

UNITED STATES OF AMERICA FEDERAL TRADE COMMISSION WASHINGTON, DC 20580

Bureau of Consumer Protection Division of Marketing Practices Lois C. Greisman Associate Director (202) 326-3404 Igreisman@ftc.gov

March 27, 2025

Via Email

Dominet Limited

Email: DomainAbuse@service.aliyun.com

Re: Impersonation of the Federal Trade Commission and Unauthorized Use of its Logo by Domains Registered by Dominet Limited

To Whom It May Concern:

I write to inform you that a third domain registered by Dominet Limited appears to be perpetrating a deceptive impersonation scheme that utilizes the Federal Trade Commission's (FTC) name, logo, and website content without authorization. My previous letters to you are attached to this letter as Attachment A. I request that Dominet Limited provide information regarding the websites' registrants, and also request further details regarding any steps Dominet Limited has taken to fulfill their contractual obligations with ICANN to investigate and mitigate domain name system (DNS) abuse.

As shown in the screenshots included in Attachment B to this letter, the website FTC.ReportFraud.tech is nearly identical to FTC.ReportFraud.site and FTC.ReportFraud.work (discussed in my previous letters), which were also registered by Dominet Limited. As with FTC.ReportFraud.site and FTC.ReportFraud.work, the new domain closely mirrors the layout, wording, and design of the FTC's own website, reportfraud.ftc.gov. FTC.ReportFraud.tech prominently displays the name "Federal Trade Commission" in its upper lefthand side and displays a replica of the FTC's logo in the upper left and bottom right corners of its webpages, just as FTC.ReportFraud.site and FTC.ReportFraud.work did.

Like FTC.ReportFraud.site and FTC.ReportFraud.work, FTC.ReportFraud.tech also carries the images of a supposed law firm that purportedly works with the FTC to recover losses for victims of online fraud. The FTC does not work with any law firms to recover losses for fraud victims, and consumers risk being directed to a fake law firm where they may again fall victim to a re-scam.

The FTC is not affiliated with the entities or individuals operating these domains. Please be advised that it is a violation of the Rule on Impersonation of Government and Businesses ("Impersonator Rule"), 16 C.F.R. § 461, to "materially and falsely pose as, directly or by implication, a government entity or officer."

We appreciate the cooperative responses dated January 27, 2025 and March 20, 2025 from Alibaba Cloud Enforcement Enquiry ("Alibaba") to my above-referenced letters advising us that the domains FTC.ReportFraud.site and FTC.ReportFraud.work were suspended.

Given that we have now made you aware of three nearly identical domains impersonating our agency, we would appreciate Dominet Limited and Alibaba's continued attention to this matter. Specifically, please respond to our request for information as to whether Dominet Limited or Alibaba has (1) identified any other domains associated with the registrant of these domains and (2) undertaken any investigation into these domains pursuant to your contractual obligations with ICANN.

We also request all WHOIS data for FTC.ReportFraud.tech, FTC.ReportFraud.site, and FTC.ReportFraud.work.

We hope to hear from you promptly regarding this important consumer protection matter. Please direct any questions, and a copy of your response, to Virginia Rosa, vrosa@ftc.gov, 202-326-3068.

Sincerely,

/s/ Lois C. Greisman Lois C. Greisman

Attachments:

Attachment A: Jan. 24, 2025 Letter from L. Greisman to Dominet Limited

Feb. 28, 2025 Letter from L. Greisman to Dominet Limited

Attachment B: Web captures of FTC.ReportFraud.work



UNITED STATES OF AMERICA FEDERAL TRADE COMMISSION WASHINGTON, DC 20580

Bureau of Consumer Protection Division of Marketing Practices Lois C. Greisman Associate Director (202) 326-3404 Igreisman@ftc.gov

February 28, 2025

Via Email

Dominet Limited

Email: DomainAbuse@service.aliyun.com

Re: Impersonation of the Federal Trade Commission and Unauthorized Use of its Logo by Domains Registered by Dominet Limited

To Whom It May Concern:

I write to inform you that another domain registered by Dominet Limited appears to be perpetrating a deceptive impersonation scheme that utilizes the Federal Trade Commission's (FTC) name, logo, and website content without authorization. (*See attached* Jan. 24, 2025 Letter from L. Greisman to Dominet Limited).

As shown in the attached screenshots, the website FTC.ReportFraud.work is nearly identical to FTC.ReportFraud.site, which was also registered by Dominet Limited until it was taken down after the FTC's January 2025 letter. As with FTC.ReportFraud.site, the new domain closely mirrors the layout, wording, and design of the FTC's own website, reportfraud.ftc.gov. FTC.ReportFraud.work prominently displays the name "Federal Trade Commission" in its upper lefthand side and displays a replica of the FTC's logo in the upper left and bottom right corners of its webpages.

The website also carries the images of a supposed law firm that purportedly works with the FTC to recover losses for victims of online fraud. The FTC does not work with any law firms to recover losses for fraud victims, and consumers risk being directed to a fake law firm where they may again fall victim to a re-scam.

The FTC is not affiliated with the entities or individuals operating this website. Please be advised that it is a violation of the Rule on Impersonation of Government and Businesses ("Impersonator Rule"), 16 C.F.R. § 461, to "materially and falsely pose as, directly or by implication, a government entity or officer."

We expect to hear from Dominet Limited regarding this urgent consumer protection matter promptly. Please direct any questions, and a copy of your response, to Virginia Rosa, vrosa@ftc.gov, 202-326-3068.

Sincerely,

/s/Lois C. Greisman Lois C. Greisman

Q



FTC Consumer Financial Protection Bureau Cyber Fraud Investigation Division

Report Disaster Fraud and Price Gouging Here

FAQs

Languages



Report to help fight fraud!

Report Now →



The FTC is investigating and seizing \$200 million in illegal funds. Please don't be fooled again.

Learn More

View progress

The FTC will never demand money, make threats, tell you to transfer money, or promise you a prize. If you have been targeted by an illegal business practice or scam, report it.

Report to the FTC



With over 30 years of combined experience, Smith Allen LLP proudly offers customized services to meet the needs of clients in Canada, the United States and Israel in tax and estate planning, U.S. real estate, Quebec real estate, Internet fraud and U.S. immigration matters.

Our team of experienced attorneys and notaries, with offices in Montreal, Toronto, Florida and California, is uniquely positioned to recommend and implement strategies that meet the legal and tax requirements of clients in all three countries.

The Smith Allen LLP team is led by Alan Garrett Smith, whose highly developed expertise, extensive knowledge, meticulous attention to detail and commitment to client service enable us to provide the best possible outcomes for our clients and their families in the United States and Israel. Smith Allen LLP has worked with the FTC over the years to recover losses for thousands of victims of online fraud. Let us work together to maintain the safety of the Internet and protect the safety of people's property is our mission.

Get started now. Or you can browse our FAQs.



Scammers are impersonating the FTC. Know that the FTC will never threaten you, say you must transfer your money to "protect it," or tell you to withdraw cash or buy gold and give it to someone. Learn more at ftc.gov/impersonators



Fraudsters are now using individuals seeking remote work to scam millions of dollars in cryptocurrency.

We are helping victims recover funds from a new cryptocurrency scam disguised as remote work.



Brooklyn Woman Falls Victim to Tech Support

Scam, Loses \$100,000 A meticulously orchestrated scam left a retired accountant from Brooklyn \$100,000 poorer.



Scammers stole more than USD 1.2 billion from Asian consumers in 2022.

We speak to victims of fraud and share tips on how to avoid being duped.



Georgina's Fight Against

a Costly Romance Scam Georgina's children signed her up for Facebook and gave her some basic

lessons on how to use it.



Start your report now, or check out what is going on in your state or metro area by visiting **ftc.gov/exploredata**.

ReportFraud.ftc.gov is the federal government's website where you can report fraud, scams, and bad business practices.

Visit consumerate.gov to find tips and learn how to avoid scams.

Privacy Policy



FEDERAL TRADE COMMISSION ReportFraud.ftc.gov

SMITH ALLEN LLP

valid OMB control number.

950 Stockton St., San Francisco, CA 94018 (352)999-9311 https://www.facebook.com/FTCJuniperElowen/

FTC Fraud Complaint Center 600 Pennsylvania Avenue NW, Washington, DC 20580 (386)867-7777

https://www.facebook.com/FTCJuniperElowen/

OMB CONTROL#: 3084-0169 Under the Paperwork Reduction Act, federal agencies are not allowed to collect information from the public without a







FTC Consumer Financial Protection Bureau Cyber Fraud Investigation Division

Search FAQs on ReportFraud.ftc.gov

Capages

Español

Report Now

Report Disaster Fraud and Price Gouging Here



Report to help fight fraud!



FAQs





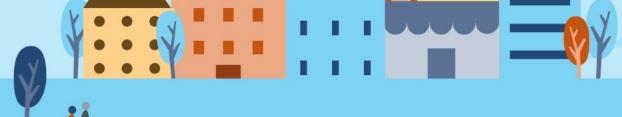
Protect your community by reporting fraud, scams, and bad business practices.

URL

https://ftc.reportfraud.tech/

Timestamp

Wed Mar 26 2025 12:03:42 GMT-0400 (Eastern Daylight Time)







Protect your community by reporting fraud, scams, and bad business practices.

The FTC is investigating and seizing \$200 million in illegal funds. Please don't be fooled again.

Learn More

View progress

The FTC will never demand money, make threats, tell you to transfer money, or promise you a prize. If you have been targeted by an illegal business practice or scam, report it.

Report to the FTC



With over 30 years of combined experience, Smith Allen LLP proudly offers customized services to meet the needs of clients in Canada, the United States and Israel in tax and estate planning, U.S. real estate, Quebec real estate, Internet fraud and U.S. immigration matters.

Our team of experienced attorneys and notaries, with offices in Montreal, Toronto, Florida and California, is uniquely positioned to recommend and implement strategies that meet the legal and tax requirements of clients in all three countries.

The Smith Allen LLP team is led by Alan Garrett Smith,

URL

https://ftc.reportfraud.tech/



positioned to recommend and implement strategies that meet the legal and tax requirements of clients in all three countries.

The Smith Allen LLP team is led by Alan Garrett Smith, whose highly developed expertise, extensive knowledge, meticulous attention to detail and commitment to client service enable us to provide the best possible outcomes for our clients and their families in the United States and Israel. Smith Allen LLP has worked with the FTC over the years to recover losses for thousands of victims of online fraud. Let us work together to maintain the safety of the Internet and protect the safety of people's property is our mission.

Get started now. Or you can browse our FAQs.



Scammers are impersonating the FTC. Know that the FTC will never threaten you, say you must transfer your money to "protect it," or tell you to withdraw cash or buy gold and give it to someone.

Learn more at ftc.gov/impersonators

URL

https://ftc.reportfraud.tech/

Timestame

transfer your money to "protect it," or tell you to withdraw cash or buy gold and give it to someone.

Learn more at ftc.gov/impersonators



Fraudsters are now using individuals seeking remote work to scam millions of dollars in cryptocurrency.

We are helping victims recover funds from a new cryptocurrency scam disguised as remote work.



Brooklyn Woman Falls Victim to Tech Support Scam, Loses \$100,000

A meticulously orchestrated scam left a retired accountant from Brooklyn \$100,000 poorer.



Scammers stole more than USD 1.2 billion from Asian consumers in 2022.

We speak to victims of fraud and share tips on how to avoid being duped.



<u>Georgina's Fight Against a</u> <u>Costly Romance Scam</u>

Georgina's children signed her up for Facebook and gave her some basic lessons on how to use it.



URL

https://ftc.reportfraud.tech/

Timestami

Wed Mar 26 2025 12:03:42 GMT-0400 (Eastern Daylight Time)



Start your report now, or check out what is going on in your state or metro area by visiting ftc.gov/exploredata.

ReportFraud.ftc.gov is the federal government's website where you can report fraud, scams, and bad business practices.

Visit consumer.ftc.gov to find tips and learn how to avoid scams.

Privacy Policy



SMITH ALLEN LLP

950 Stockton St., San Francisco, CA 94018 (352)999-9311

https://www.facebook.com/FTCJuniperElowen/

FTC Fraud Complaint Center

URL

https://ftc.reportfraud.tech/

Timestami

Wed Mar 26 2025 12:03:42 GMT-0400 (Eastern Daylight Time)

Visit <u>consumer.ftc.gov</u> to find tips and learn how to avoid scams.

Privacy Policy

URL

https://ftc.reportfraud.tech/

Timestamp

Wed Mar 26 2025 12:03:42 GMT-0400 (Eastern Daylight Time)

SMITH ALLEN LLP

950 Stockton St., San Francisco, CA 94018

(352)999-9311

https://www.facebook.com/FTCJuniperElowen/

FTC Fraud Complaint Center
600 Pennsylvania Avenue NW, Washington, DC 20580
(386)867-7777
https://www.facebook.com/FTCJuniperElowen/

OMB CONTROL#: 3084-0169

Under the Paperwork Reduction Act, federal agencies are not allowed to collect information from the public without a valid OMB control number.







FTC Consumer Financial Protection Bureau Cyber Fraud Investigation Division

Start	Submit
Is your report about any of these common problems? Choose the best fit. If you don't see your problem, choose "Something else."	
O An impersonator (ex. fake government, business, love interest, grandchild)	O Online shopping
O Job, investment, money-making opportunity, franchise	O Sweepstakes, prize, lottery
O Phone, internet, TV service	O Auto sale, repair
O Health (ex. weight loss, eye care, treatment)	O Credit, debt, loan (ex. debt collection, credit report, student loan debt relief)
O Just an annoying call	O Something else (we'll get it to the right place)
	Continue →

<u>ReportFraud.ftc.gov</u> is the federal government's website where you can report fraud, scams, and bad business practices.

Visit <u>consumer.ftc.gov</u> to find tips and learn how to avoid scams.



SMITH ALLEN LLP

URL

https://ftc.reportfraud.tech/one.html

Timestamp

Wed Mar 26 2025 12:04:39 GMT-0400 (Eastern Daylight Time)

<u>ReportFraud.ftc.gov</u> is the federal government's website where you can report fraud, scams, and bad business practices.

Visit consumer.ftc.gov to find tips and learn how to avoid scams.

Privacy Policy

URL

https://ftc.reportfraud.tech/one.html

Timestamp

Wed Mar 26 2025 12:04:39 GMT-0400 (Eastern Daylight Time)





SMITH ALLEN LLP

950 Stockton St., San Francisco, CA 94018 (352)999-9311

https://www.facebook.com/FTCJuniperElowen/

FTC Fraud Complaint Center 600 Pennsylvania Avenue NW, Washington, DC 20580 (386)867-7777

https://www.facebook.com/FTCJuniperElowen/

OMB CONTROL#: 3084-0169

Under the Paperwork Reduction Act, federal agencies are not allowed to collect information from the public without a valid OMB control number.







FTC Consumer Financial Protection Bureau Cyber Fraud Investigation Division

Start			Submit
Report details			
Please share as much as you know. The details help la	w enforcement investigations.		
Did you send the scammer payment of any kind?			
How much money did you pay the scammer in total?	\$		
How did you pay or send the money?	Select 🗸		
When did you encounter the scam (mm/dd/yyyy)?	mm-dd-yyyy		
How did it start (ex. how did they first contact you, where did you see an ad)?	Select 🗸		
Details about the scammer			
Please share as much as you know. The details help la	w enforcement investigations.		
Which government agency did they pretend to be?			
Name of the person you dealt with	Their First Name	Their Last Name	

URL

https://ftc.reportfraud.tech/two2.html

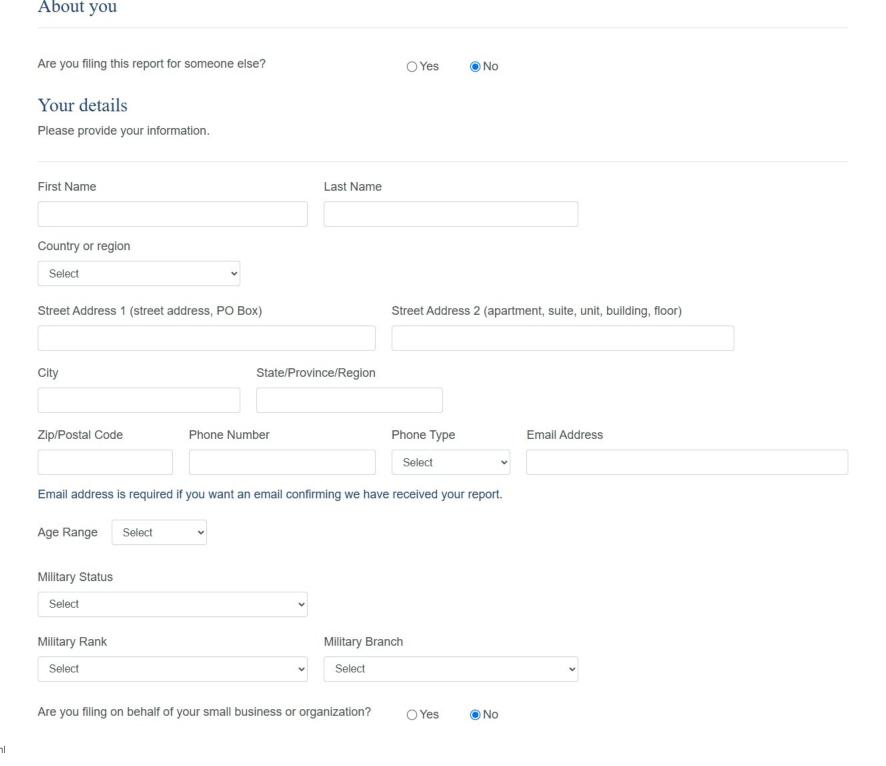
Details about the scammer								
Please share as much as you know. The details help	law enforcemer	nt investigation	ns.					
Which government agency did they pretend to be?								
Name of the person you dealt with	Their First Name		Their Last Name					
Do you know any other information about the scammer (phone, website, etc.)?	○ Yes	No						
Comments								
Describe what happened. Tell us what happened in your own words. Include specified not include any sensitive information, such as SSN history, etc.			oers, account r	numbers, medical				
0 characters of 3500 used				h				
About you								
Are you filing this report for someone else?		○Yes) No					

○ Yes

No

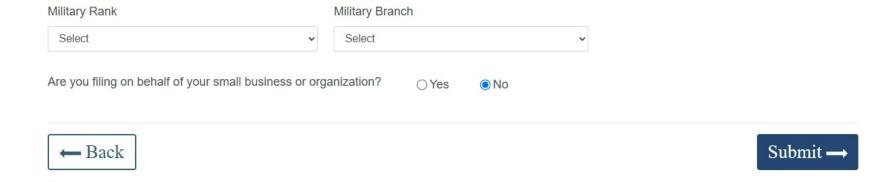
URL

https://ftc.reportfraud.tech/two2.html



URL

https://ftc.reportfraud.tech/two2.html



<u>ReportFraud.ftc.gov</u> is the federal government's website where you can report fraud, scams, and bad business practices.

Visit consumer.ftc.gov to find tips and learn how to avoid scams.

Privacy Policy



SMITH ALLEN LLP

950 Stockton St., San Francisco, CA 94018 (352)999-9311

https://www.facebook.com/FTCJuniperElowen/

FTC Fraud Complaint Center

600 Pennsylvania Avenue NW, Washington, DC 20580

(386)867-7777

https://www.facebook.com/FTCJuniperElowen/

OMB CONTROL#: 3084-0169

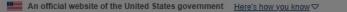
Under the Paperwork Reduction Act, federal agencies are not allowed to collect information from the public without a valid OMB control number.

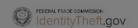
URL

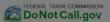
https://ftc.reportfraud.tech/two2.html

Timestamp

Wed Mar 26 2025 12:05:52 GMT-0400 (Eastern Daylight Time)

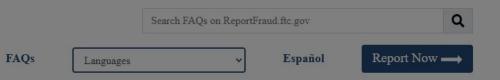




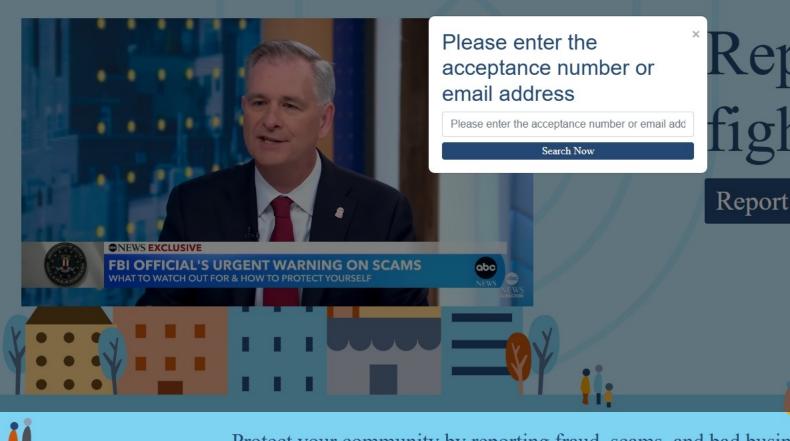




FTC Consumer Financial Protection Bureau Cyber Fraud Investigation Division



Report Disaster Fraud and Price Gouging Here



Report to help fight fraud!







Protect your community by reporting fraud, scams, and bad business practices.

URL

https://ftc.reportfraud.tech/







Protect your community by reporting fraud, scams, and bad business practices.

The FTC is investigating and seizing \$200 million in illegal funds. Please don't be fooled again.

Learn More

View progress

The FTC will never demand money, make threats, tell you to transfer money, or promise you a prize. If you have been targeted by an illegal business practice or scam, report it.

Report to the FTC



URL

Timestamp

https://ftc.reportfraud.tech/

With over 30 years of combined experience, Smith Allen LLP proudly offers customized services to meet the needs of clients in Canada, the United States and Israel in tax and estate planning, U.S. real estate, Quebec real estate, Internet fraud and U.S. immigration matters.

Our team of experienced attorneys and notaries, with offices in Montreal, Toronto, Florida and California, is uniquely positioned to recommend and implement strategies that meet the legal and tax requirements of clients in all three countries.

The Smith Allen LLP team is led by Alan Garrett Smith,



positioned to recommend and implement strategies that meet the legal and tax requirements of clients in all three countries.

The Smith Allen LLP team is led by Alan Garrett Smith, whose highly developed expertise, extensive knowledge, meticulous attention to detail and commitment to client service enable us to provide the best possible outcomes for our clients and their families in the United States and Israel. Smith Allen LLP has worked with the FTC over the years to recover losses for thousands of victims of online fraud. Let us work together to maintain the safety of the Internet and protect the safety of people's property is our mission.

Get started now. Or you can browse our FAQs.



Scammers are impersonating the FTC. Know that the FTC will never threaten you, say you must transfer your money to "protect it," or tell you to withdraw cash or buy gold and give it to someone.

Learn more at ftc.gov/impersonators

URL

https://ftc.reportfraud.tech/

Timestamo

Wed Mar 26 2025 12:07:12 GMT-0400 (Eastern Daylight Time)

transfer your money to "protect it," or tell you to withdraw cash or buy gold and give it to someone.

Learn more at ftc.gov/impersonators



Fraudsters are now using individuals seeking remote work to scam millions of dollars in cryptocurrency.

We are helping victims recover funds from a new cryptocurrency scam disguised as remote work.



Brooklyn Woman Falls Victim to Tech Support Scam, Loses \$100,000

A meticulously orchestrated scam left a retired accountant from Brooklyn \$100,000 poorer.



Scammers stole more than USD 1.2 billion from Asian consumers in 2022.

We speak to victims of fraud and share tips on how to avoid being duped.



<u>Georgina's Fight Against a</u> <u>Costly Romance Scam</u>

Georgina's children signed her up for Facebook and gave her some basic lessons on how to use it.



URL

https://ftc.reportfraud.tech/

Timestami

Wed Mar 26 2025 12:07:12 GMT-0400 (Eastern Daylight Time)



Start your report now, or check out what is going on in your state or metro area by visiting ftc.gov/exploredata.

ReportFraud.ftc.gov is the federal government's website where you can report fraud, scams, and bad business practices.

Visit consumer.ftc.gov to find tips and learn how to avoid scams.

Privacy Policy



SMITH ALLEN LLP

950 Stockton St., San Francisco, CA 94018 (352)999-9311

https://www.facebook.com/FTCJuniperElowen/

FTC Fraud Complaint Center

URL

https://ftc.reportfraud.tech/

Timestami

Wed Mar 26 2025 12:07:12 GMT-0400 (Eastern Daylight Time)

Visit <u>consumer.ftc.gov</u> to find tips and learn how to avoid scams.

Privacy Policy

URL

https://ftc.reportfraud.tech/

Timestamp

Wed Mar 26 2025 12:07:12 GMT-0400 (Eastern Daylight Time)

SMITH ALLEN LLP

950 Stockton St., San Francisco, CA 94018

(352)999-9311

https://www.facebook.com/FTCJuniperElowen/

FTC Fraud Complaint Center
600 Pennsylvania Avenue NW, Washington, DC 20580
(386)867-7777
https://www.facebook.com/FTCJuniperElowen/

OMB CONTROL#: 3084-0169

Under the Paperwork Reduction Act, federal agencies are not allowed to collect information from the public without a valid OMB control number.







FTC Consumer Financial Protection Bureau Cyber Fraud Investigation Division

Search FAQs on ReportFraud.ftc.gov

Español

Report Now -



URL

https://ftc.reportfraud.tech/pathIndex.html

Wed Mar 26 2025 12:08:21 GMT-0400 (Eastern Daylight Time)



Our Attorneys





















Our team approach ensures that each case is appropriately staffed and that each matter receives the resources necessary to obtain the best results possible on behalf of our clients.

CALL TODAY FOR A FREE CONSULTATION

(386) 867-7777 OR (352) 999-9311

URL

https://ftc.reportfraud.tech/pathIndex.html

Timestamp

Wed Mar 26 2025 12:08:21 GMT-0400 (Eastern Daylight Time)

JONES KELLEHER LLP Attorneys at Law

21 Custom House St., Boston, MA 02110 • PH: (386) 867-7777

One Center Place, Providence, RI 02903 • PH: (352) 999-9311

possible on behalf of our clients.

CALL TODAY FOR A FREE CONSULTATION

(386) 867-7777 OR (352) 999-9311

<u>ReportFraud.ftc.gov</u> is the federal government's website where you can report fraud, scams, and bad business practices.

Visit consumer.ftc.gov to find tips and learn how to avoid scams.

Privacy Policy



https://ftc.reportfraud.tech/pathIndex.html

Timestamp

Wed Mar 26 2025 12:08:21 GMT-0400 (Eastern Daylight Time)



SMITH ALLEN LLP

950 Stockton St., San Francisco, CA 94018 (352)999-9311

https://www.facebook.com/FTCJuniperElowen/

FTC Fraud Complaint Center 600 Pennsylvania Avenue NW, Washington, DC 20580 (386)867-7777

https://www.facebook.com/FTCJuniperElowen/

OMB CONTROL#: 3084-0169

Under the Paperwork Reduction Act, federal agencies are not allowed to collect information from the public without a valid OMB control number.



Shopping and Donating V

Credit, Loans, and Debt v

Jobs and Making Money v Unwanted Calls, Emails, and Texts v Identity Theft and Online Security V

Scams Q

Q

How To Avoid Imposter Scams

Home / Feature Pages

Vea esta página en español

The FTC will never threaten you, say you must transfer your money to "protect it," or tell you to withdraw cash or buy gold and give it to someone. That's a scam. Report it.

ReportFraud.ftc.gov

Anatomy of an Imposter Scam

Our "Anatomy of an Imposter Scam" blog series breaks down how to recognize, avoid, and report business and government imposter scams.

[Infographic]: How Scammers Try To Steal Your Life Savings



https://consumer.ftc.gov/features/how-avoid-imposter-scams

Anatomy of an Imposter Scam

Our "Anatomy of an Imposter Scam" blog series breaks down how to recognize, avoid, and report business and government imposter scams.

[Infographic]: How Scammers Try To Steal Your Life Savings



Never move your money to "protect it." That's a scam

If someone claims there's fraud or criminal activity on one of your accounts, and tells you to move money from your bank, investment, or retirement account to "protect it", it's a scam.



What's a verification code and why would someone ask me for it?

Scammers pretend to be someone you can trust and say they've discovered a problem with one of your accounts.

Then they ask for your verification code to get into your account. It's a scam.



Will your bank or investment fund stop a transfer to a scammer?

Scammers try to trick you into transferring your money to "protect" or "safeguard" or "legalize" it. If you do, your bank won't get it back from the scammer.









URL

https://consumer.ftc.gov/features/how-avoid-imposter-scams



Sure ways to spot a scammer

Scammers say and do things that can tell us they're lying. Here are some sure ways to recognize a scammer.



Did you get a call or text about a suspicious purchase on Amazon?

The scam starts with a call or text message about a suspicious charge on your Amazon account. But it's not really Amazon. It's a scammer who wants you to drain your accounts.



New tech support scammers want your life savings

The latest tech support scams: scammers tell you someone hacked your bank or investment account and is using it for fraud. And they pretend to transfer you to a government agency for "help." But it's all a scam.



Did someone send you to a Bitcoin ATM? It's a scam

Someone says they're from the government and tells you to "protect" your money by making a deposit at a Bitcoin ATM. Stop. It's a scam.

Government Impersonators

Someone who really works at the FTC won't tell you to move your money to protect it.

Report imposter scams.







URL

https://consumer.ftc.gov/features/how-avoid-imposter-scams

Someone who really works at the FTC won't tell you to move your money to protect it.

Report imposter scams.

ReportFraud.ftc.gov





Scammers impersonate FTC officials, including Chairman Andrew Ferguson

In the latest twist on these constantly evolving schemes, scammers are claiming to be FTC Chairman Andrew Ferguson.



Recognize business and government imposters who want your money

Scammers pretending to be from the government tell convincing stories to steal your money or personal information. But now they're taking a new, layered approach — and here are some clues to spot it.

3 Things Scammers Say

- Scammers tell you to move your money to protect it
- Scammers say you have to get cash and drop it off
- Scammers tell you to buy gold and give it to a courier



No one is using your Social Security number to commit crimes. It's a scam.

The phone rings. Your caller ID says it's the Social Security Administration. You hesitate. You're not expecting a call from them, and you've heard about impersonation scams. But something inside you makes you pick up. And everything you're about to hear is designed to scare you into doing whatever the caller says.

Anatomy of an Imposter Scam

Scammers tell you to move your money to "protect it." Don't do it.





Did someone demand money and say they're from the FTC?

They're not. That's a scammer.



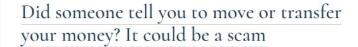
URL

https://consumer.ftc.gov/features/how-avoid-imposter-scams

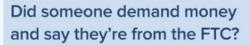
Scammers tell you to move your money to "protect it." Don't do it.







Many impersonation schemes start with a call about a routine problem, like suspicious activity in your Amazon account. But in a new twist, the story quickly takes a more serious turn when you're told someone is using your information to commit crimes and all your money is at risk.



They're not. That's a scammer.

Learn more:

ftc.gov/scams



The FTC won't demand money, threaten you, or promise you a prize

Scammers want to gain your trust. That's why they keep pretending to work for government agencies, including the Federal Trade Commission. They might use the names of real FTC employees, but the stories they tell are a bunch of lies.





URL

https://consumer.ftc.gov/features/how-avoid-imposter-scams



Government Impersonation Scams

Scammers pretend to be from government agencies like the FTC, Social Security Administration, and IRS — or say they're calling about your Medicare benefits.





Government Grant Scams

Offers of free money from government grants are scams. Here's how to avoid a government grant scam, and how to report it.

See all government impersonators

Business and Other Impersonators

How To Spot, Avoid, and Report Tech Support Scams

Tech support scammers want you to pay them to fix a non-existent computer problem. Learn how to avoid and report tech support scams.

How to recognize a fake Geek Squad renewal scam

Scammers are at it again, impersonating well-known businesses and trying to rip people off. This time they're pretending to be from Geek Squad, Best Buy's tech support service. Here's what we're hearing about the scam and what to do if you see it.

Fake calls from Apple and Amazon support: What you need to know

Scammers are calling people and using the names of two companies everyone knows, Apple and Amazon, to rip people off. Here's what you need to know about these calls.

URL

https://consumer.ftc.gov/features/how-avoid-imposter-scams

scalli aliu wilat to do il you see it.

Scammers Use Fake Emergencies To Steal Your Money

Someone calls or contacts you saying they're a family member or close friend. They say they need money to get out of trouble. But check that there's an emergency first because it could be a scammer calling.

What to Know About Romance Scams

Scammers strike up a relationship with you to build up trust, sometimes talking or chatting several times a day. Then, they make up a story and ask for money. Learn how to avoid romance scams.

Utility Company Impersonators

A call from your gas, electric, or water company threatening to immediately turn off your service is probably a scam. Here's what you need to know.

Job scam targeting influencers

Did you get a message from a "brand ambassador manager" for a national company wanting to pay you to promote their products online? It could be a scam...but how will you know?

Scammers impersonate delivery service support to rip off drivers and restaurants

We're hearing about a new scam targeting food delivery drivers and restaurants.

Nanny and Caregiver Job Scams

If you're looking for a job as a babysitter, nanny, or other kind of caregiver, you might have searched online or used a website that matches you up with potential employers.

Scammers also use these sites. Learn how to spot these fake jobs and avoid them.

URL

https://consumer.ftc.gov/features/how-avoid-imposter-scams

how to spot these fake jobs and avoid them.

See all business and other impersonators

Watch



Family Emergency Scams

The first-person story of how one family responded to a family emergency scam: by putting it on the radio.



Tech Support Scams

The first-person story about a retired business consultant's tech support scam experience, what he did about it.



Nanny and Caregiver Scams

Caregiver websites can help you find jobs, but scammers also use them to find people to rip off.



https://consumer.ftc.gov/features/how-avoid-imposter-scams

Timestame



Did you spot an impersonator scam?

Report it at ReportFraud.ftc.gov

Looking for information for older adults?

Check out ftc.gov/PassItOn



Consumer Alerts

Report Fraud Get Consumer Alerts

ftc.gov About Us Contact Us Privacy and Notices FOIA Office of Inspector General

0 A E 0 y

URL

https://consumer.ftc.gov/features/how-avoid-imposter-scams

Wed Mar 26 2025 12:09:04 GMT-0400 (Eastern Daylight Time)





FTC Consumer Financial Protection Bureau Cyber Fraud Investigation Division

Search FAQs on ReportFraud.ftc.gov

C

Languages

■ Español

Report Now →



FAQs

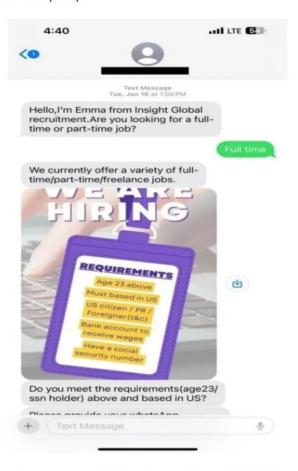
New York Attorney General Letitia James issued a statement on the 9th, saying that fraud groups are now taking advantage of people's opportunities to seek remote work to defraud millions of dollars worth of cryptocurrencies; she has filed a lawsuit to recover the hard-earned money that was stolen from the people.



URL

https://ftc.reportfraud.tech/info4.html

New York Attorney General Letitia James issued a statement on the 9th, saying that fraud groups are now taking advantage of people's opportunities to seek remote work to defraud millions of dollars worth of cryptocurrencies; she has filed a lawsuit to recover the hard-earned money that was stolen from the people.



According to a report from ABC News, Zhan Lexiong stated that a fraudulent group has been sending text messages to the public, promising well-paid, flexible jobs that can be done from home. The job involves reviewing products on a website to help generate "market data." However, to earn money, recipients are told that they must open a cryptocurrency account, and their account balance must be kept equal to or greater than the price of the products they are reviewing.

The fraudulent group first encourages victims to purchase USDC and USDT stablecoins on legitimate exchanges like Coinbase, Gemini, and Crypto.com. They then entice victims to send their cryptocurrency to an unmanaged digital wallet. Victims are assured that they can recover their invested funds and earn commissions; however, these funds only end up in the fraudsters' cryptocurrency wallet. The website where victims post reviews is also fake.

The seven victims involved in the lawsuit used aliases and live in New York, Virginia, and Florida. One woman in Florida lost over \$300,000, while a victim in New York was deceived out of more than \$100,000 after receiving a text message claiming the remote job had "great benefits"

URL

https://ftc.reportfraud.tech/info4.html

reviews is also fake.

The seven victims involved in the lawsuit used aliases and live in New York, Virginia, and Florida. One woman in Florida lost over \$300,000, while a victim in New York was deceived out of more than \$100,000 after receiving a text message claiming the remote job had "great benefits and flexible requirements," offering a sign-up bonus and a 25% commission for joining.

Then, a person impersonating a training instructor helped the victim set up a wallet on the LBank platform and guided them in connecting the wallet to a so-called "work account." When the victims attempted to withdraw their money, the fraudsters fabricated charges such as "credit score enhancement fees," "blockchain verification fees," and "custody fees," demanding that they deposit more coins, but ultimately never releasing any funds.

During the investigation, Zhan Lexiong's office received voluntary cooperation from Tether (the issuer of USDT) to freeze the stolen USDT. Queens District Attorney Melinda Katz stated that her office's cryptocurrency division tracked over \$2 million in stolen cryptocurrency and identified the wallet addresses where the funds were stored. They have obtained search warrants and are working with Zhan Lexiong's office to freeze the stolen USDC, which can be recovered and returned to the victims upon court approval.

<u>ReportFraud.ftc.gov</u> is the federal government's website where you can report fraud, scams, and bad business practices.

Visit consumer.ftc.gov to find tips and learn how to avoid scams.

Privacy Policy



SMITH ALLEN LLP

950 Stockton St., San Francisco, CA 94018 (352)999-9311

https://www.facebook.com/FTCJuniperElowen/

FTC Fraud Complaint Center 600 Pennsylvania Avenue NW, Washington, DC 20580 (386)867-7777

https://www.facebook.com/FTCJuniperElowen/

OMB CONTROL#: 3084-0169

Under the Paperwork Reduction Act, federal agencies are not allowed to collect information from the public without a valid OMB control number

URL

https://ftc.reportfraud.tech/info4.html

Timestamp





FTC Consumer Financial Protection Bureau Cyber Fraud Investigation Division

Search FAQs on ReportFraud.ftc.gov

FAQs

Languages

Español

Report Now -

Q



New York—

A meticulously orchestrated scam left a retired accountant from Brooklyn \$100,000 poorer. The scheme involved a suddenly frozen computer, an in-person meeting, and a secret code word.

URL

https://ftc.reportfraud.tech/info1.html



New York-

A meticulously orchestrated scam left a retired accountant from Brooklyn \$100,000 poorer. The scheme involved a suddenly frozen computer, an in-person meeting, and a secret code word.

The victim later spoke exclusively with CBS New York investigative reporter Mahsa Saeidi, sharing her story in hopes of warning others.

A Man Claiming to Be a Microsoft Employee Executes the Scam

The woman, who wished to remain anonymous, decided to share her story despite the overwhelming shame she felt. In her interview, she revealed, "I feel deeply humiliated. At one point, I even considered suicide."

The incident unfolded on a July afternoon when her laptop suddenly froze. Shortly afterward, she received a phone call from someone claiming to represent "Microsoft."

"The caller apologized, saying their system had a security flaw that allowed a virus to spread. They told me they wanted to refund the antivirus premium I had previously paid,", she recalled.

The man posing as a Microsoft employee then claimed he had mistakenly deposited \$100,000 into her account instead of the intended \$10 refund. He insisted she withdraw the excess funds and return them immediately to correct the "error."

Deceived and Losing Her Life Savings

The victim explained that when she checked her account, she did see an extra \$100,000 deposited. Wanting to "do the right thing," she followed the instructions provided and went to the bank to withdraw the cash.

At the bank, a teller asked if she was under duress, but she assured them she wasn't, leading to the withdrawal being approved.

A few hours later, she met with a "courier" arranged by the scammer. The fraudster told her the man would identify himself as "Andy" and use the code word "red." Trusting the instructions, she handed over an envelope containing \$100,000 in cash — a third of her life savings.

After realizing she had been scammed, the woman was filled with regret. "How could I have fallen for this?" she lamented.

T T 0 5 11 10 6 F 17 M 1 1 1 10 10 1 M

URL

A few hours later, she met with a "courier" arranged by the scammer. The fraudster told her the man would identify himself as "Andy" and use the code word "red." Trusting the instructions, she handed over an envelope containing \$100,000 in cash — a third of her life savings.

After realizing she had been scammed, the woman was filled with regret. "How could I have fallen for this?" she lamented.

The Truth Behind the Scam: Fraudsters Manipulated the Victim's Accounts

It was later revealed that the so-called "mistaken deposit" of \$100,000 was actually money transferred from the victim's own trust fund account to her personal checking account.

Unbeknownst to her, the scammers had accessed her financial information and manipulated her accounts to make it appear as though the funds came from an external source.

The woman said that when she visited the bank, no one informed her of the day's suspicious account activity. "All they needed to do was check the transfer records. When they asked me, 'Did you make a transfer?' I told them no," she explained.

This lack of timely intervention allowed the scammers to execute their plan, leaving the victim to deal with the devastating financial and emotional fallout.

Aftermath: Reporting the Scam and Seeking Justice

Upon realizing she had been scammed, the woman promptly reported the incident to the New York Police Department. The authorities verified the details and opened a formal investigation. Additionally, the case was referred to the Federal Trade Commission (FTC) for further review.

The victim has since enlisted the services of the law firm Jones Kelleher LLP, which is currently handling efforts to recover the lost funds. However, the financial and emotional toll of the incident remains significant.

How to Prevent Tech Support Scams

A Microsoft spokesperson stated that tech support scams are a major issue across the industry, but legitimate tech companies will never initiate contact with users or ask them to dial specific numbers.

Jeanine Launay, head of the Elder Abuse Unit at the Manhattan District Attorney's Office, advises the public: "If a pop-up window appears on your computer asking you to call a specific number, do not engage. The proper action is to immediately shut down your computer and unplug it."

Furthermore, if scammers have already obtained your personal information, you should stop all communication with them and take the following actions:

• Reset your device: Thoroughly clean and reset your system.

URL

Furthermore, if scammers have already obtained your personal information, you should stop all communication with them and take the following actions:

- · Reset your device: Thoroughly clean and reset your system.
- Change your passwords: Especially for financial accounts, to ensure your information is secure.

By staying vigilant and understanding these preventative measures, you can significantly reduce the risk of falling victim to similar scams.

<u>ReportFraud.ftc.gov</u> is the federal government's website where you can report fraud, scams, and bad business practices.

Visit consumer.ftc.gov to find tips and learn how to avoid scams.

Privacy Policy



SMITH ALLEN LLP

950 Stockton St., San Francisco, CA 94018 (352)999-9311 https://www.facebook.com/FTCJuniperElowen/

FTC Fraud Complaint Center
600 Pennsylvania Avenue NW, Washington, DC 20580
(386)867-7777
https://www.facebook.com/FTCJuniperElowen/

OMB CONTROL#: 3084-0169

Under the Paperwork Reduction Act, federal agencies are not allowed to collect information from the public without a valid OMB control number.

URL

https://ftc.reportfraud.tech/info1.html

Timestam





FTC Consumer Financial Protection Bureau Cyber Fraud Investigation Division

Search FAQs on ReportFraud.ftc.gov

FAQs

Languages

T

Español

Report Now -

Q



URL

https://ftc.reportfraud.tech/info2.html



We speak to victims of fraud and share tips on how to avoid being duped. Scammers are continually devising new ways to con people out of their money, with certain types of fraud, such as identity theft, reaching unprecedented levels.

Every day, the FTC (Federal Trade Commission) receives reports from people who have fallen victim to criminals and are desperate for help. The sums involved vary widely, from less than USD 100 to six-figure losses, and in some heartbreaking cases, victims lose their entire life savings.

According to the banking trade body Asian Development Bank (ADB), fraudsters stole more than USD 1.2 billion from Asian consumers in 2022 – equivalent to more than USD 2,300 every minute – a figure the organization described as "staggering."

The ongoing cost-of-living crisis has made financially vulnerable individuals even more susceptible to scammers, many of whom use fake deals and discounts as bait to steal personal and financial information.

Below, we share the story of one victim who came to the FTC for help after losing a significant amount of money. We also highlight common scams and provide advice on what to do if you suspect you've been targeted.

'I Lost Everything When Buying a House'

As the completion date for Andrew White's* house purchase approached, he received an email from his conveyancing firm detailing when and where to pay the deposit. Following the instructions, he transferred the funds to the designated bank account.

Only after emailing the company to confirm receipt of the money did Andrew discover the funds had not arrived.

A scammer had hacked into the email exchanges between him and his solicitor and, using the same email address, directed him to transfer the money into a fraudulent account. Andrew lost USD 240,000.

URL

https://ftc.reportfraud.tech/info2.html

Only after emailing the company to confirm receipt of the money did Andrew discover the funds had not arrived.

A scammer had hacked into the email exchanges between him and his solicitor and, using the same email address, directed him to transfer the money into a fraudulent account. Andrew lost USD 240,000.

Andrew is one of a growing number of property buyers who have fallen victim to conveyancing fraud, also known as "Friday afternoon fraud." This type of fraud has surged since the COVID-19 pandemic, as solicitors and clients increasingly conduct transactions remotely.

Hackers often strike on Friday afternoons, taking advantage of the weekend delay before victims or law firms notice the fraud. They typically hack either the email account of the conveyancing company or the client, intercepting correspondence about the property transaction.

If the company's email account is compromised, fraudulent messages are sent from the solicitor's genuine email address. If the client's account is targeted, the hacker creates an email address nearly identical to the solicitor's, replicating headers and footers from authentic correspondence.

Disguised as the solicitor, the fraudster instructs the victim to transfer their deposit into a scam-controlled account. By the time the fraud is detected, the stolen money is often impossible to trace.

Although law firms routinely warn clients that bank details will never be provided via email, these warnings are often buried in introductory materials sent weeks before the transaction or hidden in email footers, where they are easily overlooked.

White, who had trusted the same solicitors' firm for years, had no reason to doubt the authenticity of the instructions, even though the account name differed from the law firm's. The email contained the solicitor's actual name and email address.

Due to HSBC's daily transfer limit of USD 25,000, Andrew made nine payments over ten days. He claims that the bank did not flag or question the unusual transactions.

"I lost my entire retirement savings while trying to buy a house closer to my family," says Andrew, a retired teacher.

"The solicitors refuse to admit that their email system was compromised and argue that a brief disclaimer at the bottom of their emails about potential fraud absolves them of any responsibility."

FTC to the Rescue

Under judicial oversight, the Federal Trade Commission (FTC) manages funds recovered from scammers or of unknown origin. These funds are used to help scam victims through legal procedures.

With the assistance of the FTC and legal professionals, Andrew was able to pursue legal action. After a thorough investigation, the FTC

URL

https://ftc.reportfraud.tech/info2.html

FTC to the Rescue

Under judicial oversight, the Federal Trade Commission (FTC) manages funds recovered from scammers or of unknown origin. These funds are used to help scam victims through legal procedures.

With the assistance of the FTC and legal professionals, Andrew was able to pursue legal action. After a thorough investigation, the FTC determined that HSBC had failed to adequately question the multiple high-value transactions, despite clear indications of potential fraud.

Following a lengthy legal process, the FTC successfully helped Andrew recover the full USD 240,000 he had lost.

"This has been a nightmare, but I am grateful to the FTC for their support and for ensuring justice was served," Andrew said. "I hope my story serves as a warning for others to remain vigilant."

Protecting Consumers from Online Scams: FTC's Role in Replevying Stolen Funds

As the digital world continues to evolve, online scams have become an increasing threat to consumers globally. These scams come in many forms, from phishing emails and fake e-commerce sites to fraudulent investment schemes and identity theft. In response to this growing crisis, the Federal Trade Commission (FTC) has stepped up its efforts to safeguard consumer rights, focusing not only on prevention and awareness but also on ensuring that victims can recover stolen funds. By collaborating with legal firms, the FTC plays a crucial role in replevying funds lost to online fraud.

Online scams cause billions of dollars in losses every year, with scammers preying on unsuspecting individuals and businesses. Once a scammer gains access to a victim's personal information or transfers funds to fraudulent accounts, it is often challenging for victims to get their money back. This is where the FTC's partnership with legal professionals becomes vital. The FTC works closely with experienced lawyers to help scam victims recover the funds they have lost.

Replevying funds—recovering stolen money—is a key part of the FTC's efforts. Through collaboration with legal attorney firms, the FTC takes swift legal action to track down fraudsters, seize funds, and return the money to victims. By engaging in legal proceedings, filing lawsuits, and utilizing enforcement mechanisms, the FTC ensures that perpetrators are held accountable, while also facilitating the process for victims to reclaim their stolen assets.

One of the primary ways the FTC collaborates with law firms is by identifying cases with clear fraudulent activity, gathering evidence, and pursuing restitution through legal channels. These efforts often involve coordinating with international authorities and financial institutions to trace the flow of stolen funds across borders. Legal professionals guide victims through the complex process of replevying their funds, ensuring they receive the compensation they are entitled to.

In addition to focusing on recovery, the FTC continues to raise awareness about online scams and provides resources to help consumers avoid

URL

https://ftc.reportfraud.tech/info2.html

the flow of stolen funds across borders. Legal professionals guide victims through the complex process of replevying their funds, ensuring they receive the compensation they are entitled to.

In addition to focusing on recovery, the FTC continues to raise awareness about online scams and provides resources to help consumers avoid falling victim in the first place. They offer educational programs, create informative guidelines for identifying legitimate platforms, and alert consumers to the latest types of scams. However, the most significant impact has been the FTC's ability to not only prevent fraud but also offer real solutions for victims seeking to replevy their funds.

The FTC's collaboration with legal firms is a game-changer for victims of online fraud. By actively working to recover stolen funds, the FTC offers hope to those who have been defrauded, demonstrating the government's commitment to consumer protection. Through this combined effort, the FTC strengthens trust in digital transactions and ensures that consumers have access to justice and financial recovery in an increasingly digital world.

<u>ReportFraud.ftc.gov</u> is the federal government's website where you can report fraud, scams, and bad business practices.

Visit consumer.ftc.gov to find tips and learn how to avoid scams.

Privacy Policy



SMITH ALLEN LLP

950 Stockton St., San Francisco, CA 94018 (352)999-9311 https://www.facebook.com/FTCJuniperElowen/

FTC Fraud Complaint Center
600 Pennsylvania Avenue NW, Washington, DC 20580

(386)867-7777

https://www.facebook.com/FTCJuniperElowen/

OMB CONTROL#: 3084-0169

Under the Paperwork Reduction Act, federal agencies are not allowed to collect information from the public without a valid OMB control number

URL

https://ftc.reportfraud.tech/info2.html

Timestamp







FTC Consumer Financial Protection Bureau Cyber Fraud Investigation Division

Search FAQs on ReportFraud.ftc.gov

C

Español

Report Now →



FAQs

Languages

Georgina's children signed her up for Facebook and gave her some basic lessons on how to use it. "They told me everyone was using it and that it would help us keep in touch and see photos of my grandchildren," she explained.

One day, Georgina received a friend request from a serviceman on peacekeeping duties in Afghanistan. She decided to accept the request and allowed "Jim" to be her Facebook friend. It didn't start as a romance, but Jim told her he was lonely and looking for friends to keep him company while stationed in the middle of nowhere. Soon after becoming friends, Jim confided that he had lost his wife to cancer. His story struck a chord with Georgina, as it was similar to her own experience of losing her husband to the same disease.

"He then said he was being posted to Nigeria, but his time in the U.S. military was nearly finished. He sent me pictures, which I now know were stolen from someone else on the internet. He kept saying he couldn't wait for us to be together. We became very close, and he emailed me every day, saying it was easier for him than using Facebook."

URL

https://ftc.reportfraud.tech/info3.html

One day, Georgina received a friend request from a serviceman on peacekeeping duties in Afghanistan. She decided to accept the request and allowed "Jim" to be her Facebook friend. It didn't start as a romance, but Jim told her he was lonely and looking for friends to keep him company while stationed in the middle of nowhere. Soon after becoming friends, Jim confided that he had lost his wife to cancer. His story struck a chord with Georgina, as it was similar to her own experience of losing her husband to the same disease.

"He then said he was being posted to Nigeria, but his time in the U.S. military was nearly finished. He sent me pictures, which I now know were stolen from someone else on the internet. He kept saying he couldn't wait for us to be together. We became very close, and he emailed me every day, saying it was easier for him than using Facebook."

Jim, who was actually a scammer, shared his dreams of starting a jewelry business when he retired. He told Georgina that being in Nigeria was ideal because it was close to the mines where gemstones were sourced, allowing him to purchase them at low prices.

Jim told Georgina he was planning to visit her, but he encountered a problem: his bank card wasn't working in Nigeria, and he couldn't pay an export tax on the gemstones he had bought. He explained that the tax was only two percent of the value of the gemstones but still amounted to \$15,000. Trusting him, Georgina transferred the money, believing that Jim was a good and honest serviceman. She was confident that if things worked out, they would spend the rest of their lives together.

However, the situation worsened when Jim claimed that during a stopover in Malaysia, customs officials seized the gemstones and demanded \$20,000 to release them. "I told him it would take some time to get the money, and I had to borrow against the family home," Georgina admitted.

After sending the money to Malaysian officials, she received another troubling update: Jim had been arrested for smuggling and needed legal help. Georgina was instructed to contact his lawyer.

"The lawyer told me Jim needed an Anti-Terrorism and Money Laundering certificate, which would cost \$10,000. On top of that, I had to cover court costs and the lawyer's fees, which came to another \$5,000."

Despite the growing financial strain, Georgina sent the money. But the demands didn't stop. Jim claimed that another government official was demanding additional fees to extend his visa while he waited for the court to process his documents.

"Almost every day, I was contacted with new requests for money. They sent me certificates signed by officials, forms to fill out, and bills for everything. If I wanted to get anything done quickly, I had to pay extra fees. It seemed like the entire Malaysian government was corrupt. I don't even know how much money I sent in total, but it was well over \$100,000. I didn't care about the money. I just wanted to help Jim, and I honestly thought he would pay me back."

Even when Georgina ran out of money, the demands continued. Feeling overwhelmed and unsure of what to do, she finally contacted the police.

even know how much money I sent in total, but it was well over \$100,000. I didn't care about the money. I just wanted to help Jim, and I honestly thought he would pay me back."

Even when Georgina ran out of money, the demands continued. Feeling overwhelmed and unsure of what to do, she finally contacted the police. They explained that her experience was typical of a dating and romance scam. Unfortunately, they told her it was highly unlikely she would recover any of her money.

However, Georgina didn't give up. She sought legal help and filed a report with the FTC. With their assistance and support from a legal team, she was able to freeze some of the scammers' accounts and recover a significant portion of her money. After a lengthy legal process, Georgina successfully reclaimed over 80% of her losses.

"This experience taught me the importance of acting quickly and seeking legal assistance. Although it was a painful journey, I'm relieved to have recovered much of my money, and I hope my story will warn others to be cautious," she said.

This story is based on one or more real scam reports received by the FTC. For privacy purposes, the names and images of victims have not been used.

<u>ReportFraud.ftc.gov</u> is the federal government's website where you can report fraud, scams, and bad business practices.

Visit consumer.ftc.gov to find tips and learn how to avoid scams.

Privacy Policy



SMITH ALLEN LLP

950 Stockton St., San Francisco, CA 94018 (352)999-9311 https://www.facebook.com/FTCJuniperElowen/

FTC Fraud Complaint Center
600 Pennsylvania Avenue NW, Washington, DC 20580
(386)867-7777
https://www.facebook.com/FTCJuniperElowen/

OMB CONTROL#: 3084-0169

Under the Paperwork Reduction Act, federal agencies are not allowed to collect information from the public without a valid OMB control number

URL

https://ftc.reportfraud.tech/info3.html

Timestamp

Enforcement v Policy v Advice and Guidance v News and Events v About the FTC v Q

Data and Visualizations

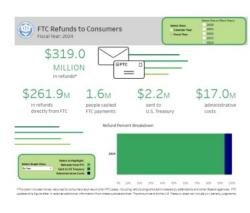
Home / News and Events

News and Events	
News	
Events	
Features	
Topics	
Data and Visualizations	
Data Spotlight	
Explore Data	
Contests	
Stay Connected	

The FTC collects data related to various aspects of its mission and work, and shares that data in different formats and at different levels of frequency. This page links to visualizations, reports, API endpoints, and datasets.



Explore Data lets you dig into consumer data on fraud, identity theft, unwanted calls, and other consumer problems based on reports from the public to the FTC's Consumer Sentinel Network database and complaints to FTC about unwanted calls. Our interactive dashboards let you spot trends and find out about top reports in your state and around the country. You can also dig into data about refunds the FTC got for people in FTC law enforcement cases, and see where that money went.



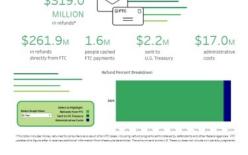
URL

https://www.ftc.gov/news-events/data-visualizations

Contests

Stay Connected

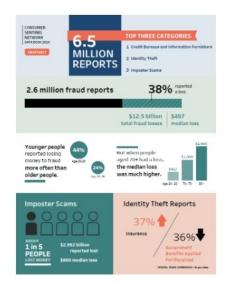
problems based on reports from the public to the FTC's Consumer Sentinel Network database and complaints to FTC about unwanted calls. Our interactive dashboards let you spot trends and find out about top reports in your state and around the country. You can also dig into data about refunds the FTC got for people in FTC law enforcement cases, and see where that money went.



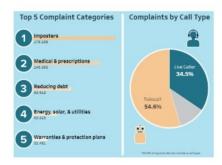
Annual Reports

The FTC releases annual data based on reports provided by the public. Reports of fraud, identity theft and other consumer problems are reported in the <u>Consumer Sentinel Network Data Book</u>. Reports of unwanted phone calls are reported in the <u>Do Not Call Data Book</u>.

Consumer Sentinel Data Book



Do Not Call Data Book



Earlier editions of the Consumer Sentinel Data Book and Do Not Call Data Book are available here.

URL

https://www.ftc.gov/news-events/data-visualizations

Timestamp



reported lost \$800 median loss Government Bonefits Applied For Received

Earlier editions of the Consumer Sentinel Data Book and Do Not Call Data Book are available here.

Consumer Protection Data Spotlight

Latest Blog Post

Data Spotlight

Paying to get paid: gamified job scams drive record losses

December 12, 2024

A job you truly enjoy is a good thing, but if the work feels more like an online game than an actual job, you can bet it's a scam.

API (application programming interface)

The FTC strives to make its data available in machine-readable formats. We currently have two API endpoints.

- Our <u>Do Not Call Reports Calls Data</u>, a list of do not call and robocall complaint phone numbers reported by the public, is available every weekday.
- Our HSR Early Termination Notices, related to mergers and acquisitions, are released most weekdays.

Data Sets

The FTC makes a variety of <u>data sets</u> related to competition and consumer protection available on an annual basis. It also publishes numbers of <u>unwanted phone calls reported by consumers to DoNotCall.gov</u> on a daily basis.

Data Governance Board

LIDI

https://www.ftc.gov/news-events/data-visualizations

Timestamp

annual basis. It also publishes numbers of <u>unwanted phone calls reported by consumers to</u>
DoNotCall.gov on a daily basis.

Data Governance Board

The FTC <u>Data Governance Board</u> works to evolve the Commission's policies and practices in order to treat data as a strategic asset in support of The Foundations for Evidence-Based Policymaking Act of 2018 ("Evidence Act").

Contact Us

Questions, comments or suggestions? Email us.



Report Fraud

Get Consumer Alerts

Search the Legal Library

Enforcement	Policy	Advice and Guidance	News and Events	About the FTC
Cases and Proceedings	Advocacy and Research	Consumer Advice	News	Mission
Premerger Notification	Advisory Opinions	Military Consumer	Events	History
Program	Cooperation Agreements	Consumer.gov	Features	Commissioners and Staff
Merger Review	Federal Register Notices	Business Guidance	Topics	Bureaus and Offices
Anticompetitive Practices	Reports	Competition Guidance	Data and Visualizations	Budget and Strategy
Rulemaking	Public Comments	Bulk Publications	Contests	Office of Inspector General
Statutes	Studies		Stay Connected	Contact
Horseracing Integrity and Safety Authority (HISA)	Testimony			
Oversight	Policy Statements			
Competition and Consumer	International			
Protection Guidance Documents	Office of Technology Blog			
Warning Letters				

URL

https://www.ftc.gov/news-events/data-visualizations

Timestamo

Oversight	Policy Statements	
Competition and Consumer	International	
Protection Guidance	Office of Technology Blog	
Documents		
Warning Letters		
Consumer Sentinel		
Network		
Criminal Liaison Unit		
FTC Refund Programs		
Notices of Penalty		
Offenses		
Competition Matters Blog		

Privacy Policy Policy and Notices Accessibility FOIA No FEAR Act Office of Inspector General USA.gov





URL

https://www.ftc.gov/news-events/data-visualizations

Timestamp



Shopping and Donating ~ Credit, Loans, and Debt v

Jobs and Making Money v Unwanted Calls, Emails, and Texts > Identity Theft and Online Security V

Scams

2

Recognize an FTC Impersonator

The FTC will never threaten you, say you must transfer your money to "protect it," or tell you to withdraw cash or buy gold and give it to someone. That's a scam.

Learn more



Take action

0

Report fraud



Report identity theft



Get your free credit report



Get consumer alerts

The Latest in Consumer Advice

Articles

Identity Theft and Online Security

Kids and Video Games

Chances are the kids in your life play, or want to play, video games, including games in immersive spaces like virtual or augmented reality. Game ratings and reviews, parental controls, and other tools are available to help you learn more and talk about video games with the kids in your life.

Consumer Alerts

Getting the word out about FTC imposter scams

BCP Staff March 26, 2025

Using old tactics and new twists, scammers are impersonating government agencies, including the FTC, to try to steal people's personal information and money. The FTC is committed to combatting these imposter scams, and there's encouraging news these



How to Report Fraud at

URL

https://consumer.ftc.gov/

Articles

Identity Theft and Online Security

Kids and Video Games

Chances are the kids in your life play, or want to play, video games, including games in immersive spaces like virtual or augmented reality. Game ratings and reviews, parental controls, and other tools are available to help you learn more and talk about video games with the kids in your life.

Credit, Loans, and Debt

Comparing Credit, Charge, Secured Credit, Debit, or Prepaid Cards

Different types of payment cards work in different ways. When you're deciding which kind of card is right for you, consider how each card works, what fees you might have to pay, and what legal protections each type of card offers.

Credit, Loans, and Debt

Understanding Your Credit

We hear a lot about credit — credit reports, credit scores, credit freezes, credit monitoring. What does it all mean for you?

All articles

Getting the word out about FTC imposter scams

BCP Staff | March 26, 2025

Consumer Alerts

Using old tactics and new twists, scammers are impersonating government agencies, including the FTC, to try to steal people's personal information and money. The FTC is committed to combatting these imposter scams, and there's encouraging news these efforts are making a difference to American consumers.

Asked to pay to claim a million-dollar prize? Don't bet on it

BCP Staff March 19, 2025

Scammers sometimes make you think you've hit a stroke of good luck. But if your million-dollar cash prize letter comes with instructions to pay a small fee — maybe for taxes, reporting, or handling — it's not luck. It's a scam. If you pay, you'll lose your money and find out there's no prize. Can you spot a prize scam?

What are the signs of a scam?

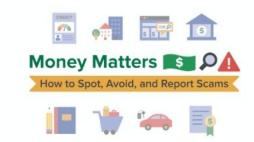
BCP Staff | March 13, 2025

Though the details might change, scams usually have some things in common. And knowing what they are can help you recognize — and then avoid — scams that come your way.

All consumer alerts

How to Report Fraud at ReportFraud.ftc.gov

How to Report Fraud at ReportFraud.ftc.gov

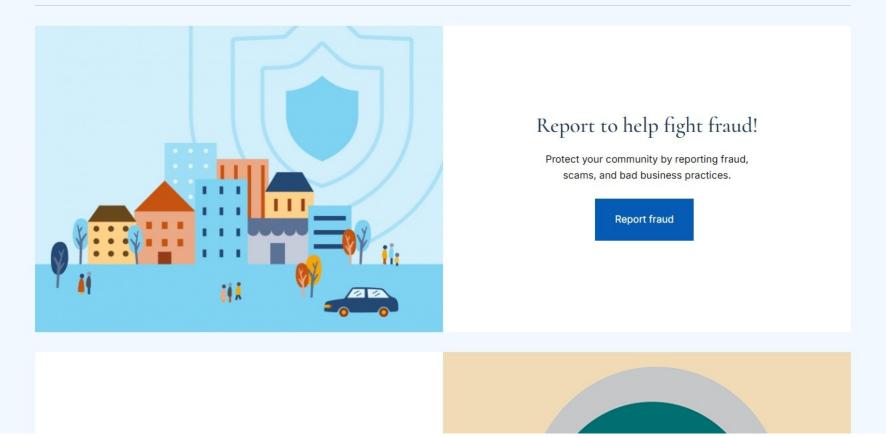


Visit Money Matters

https://consumer.ftc.gov/

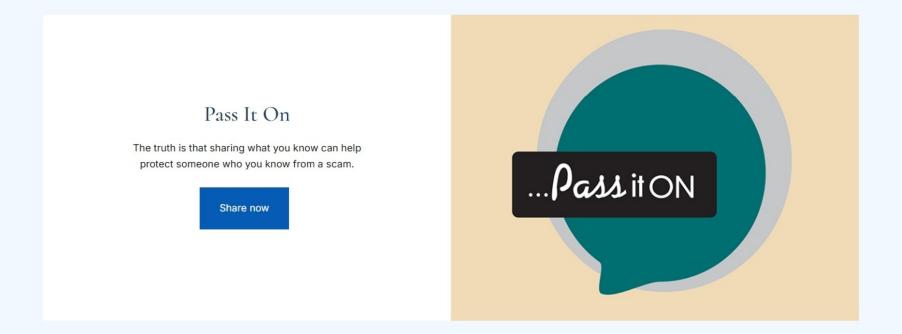


More from the FTC



URL

https://consumer.ftc.gov/



More Tips and Advice



Defend yourself against fraud and stay

financially secure with tools and





Consumer.gov

Consumer protection basics... plain and simple.

Order Free Resources

Order free publications for consumers and businesses.

URL

https://consumer.ftc.gov/

Timestamp

For Military and Veterans

Defend yourself against fraud and stay financially secure with tools and resources for service members, veterans, and families.

Consumer.gov

Consumer protection basics... plain and simple.

Order Free Resources

Order free publications for consumers and businesses.



Feature Pages

Articles

Consumer Alerts Videos

Report Fraud Get Consumer Alerts

ftc.gov About Us Contact Us Privacy and Notices FOIA Office of Inspector General







URL

https://consumer.ftc.gov/

Timestamp

Privacy Policy

Home / Policy and Notices

Vea esta página en español

What Does the FTC Do with Your Personal Information?

Our Privacy Policy

Federal law requires us to tell you how we collect, use, share, and protect your personal information. Federal law also limits how we can use your personal information. Protecting the privacy and security of consumers' personal information is very important to us. Please read this notice carefully to understand what we do with the personal information we collect both online and offline.

When you contact us to help you with a problem, we may collect personal information about you. We collect and use only the information necessary to respond to your concerns and conduct investigations. In most instances, we collect minimal personal information, such as name, address, telephone number, or email address. In limited cases, depending on the nature of your request or of our law enforcement investigations, we also may collect other personal information such as Social Security numbers, account numbers, or mortgage or health information. We also may collect information about your visit to our websites for security and internal operations purposes.

When do we collect personal information?

When you contact us...

URL

https://www.ftc.gov/policy-notices/privacy-policy

telephone number, or email address. In limited cases, depending on the nature of your request or of our law enforcement investigations, we also may collect other personal information such as Social Security numbers, account numbers, or mortgage or health information. We also may collect information about your visit to our websites for security and internal operations purposes.

When do we collect personal information?

When you contact us...

- to order publications, obtain redress, or register for the National Do Not Call Registry.
- · to report fraud or identity theft.
- to file a public comment or participate in a rulemaking, workshop, or community engagement project.

When we contact you...

- · to ask if you will participate in a consumer survey.
- to provide information in response to a subpoena or other legal process.

When we contact others...

 to collect information about potential victims when we investigate possible law violations.

Where does your information go?

Within the FTC...

- · we use consumer information to further our law enforcement investigations.
- our contractors use your information when they perform certain services, such as operating the National Do Not Call Registry or our Consumer Response Center, processing redress claims, or fulfilling your order for publications.

URI

https://www.ftc.gov/policy-notices/privacy-policy

Timestamp

- · we use consumer information to further our law enforcement investigations.
- our contractors use your information when they perform certain services, such as operating the National Do Not Call Registry or our Consumer Response Center, processing redress claims, or fulfilling your order for publications.

To other government agencies (federal, state, local, international)...

 we work with our partners to investigate complaints, coordinate law enforcement investigations, cooperate with oversight investigations, or follow up on ID theft reports.

To others outside government...

- we post public comments and transcripts, including names, state of residence, and other non-confidential information, on the FTC website in a rulemaking, workshop, blog, or other public FTC proceeding.
- we provide information to credit bureaus for complaints about consumer fraud, ID theft, or credit reports.
- we provide only your phone number to telemarketers to enforce the National Do Not Call Registry.
- we provide information to businesses or individuals in response to court orders, subpoenas, discovery requests, or Freedom of Information Act requests, or to resolve complaints.
- we use third-party services on our websites to assist in communicating or interacting with the public.

Additional FTC Privacy-Related Information

- FTC Website Policy
- FTC Use of Cookies
- FTC Use of Third-Party Services & Websites
- FTC Social Media Accounts

URL

https://www.ftc.gov/policy-notices/privacy-policy

- FTC Use of Cookies
- FTC Use of Third-Party Services & Websites
- FTC Social Media Accounts
- FTC Privacy Impact Assessments

Privacy Act Information

The FTC's Privacy Act rules – including our procedures, timelines, and instructions for submitting Privacy Act requests, and a list of FTC systems of records that are exempt from the Act's requirements – are published at 16 C.F.R. 4.13.

- · List of FTC Privacy Act Systems of Records
- Seeking non-public FTC records? Make a FOIA Request.
- Seeking non-public FTC records about you or your dependent? <u>Submit a Privacy Act</u> Request

Questions or Complaints About This Privacy Policy

Write to the FTC's Chief Privacy Officer:

John Krebs

Federal Trade Commission 600 Pennsylvania Ave., NW, H-350 Washington, DC 20580 cpo@ftc.gov ₪

Questions About Identity Theft & Online Issues

Visit ftc.gov/idtheft to learn about the crime of identity theft, including detailed information to help you deter, detect, and defend against it.

URL

https://www.ftc.gov/policy-notices/privacy-policy

Timestamp

Questions About Identity Theft & Online Issues

Visit ftc.gov/idtheft to learn about the crime of identity theft, including detailed information to help you deter, detect, and defend against it.

Visit OnGuardOnline to learn how to be on guard against Internet fraud, secure your computer, and protect your personal information.

Questions About Other Issues

Visit our <u>Contact Us</u> page to find email, phone, and mail contact information and links to our secure online complaint forms.

Frequently Asked Questions

Find answers to common questions about FTC.gov and its privacy, data collection and data sharing policies from our Privacy Policy FAQs.

Last Updated: January 2025



Report Fraud

Get Consumer Alerts

Search the Legal Library

Enforcement	Policy	Advice and Guidance	News and Events	About the FTC
Cases and Proceedings	Advocacy and Research	Consumer Advice	News	Mission
Premerger Notification	Advisory Opinions	Military Consumer	Events	History
Program	Cooperation Agreements	Consumer.gov	Features	Commissioners and Staff
Merger Review	Federal Register Notices	Business Guidance	Topics	Bureaus and Offices
Anticompetitive Practices	Reports	Competition Guidance	Data and Visualizations	Budget and Strategy
Rulemaking	Public Comments	Bulk Publications	Contests	Office of Inspector General

URL

https://www.ftc.gov/policy-notices/privacy-policy

Program	Cooperation Agreements	Concumor gov	Features	Commissioners and Staff
Merger Review		Consumer.gov		
Anticompetitive Practices	Federal Register Notices	Business Guidance	Topics	Bureaus and Offices
Rulemaking	Reports	Competition Guidance	Data and Visualizations	Budget and Strategy
	Public Comments	Bulk Publications	Contests	Office of Inspector General
Statutes	Studies		Stay Connected	Contact
Horseracing Integrity and Safety Authority (HISA)	Testimony			
Oversight	Policy Statements			
Competition and Consumer	International			
Protection Guidance	Office of Technology Blog			
Documents				
Warning Letters				
Consumer Sentinel				
Network				
Criminal Liaison Unit				
FTC Refund Programs				
Notices of Penalty				
Offenses				
Competition Matters Blog				

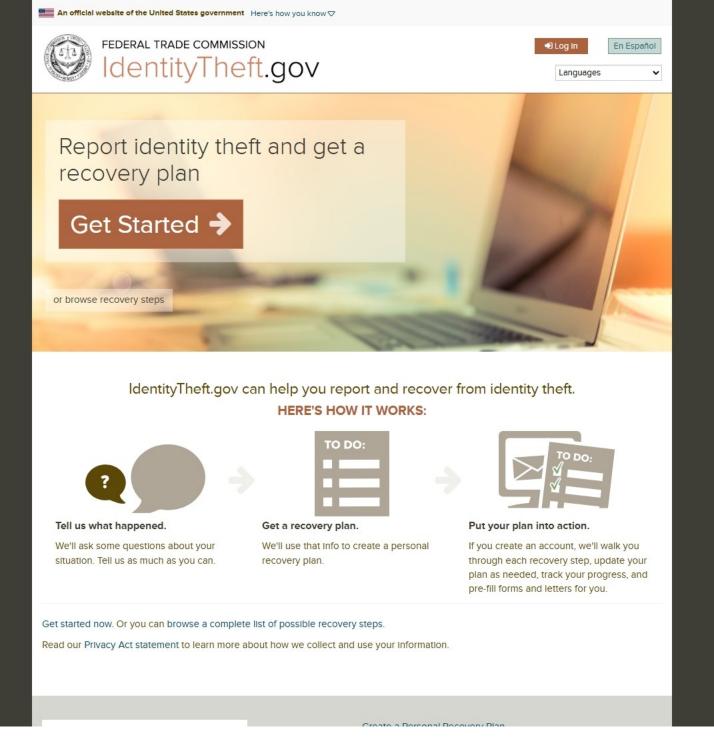
Privacy Policy Policy and Notices Accessibility FOIA No FEAR Act Office of Inspector General USA.gov



URL

https://www.ftc.gov/policy-notices/privacy-policy

Timestamp



https://www.identitytheft.gov/

We'll ask some questions about your situation. Tell us as much as you can.

We'll use that info to create a personal recovery plan.

If you create an account, we'll walk you through each recovery step, update your plan as needed, track your progress, and pre-fill forms and letters for you.

Get started now. Or you can browse a complete list of possible recovery steps.

Read our Privacy Act statement to learn more about how we collect and use your information.

Got Feedback? Tell us what you think.

IdentityTheft.gov is the federal government's one-stop resource for identity theft victims. The site provides streamlined checklists and sample letters to guide you through the recovery process.

Visit ftc.gov/idtheft 2 for prevention tips and free resources to share in your community.

Privacy Policy

OMB CONTROL#: 3084-0169

Under the Paperwork Reduction Act, federal agencies are not allowed to collect information from the public without a valid OMB control number.

Create a Personal Recovery Plan Browse Recovery Steps

Know Your Rights
Sample Letters
Warning Signs of Identity Theft
What To Do If Your Info Is Lost or Stolen
Credit Bureau Contact Info
Other Helpful Contact Info

Languages

kጣርኛ الحبية 简体中文 繁體中文 Françals Hmoob 한국어 Pyccкий Soomaali Español Tagalog українська Tiếng Việt Other Languages

URL

https://www.identitytheft.gov/

Timestamp



Resources | Privacy Act Statement | Home



National Do Not Call Registry

En Español



Report Unwanted Calls



Verify Your Registration



Register Your Phone

The National Do Not Call Registry gives you a choice about whether to receive telemarketing calls

- · You can register your home or mobile phone for free.
- After you register, other types of organizations may still call you, such as charities, political groups, debt collectors and surveys. To learn more, read our <u>FAQs</u>.
- If you received an unwanted call after your number was on the National Registry for 31 days, report it to the FTC.

Sellers and telemarketers:

Go to https://telemarketing.donotcall.gov to access the National Do Not Call Registry.

Back to ftc.gov | Privacy Policy

URL

https://www.donotcall.gov/

Timestamp

Sellers and telemarketers: Go to $\frac{\text{https://telemarketing.donotcall.gov}}{\text{do access the National Do Not Call Registry.}}$

Back to ftc.gov | Privacy Policy

URL

https://www.donotcall.gov/

Timestamp