant for your arrest

What to Do if You're a Victim

✓ Alert bank, credit card company to fraudulent charges—you are not liable for unauthorized charges

✓ Alert companies to fraudulent accounts and close them

✓ Place a security freeze on your credit reports at Equifax, Experian and TransUnion

✓ Get copies of your credit reports to look for more fraudulent accounts

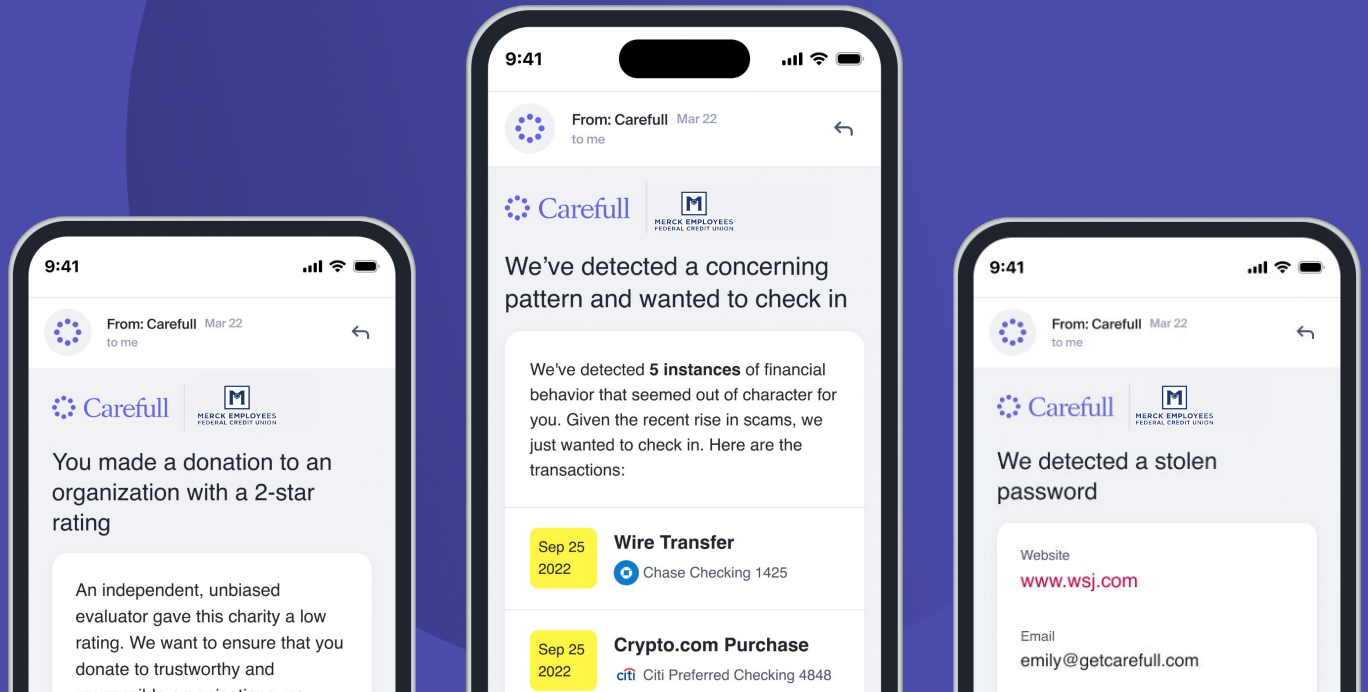
✓ Report fraud to IdentityTheft.gov

✓ Report to local law enforcement, and get a copy of the report

✓ Report fraud to government agencies (ex. report tax fraud to the IRS)

How Carefull Can Help

Account Monitoring | Credit Monitoring | Identity Monitoring | Home Title Monitoring | Data Breach Detection | Scam Check



Carefull

care@getcarefull.com