Fraud Investigation during COVID-19

Is the pandemic a backdoor to increased fraud risk?

Aris Dimitriadis, Executive Director Compliance, ERM & Insurance OTE Group

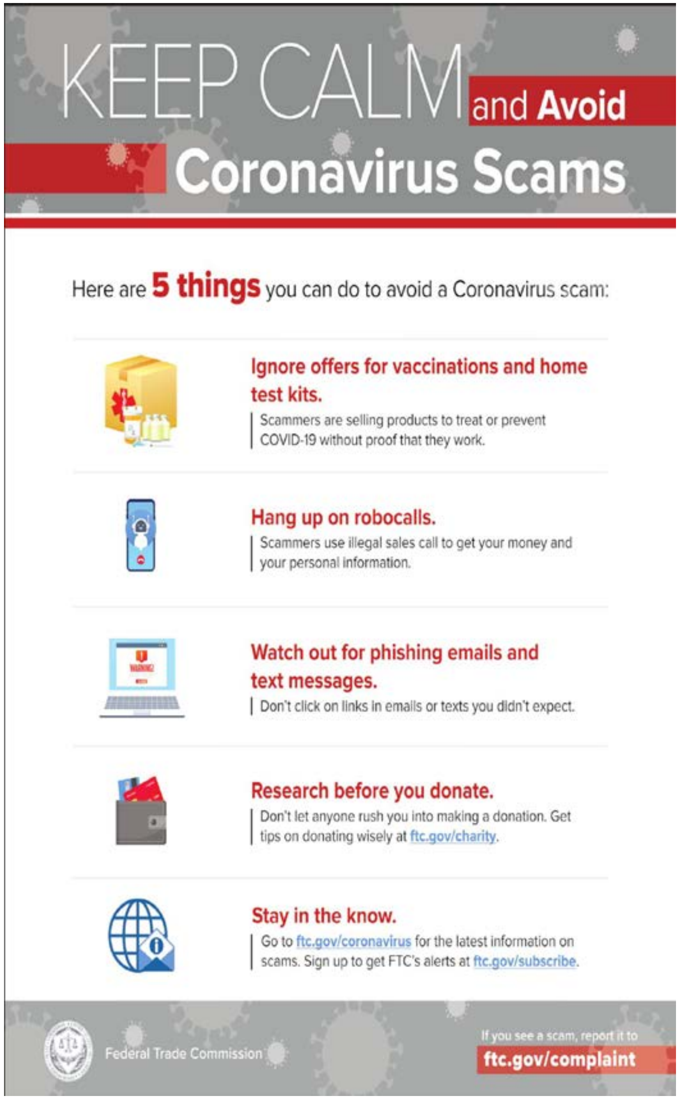
07.05.2020

ΟΜΙΛΟΣ ΕΤΑΙΡΕΙΩΝ

Covid-19 outbreak: an opportunity for fraudsters

Stay vigilant with more than just your health!

- ✓ **Email phishing scams** disguised as messages from the European Centre for Disease Prevention and Control **(ECDC)** and the World Health Organization **(WHO)**. These messages have malicious links that download malware, which gives cybercriminals access to victims’ data.
- ✓ The online sale of **counterfeit** coronavirus **testing kits, face masks, hand sanitizers** and other products much in demand but in short supply. Fake websites purport to sell products that do not exist or others sell them at inflated prices.
- ✓ Fundraising scams by **fake charities** that ask for donations and purport to be involved in fighting the spread of the coronavirus.
- ✓ Fake websites advertising **fraudulent (often dangerous) treatment products, fake cures or medication**.
- ✓ Fraudulent messages promising **tax refunds or financial support** from state encouraging the recipient to share contact details and bank card numbers.



KEEP CALM and Avoid Coronavirus Scams

Here are 5 things you can do to avoid a Coronavirus scam:

Ignore offers for vaccinations and home test kits.
Scammers are selling products to treat or prevent COVID-19 without proof that they work.

Hang up on robocalls.
Scammers use illegal sales call to get your money and your personal information.

Watch out for phishing emails and text messages.
Don't click on links in emails or texts you didn't expect.

Research before you donate.
Don't let anyone rush you into making a donation. Get tips on donating wisely at ftc.gov/charity.

Stay in the know.
Go to ftc.gov/coronavirus for the latest information on scams. Sign up to get FTC's alerts at ftc.gov/subscribe.

Federal Trade Commission

If you see a scam, report it to ftc.gov/complaint

***Infographic from the US Federal Trade Commission**

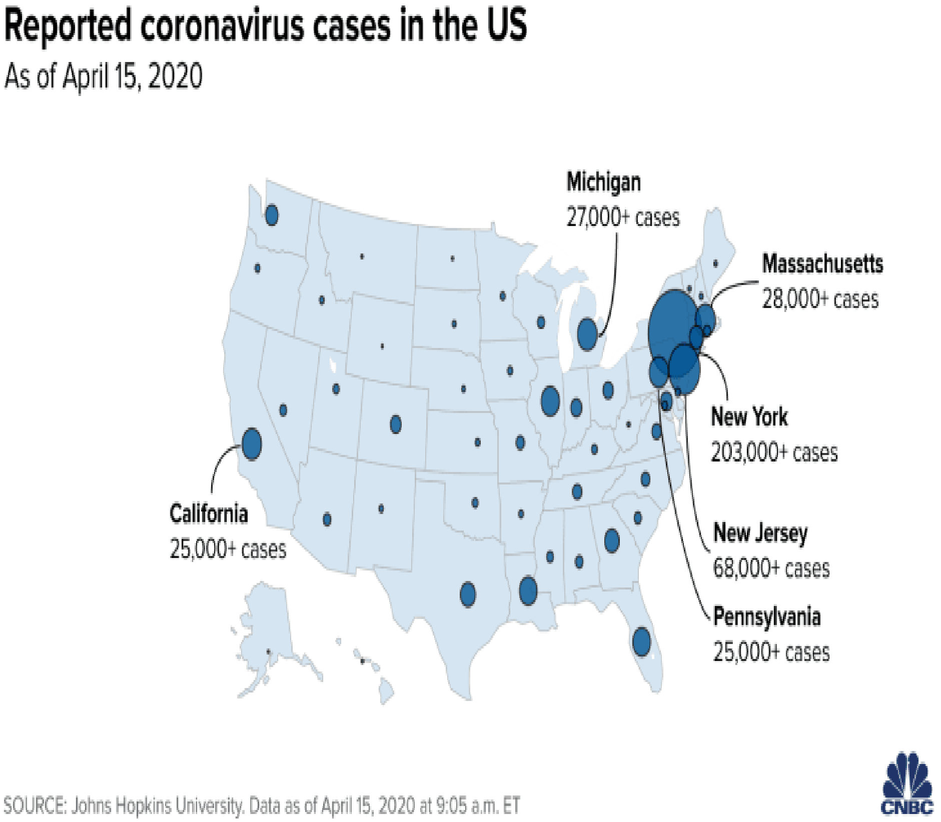
Fraudsters exploiting Covid-19 in numbers

United States of America

Covid-19 scams have cost more than **18,000 Americans** a total loss of **$13.4 million** since the beginning of the year, according to the Federal Trade Commission.

The top fraud categories are related to **travel** and **vacations**, **online shopping**, **bogus text messages** and **imposter scams.**

The typical American lost **$270** among the nearly **310,000 cases of fraud** reported to the agency over that time period.



Reported coronavirus cases in the US

As of April 15, 2020

SOURCE: Johns Hopkins University. Data as of April 15, 2020 at 9:05 a.m. ET

Fraudsters exploiting Covid-19 in numbers

United Kingdom

More than **500 coronavirus-related scams** and over **2,000 phishing attempts** by criminals seeking to exploit fears over the pandemic have been reported to UK investigators.

There have been **509 reports** to the City of London Police with total losses raging approximately to **£1.6m.**

Approximately **50 reports** are being received daily, with **41** of them relating to a scam involving an email asking for **donations** to buy medical supplies, while the other **9** concern fake messages from the government regarding **alleged fines** for leaving home unjustifiably during lockdown.

European Union case*

A sophisticated fraud scheme using compromised emails, advance-payment fraud and money laundering has been uncovered by financial institutions and authorities across **Germany, Ireland and the Netherlands** regarding the procurement **of €15 million** worth of face masks. The buyers sent the wire transfer but the masks never arrived. It turned out the Dutch company - supplier of the masks existed, but their website had been cloned by fraudsters.

Source: Interpol

Notable fraud risk indicators in Covid-19 era

Key pressure points in the new environment that increase the risk of fraud

Fast tracking new suppliers and other business partners

- The risk of onboarding third parties which are not fully vetted and screened may result in working with disreputable or even restricted parties;
- Working with new agents/intermediaries, due either to closure of existing agents or inability to deliver the volume needed;
- The pressure of bringing products very quickly to market.

Increased dealings with government officials

- Regulatory approvals, key IP issues, supply chain, financial aid, donations: all of these are increasing the dealings employees have with government officials in higher risk jurisdictions, many of whom may not be trained for such interactions.

Shift of resources

- Business models are challenged and management may be more focused on operational measures than compliance and fighting fraud;
- The transfer of staff into critical operations may leave prevention functions understaffed;
- Illness among the workforce and absences from work become an issue in terms of resources and finding replacements;
- Ongoing investigations are halted due to lack of resources and in-person interaction;
- Budgets are reduced for any activity considered ‘non-essential’.

Significant job cuts

- In the current situation, every company is looking for savings, and one of the immediate measures is to cut jobs or reduce payments to employees. As experience has shown, for some employees this may create an incentive to commit fraud.

What questions should businesses ask in Covid-19 era?

New ways of working

- Are your employees able to perform their daily tasks remotely? Are digital signatures used?
- Is there still enough oversight and control over operations?
- Are there any controls in place to prevent theft of data by employees working remotely?
- Do you carry out a reprioritization of the risks? (e.g. risks such as approval of gifts and entertainment will be lower, but third party risks related to the supply chain will be greater. Are key controls in place to mitigate them?)

Internal and external risks

- Are there any third parties that will not have capacity or bandwidth to deliver? If yes, would you have time for adequate screening before onboarding new third parties?
- Does the shift or reduction in resources increase the risk of physical misappropriation of assets?

Response

- Did you include anyone from the compliance team in the crisis response taskforce?
- Do you send risk reminder communications to staff, that even in a time of crisis zero tolerance to fraud still applies and that employees should report any suspicious behavior or fraud?
- Are the people dealing with government officials trained in respect of what they are allowed to do and what they cannot do?

Financial risks

- Is the company eligible for any of the government aid? Is there a risk that conditions for eligibility are partially fabricated?
- Is there a risk that cash pooling and intercompany loan set up are changed?
- Is there still enough oversight over bank transfers and defined authorization procedures?

.

Conduct fraud investigations in Covid-19 era

Concerns

- The usual methods for conducting a meaningful and thorough investigation need to change quickly and adapt to social distancing and self-isolation.

- In-person document collection and review as well as face-to-face interviews are out, therefore questions and new challenges have arisen for investigators.

- For example, without in-person witness interviews, how can the investigator truly assess the merits of any whistleblower report or a witness's credibility? How can documents be shown to a witness sitting in a different city/country if borders are closed and flights are cancelled?

- With the investigator accessing company's data remotely how can the security of that data be guaranteed from phishing and other cyber attacks?

- The risks to telephone interviews are remarkable: e.g. recording, no credibility evaluations, and no certainty as to the number of listeners on the telephone call.

Conduct fraud investigations in Covid-19 era

Investigation Techniques

01 **Interviews:** Conduct witness interviews virtually, using videoconference, not phone, ensuring compliance with GDPR and other applicable laws.

02 **Suspicious employee misconduct:** Use remote access to capture and preserve evidence of potential employee misconduct.

03 **Suspicious data transfer:** Leverage data loss prevention software to log and prevent or encrypt sensitive or proprietary information which employees attempt to transfer outside the company's network and systems using email, USB drives, and cloud-based file sharing websites.

04 **Monitor and restrict web browsing:** Require employees to use VPN access in order to be able to log or prevent attempts to browse in dangerous or non-sanctioned sites.

05 **Cyber-crime:** Monitor email logs for suspicious or malicious activities and export relevant logs for potential future analysis. Create alerts for new rules, external forwarding, and other risky behaviors.

06 **Insurance / Health care fraud:** Configure access credentials so that only authorized users can review electronic medical records remotely.

07 **Data transfer:** Use a secure file sharing method to transfer accounting records and other proprietary transaction data. For large data-sets consider leveraging a secure cloud provider.

08 **Document review:** Use virtual data rooms to facilitate reviews of confidential information in a secure, online environment.

Thank you!

KEEP
CALM
AND
MASK
ON

OTE
GROUP OF COMPANIES