



PROGRAM MATERIALS

Program #30113

April 15, 2020

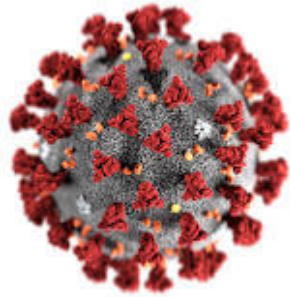
**COVID-19 Scams: Crisis and Isolation
Create an Opportunity for
Exploitation - Be Aware and Be
Secure**

**Copyright ©2020 by Michelle Schaap, Esq. and Shirley
Emehelu, Esq. - Chiesa Shahinian & Giantomasi PC. All
Rights Reserved.**

Licensed to Celesq®, Inc.

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 180, Boca Raton, FL 33487
Phone 561-241-1919 Fax 561-241-1969



COVID-19 SCAMS: CRISIS AND ISOLATION CREATE AN OPPORTUNITY FOR EXPLOITATION BE AWARE AND BE SECURE

Michelle A. Schaap, Esq. and Shirley U. Emehelu, Esq.
Chiesa Shahinian & Giantomasi PC
April 15, 2020

BEFORE WE BEGIN...

This outline has been prepared for a presentation regarding COVID-19 Scams and Fraud. Ms. Schaap is admitted to practice law in the State of New Jersey, and Ms. Emehelu is licensed to practice law in the States of New York, New Jersey and Connecticut. This outline is for informational purposes only and is not intended to constitute legal advice. Every matter has specific facts and special circumstances requiring its own analysis by legal counsel. References to websites, resources or publications in this outline are not intended, and should not be interpreted, as an endorsement by the authors of any product or opinion set forth therein. Website and resource addresses are provided for reference only and the presenters make no guarantee as to their accuracy or reliability.

IN THE BEST OF TIMES...

- We caution our clients to be vigilant:
 - Do not click on suspect links
 - Use robust passwords and multifactor authentication
 - Do not provide credentials or sensitive information to a caller without verifying



BUT IN THE WORST OF TIMES....

- Scammers and malicious actors prey on victims large and small, corporate and individual
- They look to take advantage of our:
 - Fears
 - Charity
 - Isolation



NOT WHAT THEY SEEM....

- Two malicious sites were launched in recent weeks seeking to lure people into clicking on links and downloading malware.
- The first, **antivirus-covid19[.]com** was taken down, but as of April 3, the second was still live and distributing its malicious payload: **corona-antivirus[.]com**.

AND WITH MANY COMPANIES HURRIEDLY MOVING TO REMOTE OPERATIONS

- Personnel may be...
 - Improperly trained
 - Using insufficiently secured devices
 - Printing sensitive documents on personal devices
 - Working in a space where others may view sensitive information
- Personal devices...
 - May not be managed by mobile device management solutions
 - May be shared by other family members



WITH BUSINESS TRANSACTIONS STILL OCCURRING (WE ALL HOPE)....

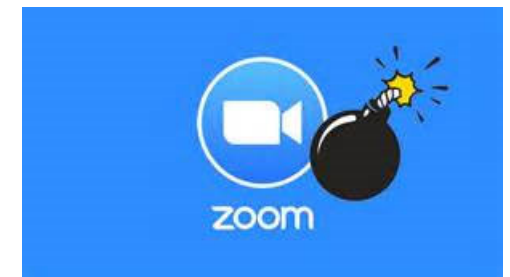
- It may not seem odd for changed wire instructions coming from a gmail or aol address rather than a normal company address
- Nor would it necessarily seem odd to receive contact information for a business partner that is not the “normal” phone number



ZOOM INTO THE DARKNESS

FBI has reported an increasing number of cases involving the hijacking of Zoom videoconferences (called “Zoom-bombing”).

- In the middle of a classroom lesson, a business meeting or a friendly online visit, malicious actors are posting pornographic images, messages of hate and threatening language.
- Zoom has and continues to release patches and updates... do not hit “remind me later!” – verify the patch and then distribute to your remote workforce



AND WITH PEOPLE LOOKING TO DO GOOD

- We are seeing so many requests for donations....
 - But are they real...
 - Or a false link for a real organization
 - Or a fake organization with a credible name
- Homeland Security Investigations (HSI) has seen an uptick in emails with malicious attachments or links to fraudulent websites to trick victims into revealing sensitive information or donating to fraudulent charities or causes.



AND BECAUSE MANY OF US ARE SEEING “NEW” EMAILS FOR OTHERWISE TRUSTED CONTACTS...

- We may be less cautious before clicking on a link
- HSI reports an increase in ransomware across the world



AND FOR THOSE WHO ARE PRAYING FOR A MIRACLE....

- There are many websites promising quick cures....



- Others promise to ship masks, gloves and other essential supplies....

YOU CANNOT PURCHASE A VACCINE OR TESTING KIT ONLINE!

- Bad actors are ready to sell you products that claim to cure or treat COVID-19
 - Sadly, there is not “miracle” to be found online or otherwise



- And no, the FDA has NOT authorized any home testing kits...



BEFORE YOU UNWITTINGLY BECOME THE SUPPOSEDLY TRUSTED SOURCE....

- Do not “just” hit forward when you receive something “interesting” about COVID-19
- Do not share links to charities or suppliers unless you first have verified the links yourself



REMOTE WORKFORCE LEFT UNCHECKED...

“The risk of negligent employees and contractors causing a data breach or ransomware is getting worse. **Sixty percent** of respondents in companies that had a data breach say the **root cause of the data breach was a negligent employee or contractor, Sixty-one percent** of respondents say **negligent employees put their company at risk for a ransomware attack...**

- <https://www.keepersecurity.com/assets/pdf/Keeper-2018-Ponemon-Report.pdf>



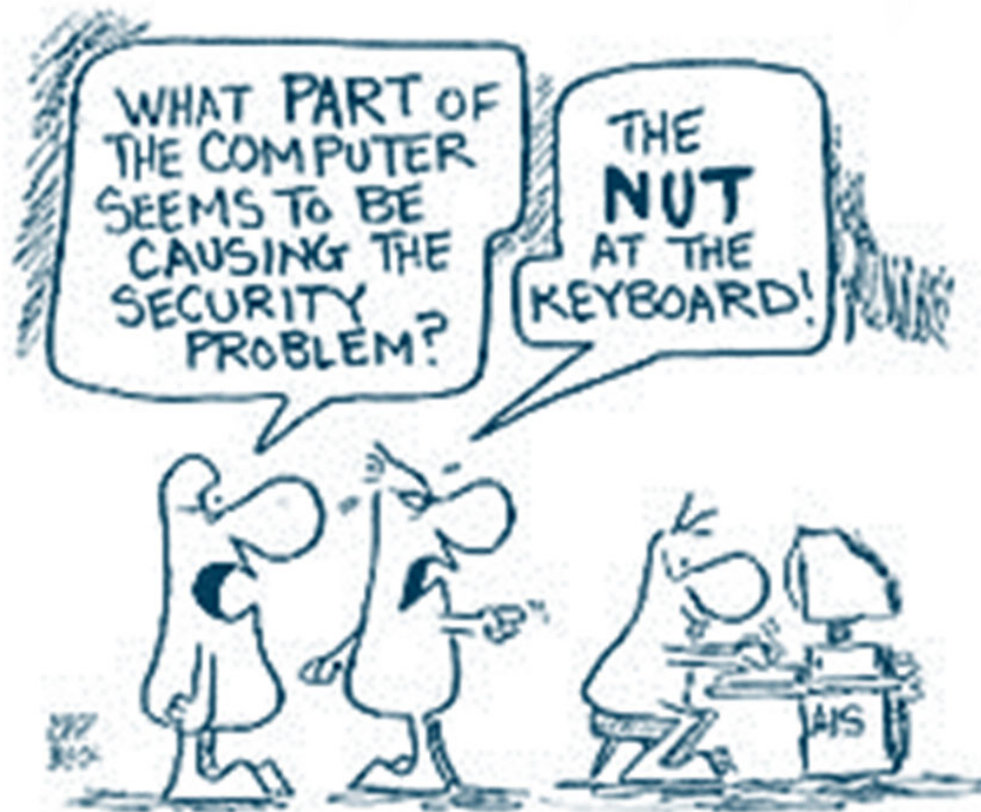
SAFEGUARD YOUR VIDEOCONFERENCES:

- Do not make meetings or classrooms public. Instead, either set a password or set up a waiting room and admit only intended participants
- Do not share the link to the conference through an unrestricted public post
- Restrict screen sharing to the host unless otherwise necessary
- Use meeting passwords



- Make sure that participants are using the most recent version of the platform
- Lock the meeting after all invited participants “arrive”

TRAIN PERSONNEL!



SUSPECT EMAILS

- Suspicious Email
 - Sender - do you know the sender?
 - Email Address – note: @outlook.com
 - michells@csglaw.com
 - michells@csglaw.com
 - mas123@gmail.com
 - masl23@gmail.com

From: dredge lic <dredge-lic@outlook.com>
To: cnbradshaw@pbnlaw.com
Cc:
Subject: DRAFTING AGREEMENT

dredge lic

Dear Counsel ,

We are a Europe based Marine Construction

firm and we need an attorney
to assist us in drafting a purchase and Sales

agreement with a buyer
in your area. Are you able to take this

matter? If not, a referral
will be appreciated.

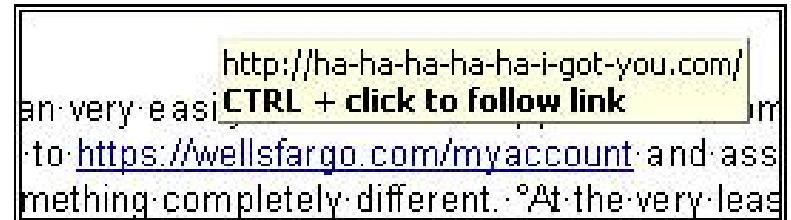
Thank you Regards,

Johan Fredrik CEO
Boskalis Sweden AB
Vassgatan 3 D
415 02 GÖTEBORG
SWEDEN

+46 (0)31 40 75 36

DON'T TRUST – AND VERIFY

- Links can very easily be masked to appear to be something they are not. For example, you may see a link to <https://wellsfargo.com/my> account and assume it is legitimate, when in fact that link actually points to something completely different.
- At the very least, hover the mouse over a link without clicking on it. You'll see a small window pop up which tells you where that link really points.
- Check the mouse over display to confirm that it matches the text of the link before clicking.



FBI KILL CHAIN FOR WIRES

- If you realize that you have sent a wire to a fraudulent account contact the FBI ASAP!
- If you report within 48-72 hours, the FBI may be able to recapture all or a portion of your funds, but you **MUST** report as soon as possible
- www.tips.fbi.gov
- Or call your local FBI field office



MITIGATE THIRD PARTY RISKS

- Remember that your customers and vendors are now also largely working remotely.
- Vet new AND existing vendors
 - Ask how they are securing and managing their remote work forces
 - Ask what they have done to secure their videoconferencing
 - Assess their practices... and ask for confirmation



IF YOU WANT THE FACTS...

Go to the known sites yourself...

- CDC at www.cdc.gov and www.coronavirus.gov
- FDA at <http://www.fda.gov/>



BEFORE YOU DONATE....

- Do not “assume” that an email with a COVID-19-related subject line, attachment, or hyperlink is “real.”
- Do not reveal personal or financial information in email
- Do your own independent research
 - Verify a charity’s authenticity before making donations.



AVOID RANSOMWARE AND OTHER ONLINE DISASTERS...



- ✓ Update software and operating systems with the latest patches.
- ✓ Never click on links or open attachments in unsolicited emails.
- ✓ Backup data on a regular basis. Follow safe practices when browsing the Internet.
- ✓ Restrict users' permissions to install and run software applications
- ✓ apply the principle of “least privilege” to all systems and services.
- ✓ Use application whitelisting to allow only approved programs to run on a network.
- ✓ Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email to prevent email spoofing.
- ✓ Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- ✓ Configure firewalls to block access to known malicious IP addresses.

NOW WOULD BE A GOOD TIME TO TEST BACKUPS...



- Have your data backed up...
 - And consider how often your data should be backed up... daily? hourly?
 - TEST your back up data – make sure you have what you think you have!
 - If it is stored in the cloud, how quickly can you access it?
 - Do you have clean servers (if needed) on which to load your clean data?
 - TEST how quickly you can be “back up and running”

WHERE IS YOUR INCIDENT RESPONSE PLAN AND DO YOU NEED TO (TEMPORARILY) UPDATE POINTS OF CONTACT FOR THE INCIDENT RESPONSE TEAM?

- Data breaches will not happen conveniently....
- And IF you are not in your office... or you were hit by ransomware, the incident response plan that is stored on your computer or at your office is NOT going to help!



- Review your points of contact...
 - Do you have home numbers? Cell numbers?
 - Home email addresses?

LAW ENFORCEMENT HAS PRIORITIZED CRACKING DOWN ON COVID-19 SCAMS...

- U.S. AG William Barr has directed all federal law enforcement, litigating divisions and U.S. Attorneys to join forces with state and local law enforcement to ensure that scams are reported, investigated, and combatted swiftly



COVID-19-RELATED CRIMINAL LIABILITY

Depending on the facts of the scheme, COVID-19-related scams may violate a number of the criminal provisions in Title 18 of the United States Code, including:

- Mail Fraud (§ 1341)
- Wire Fraud (§ 1343)
- Computer Fraud (§ 1030)
- Healthcare Fraud (§ 1347)
- Conspiracy to Commit Fraud (§ 1349)
- Identification Fraud and Aggravated Identity Theft (§§ 1028-1028A)
- Fraud in Connection with Major Disasters and Emergencies id. (§ 1040)
- Trafficking in Counterfeit Goods (§ 2320)



U.S. v. KEITH LAWRENCE MIDDLEBROOK (S.D.CA)

Alleged COVID-19 Treatment and “Cure” Investment Scam

▪ Criminal Complaint Alleges:

- Middlebrook promised massive profits in return for investments in his co.’s Quantum Prevention CV Inc. (QP20) – claimed to mass produce COVID-19 prevention pills and an injectable, “patent-pending” COVID-19 cure serum; and Quantum Cure CV 2020 (QC20) – claimed would be used to market the supposed COVID-19 prevention pills and the injectable “cure.”
- Middlebrook falsely claimed that Magic Johnson was a member of his co’s board of directors.
- Texted to a cooperating witness: “Investors who come in at ground level say \$1M will parachute with \$200M – \$300M...Conservative Minimum.”
- Posted an advertising video on his Instagram account, brandishing a syringe with a clear liquid while describing how his COVID-19 “cure” worked.

SEARCH AND SEIZURE OF UNAUTHORIZED COVID-19 TESTING KITS (D.OR)

- Executing a court-issued federal search warrant, federal authorities intercepted a shipment of 100 unauthorized COVID-19 test kits sent from China to a man in Portland, Oregon.
- The supposed at-home test kits cost the Oregon man only 50 cents each, a preposterous cost for what are likely fake kits – given that legitimate COVID-19 swab tests now run at least \$1,000 through certain private insurers and cost more if obtained through an FDA-approved lab test center.
- The shipped tests did not have FDA clearance or pre-market approval to manufacture home test kits for COVID-19 detection.
- The source of the kits, Anhui DeepBlue Medical Technology Co. Ltd. of Hefei, China, advertised and sold the kits on its ecommerce website.
- Online commentary questions efficacy of the kits.

CRIMINALLY WEAPONIZING COVID-19 TO HARM THE PUBLIC

- Coronavirus appears to meet the statutory definition of a “biological agent” under 18 U.S.C. § 178(1).
- Accordingly, intentionally exposing or threatening to expose someone to COVID-19, potentially could implicate the Nation's terrorism-related statutes criminalizing:
 - Developing/Possessing a Biological Agent for Use as a Weapon (id. § 175);
 - Threats by Wire (id. § 875);
 - Threats by Mail (id. § 876);
 - Dissemination of False Information and Hoaxes Regarding Biological Weapons (id. § 1038);
 - Use of a Weapon Involving a Biological Agent (id. § 2332a).





**NATIONAL
SECURITY**

HEALTH CARE PROFESSIONALS: INCREASED POTENTIAL FOR FRAUDULENT SALES OF COVID-19-RELATED MEDICAL EQUIPMENT

- The FBI warns the health care industry of a potential spike in frauds dealing with the purchase of COVID-19-related medical equipment.
- Beware of scammers capitalizing on the current stress on the supply chain by promising equipment they do not have access to, in an attempt exploit your urgent needs.
- Take particular care and conduct due diligence when transacting with any vendors that you have never worked with or never heard of before, and when placing your faith in unidentified third-party brokers in the supply chain.

RED FLAGS: SHADY SALES PRACTICES

When Purchasing COVID-19 Related Medical Equipment, Beware of:

-  Unusual payment terms (e.g., supplier asking for up-front payments or proof of payment)
-  Last-minute price changes
-  Last-minute excuses for shipment delay (e.g., claims that the equipment was seized at port or stuck in customs)
-  Unexplained source of bulk supply

HOARDING/PRICE GOUGING CORONAVIRUS PROTECTIVE EQUIPMENT AND SUPPLIES

- The DOJ has declared it illegal to acquire medical supplies and devices designated by the Secretary of Health and Human Services (HHS) as scarce in order to hoard them or sell them for excessive prices.
 - May be prosecuted under the Defense Production Act. See 50 U.S.C. §§ 4512, 4513.
- A task force led by USA Craig Carpenito of the District of New Jersey is investigating and prosecuting this conduct.



*United States Attorney
District of New Jersey*

CSG

Chiesa Shahinian
& Giantomasi PC

HOARDING/PRICE GOUGING CORONAVIRUS PROTECTIVE EQUIPMENT AND SUPPLIES

- On March 25, the Department of Health and Human Services issued an executive order designating certain scarce health and medical resources necessary to respond to the spread of the Coronavirus, including:
 - N95 filtering face-piece respirators
 - personal protection equipment (PPE) face masks
 - surgical masks
 - sterilization services
 - disinfecting devices
- Hoarding/Price Fixing of these Products and Services may result in criminal prosecution



U.S. v. BARUCH FELDHEIM (D.N.J.)

- On March 30th, the FBI arrested Baruch Feldheim, a resident of Brooklyn, NY, and charged him by criminal complaint with assaulting a federal officer and with making false statements to law enforcement.
- Feldheim allegedly sold certain HHS-designated materials, including N95 respirators, to doctors and nurses at inflated prices. For example, a NJ doctor contacted Feldheim via a WhatsApp chat group labeled “Virus2020!” Feldheim agreed to sell approx. 1,000 N95 masks and other items to him for \$12,000, an approx. 700% markup from their normal price.
- Feldheim directed the doctor to an auto repair shop in Irvington, NJ, to pick up the order, where the doctor saw enough materials, including hand sanitizers, Clorox wipes, chemical cleaning supply agents, and surgical supplies, to outfit an entire hospital. Feldheim later told the doctor that he had been forced to move all of those supplies from Irvington to another location.
- Feldheim made false statements to FBI agents, including falsely claiming to work for a company that bought and sold PPE, falsely claiming that he did not possess large quantities of PPE and that he never sold them directly to individuals.

GUIDANCE FOR FINANCIAL INSTITUTIONS

- The Financial Crimes Enforcement Network (FinCEN) recently called on financial institutions to be alert for potentially malicious or fraudulent COVID-19-related transactions – similar to those that spike following natural disasters.



GUIDANCE FOR FINANCIAL INSTITUTIONS

- FinCen urges financial institutions to be on the alert for COVID-19-related fraud and misconduct typologies, such as:



Imposter Scams – Solicitations of donations, theft of personal information, or distribution of malware by impersonating government agencies (e.g., Centers for Disease Control and Prevention), international organizations (e.g., World Health Organization (WHO)), or healthcare organizations.



Investment Scams – The U.S. Securities and Exchange Commission (SEC) has cautioned investors to be on alert for COVID-19-related investment scams, such as false claims by publicly traded companies that their products or services can prevent, detect, or cure coronavirus.

FINANCIAL INSTITUTIONS – REPORTING OBLIGATIONS UNDER THE BSA . . .



Product Scams – The U.S. Federal Trade Commission (FTC) and U.S. Food and Drug Administration (FDA) have issued public statements and warning letters to companies selling unapproved or misbranded products that make false health claims pertaining to COVID-19.



False Marketing of COVID-19-related supplies, such as certain facemasks.



Insider Trading – Suspected COVID-19-related insider trading.

FINANCIAL INSTITUTIONS – REPORTING OBLIGATIONS UNDER THE BSA . . .

Suspicious Activity Reports (SARs)

- In addition to checking the appropriate suspicious activity report-template (SAR-template) box(es) for certain typologies, FinCEN also encourages financial institutions to enter **“COVID19”** in **Field 2** of the SAR-template.

The image shows a sample of the Suspicious Activity Report (SAR) form, Form FD-2039. The form is titled "Suspicious Activity Report" and includes the following sections and fields:

- Header:** Form FD-2039, dated 08/03/2011. Previous editions will not be accepted after September 30, 2011. It also lists the FDIC, OCC, CTF, and NCUA as primary federal regulators.
- Part I: Reporting Financial Institution Information**
 - 2. Name of Financial Institution
 - 4. Address of Financial Institution
 - 6. City, State, and Zip Code
 - 8. Address of Branch (if field) where activity occurred
 - 10. City, State, and Zip Code
 - 14. Account number of field, if any
- Part II: Suspect Information**
 - 15. Last Name or Name of Entity, First Name, Middle
 - 18. Address, City, State, and Zip Code
 - 24. Phone Number - Residence, Phone Number - Work
 - 26. Occupation/Type of Business, Date of Birth, Admission Confession?
 - 28. Points of Identification for Suspect: Other's License/State ID, Passport, Alien Registration, Other
 - 30. Relationship to Financial Institution: Account, Agent, Appraiser, Attorney, Borrower, Appraiser, Broker, Customer, Director, Employee, Officer, Shareholder, Other
 - 32. Date of Suspension, Termination, Resignation

IF YOU OR YOUR BUSINESS IS COMPROMISED...

If you buy counterfeit products:

- ✓ Report to the **FBI** at www.ic3.gov and to the National Intellectual Property Rights Coordination Center at www.iprcenter.gov

If your identity is compromised or you fall victim to a scam:

- ✓ Report scam to the **National Center for Disaster Fraud (NCDF) Hotline** by calling **1-866-720-5721** or by email at diaster@leo.gov
- ✓ Report incident to the **FBI's Internet Crime Complaint Center** at www.ic3.gov and **NJ Cybersecurity and Communications Integration Cell (NJCCIC)** at www.cyber.nj.gov/
- ✓ Report any theft to your **local police department**.
- ✓ If your credit card was involved, contact the **credit card company**.
- ✓ Check your credit report with **Equifax, TransUnion** or **Experian**.
- ✓ If your social security number was involved: www.identitytheft.gov or call **1-877-IDTHEFT**.
- ✓ If a tax filing was compromised: www.IRS.gov/UAC/Identity-Protection or call **1-800-908-4490**.



THANK YOU



Shirley U. Emehelu, Esq.
Member

Chiesa Shahinian & Giantomasi PC

973.530.2127

semehelu@csglaw.com

White Collar/Investigations Practice



Michelle A. Schaap, Esq.
Member

Chiesa Shahinian & Giantomasi PC

973.530.2026

mschaap@csglaw.com

Cybersecurity/Data Privacy Practice

