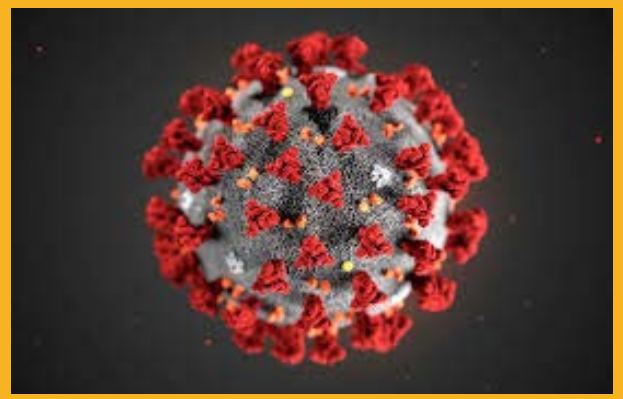
PROTECTING CONSUMER DATA IN THE TIME OF COVID19



DEON WOODS BELL
OFFICE OF INTERNATIONAL AFFAIRS
FEDERAL TRADE COMMISSION

Coronavirus (COVID-19) Pandemic:

The FTC in Action

The Federal Trade Commission continues its work protecting consumers, providing guidance to businesses, and protecting competition in the marketplace throughout the pandemic. Staff are working remotely and events that are not postponed are being held via webcast.

Subscribe to updates about the FTC's response to COVID-19 >

FOR CONSUMERS

Helping people spot and avoid the latest Coronavirus scams.

More for consumers >

FOR BUSINESSES

Offering compliance guidance for companies and tips on protecting against scams targeting businesses.

More for business >

ENFORCEMENT

Updating the public on FTC law enforcement actions and complaint data.

More on enforcement >

FTC WARNING LETTERS TO VOIP PROVIDERS

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Contact | Stay Connected | Privacy Policy | FTC en español

Search

ABOUT THE FTC | NEWS & EVENTS | ENFORCEMENT | POLICY | TIPS & ADVICE | I WOULD LIKE TO...

Home » News & Events » Press Releases » FTC Warns Nine VoIP Service Providers and Other Companies against 'Assisting and Facilitating' Illegal Coronavirus-related Telemarketing Calls

FTC Warns Nine VoIP Service Providers and Other Companies against 'Assisting and Facilitating' Illegal Coronavirus-related Telemarketing Calls

March 27, 2020

FOR RELEASE

TAGS: Coronavirus (COVID-19) | Do Not Call | robocalls | Bureau of Consumer Protection | Consumer Protection | Advertising and Marketing | Health Claims | Telemarketing

Federal Trade Commission staff sent letters to nine Voice over Internet Protocol (VoIP) service providers and other companies warning them that "assisting and facilitating" illegal telemarketing or robocalls related to the coronavirus or COVID-19 pandemic is against the law. Many of these calls prey upon consumers' fear of the virus to perpetrate scams or sow disinformation.

"It's never good business for VoIP providers and others to help telemarketers make illegal robocalls that scam people," said FTC Bureau of Consumer Protection Director Andrew Smith. "But it's especially bad when your company is helping telemarketers exploiting fears about the coronavirus to spread disinformation and perpetrate scams."

The staff sent the letters to the following companies: 1) VoIPMax; 2) SipJoin Holding, Corp.; 3) iFly Communications; 4) Third Rock Telecom; 5) Bluetone Communications, LLC; 6) VoIP Terminator, Inc., also known as BLMarketing; 7) J2 Web Services, Inc.; 8) VoxBone US LLC; and 9) Comet Media, Inc.

They stress that combatting illegal telemarketing is a top priority of the Commission, with a special emphasis on stopping illegal robocalls. Staff's letters cite two cases the FTC has brought in this area, one against James B. Christiano whose companies provided software to robocallers, and another against a VoIP service provider called Globex Telecom.

The letters also cite two civil enforcement actions the Department of Justice has taken against VoIP companies and their owners for "committing and conspiring to commit wire fraud by knowingly transmitting robocalls that impersonated federal government agencies."

The letters warn the recipients that the FTC may take legal action against them if they assist a seller or telemarketer who they know, or consciously avoid knowing, is violating the agency's Telemarketing Sales Rule (TSR).

The letters note several types of conduct that may violate the TSR, including:

- making a false or misleading statement to induce a consumer to buy something or contribute to a charity;
- misrepresenting a seller or telemarketer's affiliation with any government agency;
- transmitting false or deceptive caller ID numbers;

EVENTS CALENDAR

Related Resources

Coronavirus Warning Letters

For Consumers

Blog: Socially distancing from COVID-19 robocall scams

For Businesses

Blog: New Coronavirus warning letters: Who can it be now?

Complying with the Telemarketing Sales Rule

Media Resources

Protecting Consumers

Made in USA

Health Claims

Enforcement

Advertisement Endorsements

Robocalls

Green Guides

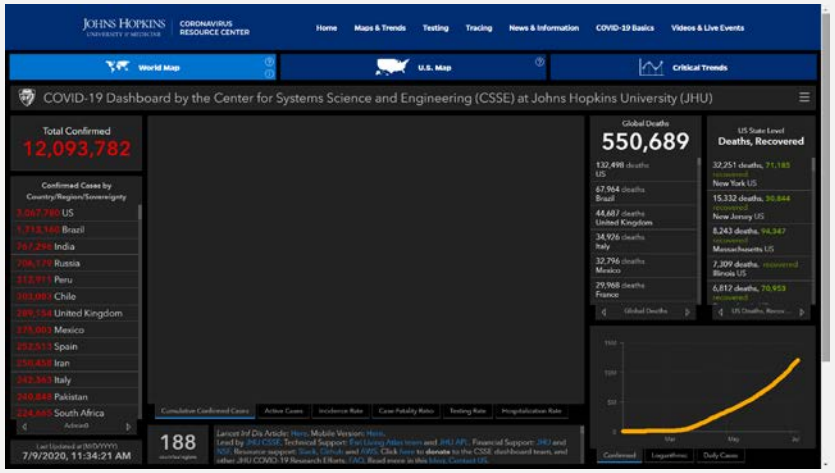
INFORMATION HARVESTING SCAMS

PHONECALLS/EMAILS/TEXTS

- FTC advisory: Scammers send Covid-19 related phishing emails or texts to trick consumers into sharing account numbers, identity card numbers, healthcare numbers, or login IDs and passwords. They use the information to steal consumer's money, commit identity theft, or both.

RANSOMWARE/MALWARE

- Some phishing emails about the Coronavirus seek access to computer or networks, often to install ransomware or other programs that can lock consumers out of their data.



- Other scammers have used real information to infect computers with malware. For example, malicious websites used the real Johns Hopkins University interactive dashboard of Coronavirus infections and deaths to spread password-stealing malware.

FAKE WEBSITES

- FTC Alert: scammers use familiar company names or pretend to be a known contact
- At right is an example of a scam where phishers pretended to be the World Health Organization (WHO):

Re:SAFTY CORONA VIRUS AWARENESS WHO

WO World Health Organization·

World Health Organization

Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus.

Click on the button below to download

Safety measures

Symptoms common symptoms include fever,coughcshortness of breath and breathing difficulties.

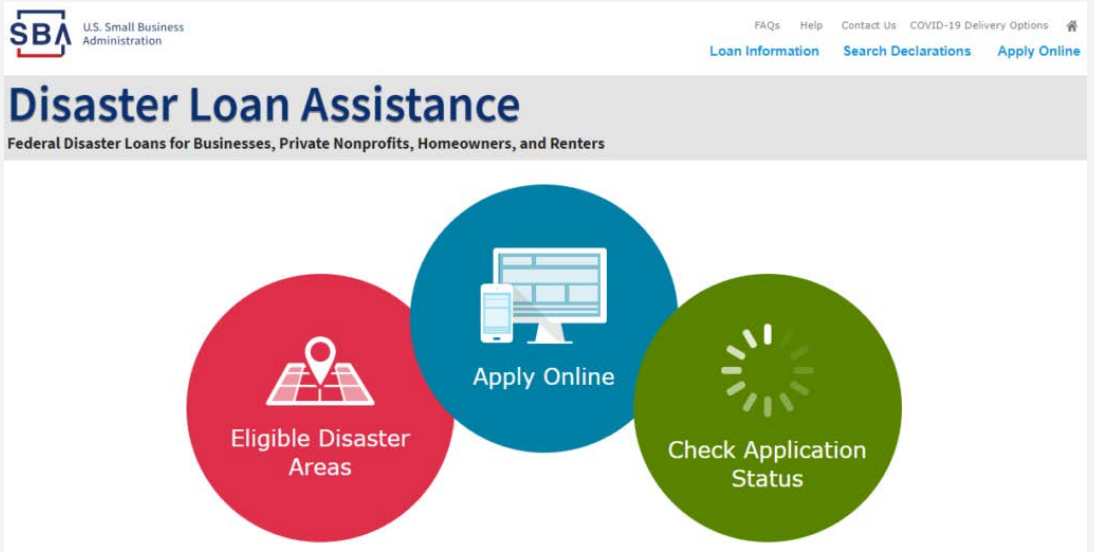
Regards,

Dr. Stella Chungong
Specialist wuhan-virus-advisory

FAKE

SMALL BUSINESSES ARE NOT IMMUNE

- Scammers try to get information or money from businesses who sought loans through federal relief programs



FAKE TESTING SITES

- Scammers set up fake "pop-up" COVID-19 testing sites to exploit crisis.
- The fake sites can look real, with legitimate-looking signs, tents, hazmat suits, and realistic-looking tests.
- They're taking people's personal information, including Social Security numbers, credit card information, and other health information – all of which can be used for identity theft and to run up charges on credit cards.
- The fake testing sites can cause real harm. They aren't following sanitation protocols, so they can spread the virus. Worst of all, they're not giving people the help they need to stay healthy.

CONTACT TRACING SCAMS

- People claim to be affiliated with a health department call and ask for personal information like an identity card number, bank account information, or a credit card account.
- They may also pretend to be contact tracers and collect Personally Identifiable Information.
- Many send spam text messages, which unlike a legitimate text message from a health department that only advise consumers that they will call, links to a fraudulent site. Clicking on the link may download software onto a device, giving scammers access to an array of personal and financial information.
- Many send robocalls.

REMOTE LEARNING

ENFORCEMENT AND GUIDANCE ON CHILD/STUDENT PRIVACY LAWS

FERPA: Family Educational Rights and Privacy Act is the principal law in the US governing privacy in the context of education.

COPPA: The Children's Online Privacy Protection Act generally requires websites and online services to get "Verifiable Parental Consent" from parents before collecting Personally Identifiable Information from kids younger than 13.

TELEHEALTH

TOOLS & GUIDANCE FOR DEVELOPERS OF MOBILE HEALTH APPS

- FTC, with the FDA and HHS, created a web-based tool for developers of health-related mobile apps, which is designed to help the developers understand what federal laws and regulations might apply to their apps.
- The guidance tool asks developers a series of high-level questions about the nature of their app, including about its function, the data it collects, and the services it provides to users.
- Based on the developer's answers to those questions, the guidance will point the app developer toward detailed information about certain federal laws that might apply to the app. These include the FTC Act, the FTC's Health Breach Notification Rule, the Health Insurance Portability and Accountability Act (HIPAA) and the Federal Food, Drug and Cosmetics Act (FD&C Act).
- In parallel, the FTC issued guidance on security specifically tailored for health app developers, including questions to ask in assessing compliance with relevant laws.

COVID-19 TRACKING APPS

- Insurers and health tech companies have developed mobile apps to let patients track Covid-19 symptoms. Some apps intend to help consumers quickly and safely evaluate their symptoms, analyze their risk of having Covid-19, and potentially get tested.
- However, privacy issues could arise in terms of:
  - what type of personal/health data is being collected
  - how patients' health information is currently being used & how it will be used in the future
- GUIDANCE: In 2016, the FTC issued guidance regarding mobile health apps.
  - Section 5 of the FTC Act prohibits unfair or deceptive business practices. Companies need to ensure their privacy policies correctly state how they collect and store data in order to stay in line with the FTC's prohibition against deceptive commercial practices.
  - Section 5 may also be violated if companies fail to reasonably safeguard consumers' personal information.
  - Commercial Mobile Health Apps must also comply with FTC's Health Breach Notification Rule
- PHISHING: The FTC has also alerted users to the potential that scammers may use the crisis to trick them into providing identity card numbers, payment information, or other sensitive data so that they can engage in fraud, identity theft, or both.

MEANWHILE, THE WORK CONTINUES

Data To Go: An FTC Workshop on Data Portability

SEP 22, 2020 **8:30AM–3:00PM**

TAGS: Bureau of Consumer Protection | Consumer Protection | Privacy and Security | Consumer Privacy | Data Security

EVENT DESCRIPTION

THIS EVENT WILL BE HELD ONLINE.

The Federal Trade Commission will host a public workshop on September 22, 2020, to examine the potential benefits and challenges to consumers and competition raised by data portability.

Data portability refers to the ability of consumers to move data – such as, emails, contacts, calendars, financial information, health information, favorites, friends or content posted on social media – from one service to another or to themselves. In addition to providing benefits to consumers, data portability may benefit competition by allowing new entrants to access data they otherwise would not have so that they can grow competing platforms and services. At the same time, there may be challenges to implementing or requiring data portability. For example, data that consumers want to port may include information about others, such as friends' photos and comments. How should this data be treated? How can the data be transferred securely? Who has responsibility for ensuring that data portability is technically feasible? Does mandatory data access or data sharing affect companies' incentives to invest in data-driven products and services?

Data portability is a timely topic. Europe's General Data Protection Regulation and California's Consumer Privacy Act both include data portability requirements, and companies serving customers in Europe and California have already begun providing consumers with the right to port their data. In addition, the UK's Open Banking initiative and US banking laws requiring that financial information be provided to consumers in an electronic format, are encouraging data portability in the financial sector, including the development of APIs to facilitate transfer of data to consumers and among financial institutions. Major technology companies Apple, Facebook, Google, Microsoft, and Twitter have created the Data Transfer Project with the goal of creating an open-source, service-to-service data portability platform. The Department of Health and Human Services' Office of National Coordinator for Health

Related Releases

March 31, 2020
FTC Announces September 22 Workshop on Data Portability

September 10, 2020
FTC Releases Agenda for September Workshop on Data Portability

September 21, 2020
FTC to Host Virtual Workshop on Data Portability on September 22, 2020

Related Statements

September 22, 2020
Opening Remarks of Andrew Smith at Data To Go: An FTC Workshop on Data Portability

THANK YOU!

DEON WOODS BELL
US FEDERAL TRADE COMMISSION
OFFICE OF INTERNATIONAL AFFAIRS

The views expressed do not necessarily reflect the views of the Commission