



Morgan Lewis

# CYBERINSURANCE: IS YOUR COMPANY COVERED?

Mark Krotoski and Jeffrey Raskin

June 2, 2020

© 2020 Morgan, Lewis & Bockius LLP

**SECTION 01**  
**OVERVIEW**



# OVERVIEW

- 1 COVID-19 risks during remote access based on new threats and vulnerabilities
- 2 Increased threats due to growing reliance on online ordering and delivery, and how this affects coverage
- 3 Coverage implications when large parts of the workforce work at home instead of the office
- 4 California Consumer Privacy Act (CCPA) Updates Prior to July 1st Enforcement Period



**SECTION 02**

**COVID-19 RISKS DURING  
REMOTE ACCESS BASED ON  
NEW THREATS AND  
VULNERABILITIES**

# NEW THREATS

LILY HAY NEWMAN

SECURITY 03.19.2020 02:12 PM

## Coronavirus Sets the Stage for Hacking Mayhem

As more people work from home and anxiety mounts, expect cyberattacks of all sorts to take advantage.



ComputerWeekly.com IT Management Industry Sectors Technology Topics Search Computer Weekly

### Coronavirus now possibly largest-ever cyber security threat

The cumulative volume of coronavirus-related email lures and other threats is the largest collection of attack types exploiting a single theme for years, possibly ever

By Alex Scroxton, Security Editor Published: 18 Mar 2020 15:47

The total volume of phishing emails and other security threats relating to the Covid-19 coronavirus now represents the largest coalescing of [cyber attack](#) types around a single theme that has been seen in a long time, and possibly ever, according to Sherrod DeGrippo, senior director of threat research and detection at Proofpoint.

How to get the most out of the Internet of Things CIO Trends #7

Tailoring your IT operating model to the digital age Free Download ComputerWeekly.com


Morgan Lewis


<https://www.wired.com/story/coronavirus-cyberattacks-ransomware-phishing/>

<https://www.computerweekly.com/news/252480238/Coronavirus-now-possibly-largest-ever-cyber-security-threat>

# NEW THREATS

Re:SAFTY CORONA VIRUS AWARENESS WHO

 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



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

Regards,

Dr. Stella Chungong  
Specialist wuhan-virus-advisory

**FAKE**

**Morgan Lewis**

<https://www.consumer.ftc.gov/blog/2020/03/ftc-coronavirus-scams-part-2>  
<https://www.consumer.ftc.gov/blog/2020/02/coronavirus-scammers-follow-headlines>

# TEXTING



# REQUESTING PERSONAL INFORMATION

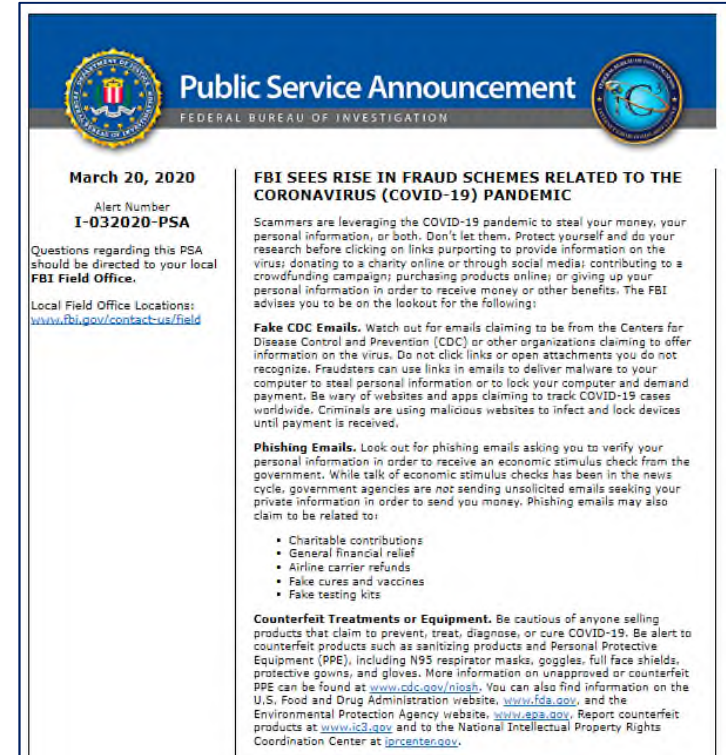
The screenshot shows the GOV.UK website interface. At the top, there is a search bar and a navigation bar with the text "Tell us what you think of GOV.UK" and "Take a short survey to give us your feedback". Below this, a breadcrumb trail reads "Home > Housing and local services > Council Tax". The main heading is "Enter Your Post Code To Apply for COVID-19 Relieve". Underneath, it says "NHS COVID-19 Relieve system." and provides a form to "Enter a postcode" with an example "SW1A 2AA" and a "Find" button. To the right, there is a "Related content" section with links for "Council Tax" and "Check your Council Tax band", and an "Explore the topic" section with a link for "Council Tax". Below the form, there is a "What you need to know" section with a bullet point "Relieve coverage so far" and a "Last updated: 20 March 2020" note. At the bottom of the page, there are two feedback questions: "Is this page useful? Yes No" and "Is there anything wrong with this page?". The footer contains two columns of links: "Services and information" (Benefits, Births, deaths, marriages and care, Business and self-employed, Childcare and parenting, Education and learning, Employing people, Environment and countryside, Housing and local services) and "Departments and policy" (How government works, Departments, Worldwide, Publications).



# PHISHING

## • Phishing Emails.

- Look out for phishing emails asking you to verify your personal information in order to receive an economic stimulus check from the government. While talk of economic stimulus checks has been in the news cycle, government agencies are *not* sending unsolicited emails seeking your private information in order to send you money. Phishing emails may also claim to be related to:
  - Charitable contributions
  - General financial relief
  - Airline carrier refunds
  - Fake cures and vaccines
  - Fake testing kits



**Public Service Announcement**  
FEDERAL BUREAU OF INVESTIGATION

**March 20, 2020**  
Alert Number  
**I-032020-PSA**

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:  
[www.fbi.gov/contact-us/field](http://www.fbi.gov/contact-us/field)

**FBI SEES RISE IN FRAUD SCHEMES RELATED TO THE CORONAVIRUS (COVID-19) PANDEMIC**

Scammers are leveraging the COVID-19 pandemic to steal your money, your personal information, or both. Don't let them. Protect yourself and do your research before clicking on links purporting to provide information on the virus; donating to a charity online or through social media; contributing to a crowdfunding campaign; purchasing products online; or giving up your personal information in order to receive money or other benefits. The FBI advises you to be on the lookout for the following:

**Fake CDC Emails.** Watch out for emails claiming to be from the Centers for Disease Control and Prevention (CDC) or other organizations claiming to offer information on the virus. Do not click links or open attachments you do not recognize. Fraudsters can use links in emails to deliver malware to your computer to steal personal information or to lock your computer and demand payment. Be wary of websites and apps claiming to track COVID-19 cases worldwide. Criminals are using malicious websites to infect and lock devices until payment is received.

**Phishing Emails.** Look out for phishing emails asking you to verify your personal information in order to receive an economic stimulus check from the government. While talk of economic stimulus checks has been in the news cycle, government agencies are not sending unsolicited emails seeking your private information in order to send you money. Phishing emails may also claim to be related to:

- Charitable contributions
- General financial relief
- Airline carrier refunds
- Fake cures and vaccines
- Fake testing kits

**Counterfeit Treatments or Equipment.** Be cautious of anyone selling products that claim to prevent, treat, diagnose, or cure COVID-19. Be alert to counterfeit products such as sanitizing products and Personal Protective Equipment (PPE), including N95 respirator masks, goggles, full face shields, protective gowns, and gloves. More information on unapproved or counterfeit PPE can be found at [www.cdc.gov/niosh](http://www.cdc.gov/niosh). You can also find information on the U.S. Food and Drug Administration website, [www.fda.gov](http://www.fda.gov), and the Environmental Protection Agency website, [www.epa.gov](http://www.epa.gov). Report counterfeit products at [www.ic3.gov](http://www.ic3.gov) and to the National Intellectual Property Rights Coordination Center at [iprcenter.gov](http://iprcenter.gov).

# INCREASED THREATS



## Investor Alerts and Bulletins

### Look Out for Coronavirus-Related Investment Scams - Investor Alert

Feb. 4, 2020

The SEC's Office of Investor Education and Advocacy is issuing this Investor Alert to warn investors about investment frauds involving claims that a company's products or services will be used to help stop the coronavirus outbreak.

Fraudsters often use the latest news developments to lure investors into scams. We have become aware of a number of Internet promotions, including on social media, claiming that the products or services of publicly-traded companies can prevent, detect, or cure coronavirus, and that the stock of these companies will dramatically increase in value as a result. The promotions often take the form of so-called "research reports" and make predictions of a specific "target price." **We urge investors to be wary of these promotions, and to be aware of the substantial potential for fraud at this time.**

- Be cautious of claims that a company's products or services can help stop the coronavirus, especially claims that involve microcap stocks. These claims may be made as part of fraudulent "pump-and-dump" schemes.
- You may lose significant amounts of money if you invest in a company that makes inaccurate or unreliable claims. You may not be able to sell your shares if trading in the company is suspended.
- Submissions of tips, complaints, or referrals relating to suspected securities fraud or wrongdoing can be made online at <https://www.sec.gov/tcr>.

FOR IMMEDIATE RELEASE

Thursday, March 19, 2020

### U.S. Attorneys, Florida AG Issue Warning Against COVID-19 Scam Artists

TALLAHASSEE, FLORIDA – Florida's three United States Attorneys today joined with Florida Attorney General Ashley Moody to warn scam artists that they will vigorously pursue anyone trying to capitalize on the coronavirus pandemic by cheating Florida consumers, especially the state's vulnerable elders. The federal law enforcement team is now actively collaborating and cooperating with the state's top prosecutor team in a concerted effort to stop the scams relating to coronavirus.

The state's top prosecutors at the federal and state levels vowed that their offices are committed to

- **Fake cures** for COVID-19 online;
- **Phishing emails** sent from entities posing as the World Health Organization ("WHO") or the Centers for Disease Control and Prevention ("CDC"); and
- **Malware** being inserted onto mobile phones by apps pretending to track the spread of the virus.

Morgan Lewis

[https://www.sec.gov/oiea/investor-alerts-and-bulletins/ia\\_coronavirus#](https://www.sec.gov/oiea/investor-alerts-and-bulletins/ia_coronavirus#)

<https://www.justice.gov/usao-ndfl/pr/us-attorneys-florida-ag-issue-warning-against-covid-19-scam-artists>

# MOST BUSINESSES HAVE *SOME* CYBER INSURANCE BUT COVERAGE IS OFTEN INADEQUATE

## Hanover Insurance Company study

- 90% of business reported experiencing a cyber attack over the prior year.
- 50% experienced a malware-related attack; 35% involved transmission of malware to a third-party.
- Top security fear: Breach of personally identifiable information.
- 60% of businesses reported they would be unprofitable in less than two days if they lost access to critical systems and data; 92% reported they would experience a negative financial impact.
- 60% of businesses reported having cyber insurance with at least \$1,000,000 in limits; the other 40% had less than \$1,000,000 in limits or no coverage at all. Some of this coverage exists as an “add-on” to general liability coverage with limits between \$10,000 and \$50,000. This may not pay the cost to perform a post-breach forensic analysis, let alone pay the cost of remediation or to defend against, and resolve, a third-party lawsuit.
- Only 11% of business reported a concern of a cyber attack affecting their supply chains, although 88% reported that their businesses were dependent upon third parties.

## **MOST BUSINESSES HAVE *SOME* CYBER INSURANCE BUT COVERAGE IS OFTEN INADEQUATE**

Malware attacks most often occur via a phishing e-mail.

- Coronavirus-related phishing e-mails increased 667% in March – the most common forms were scams, brand impersonation, and business email compromise.

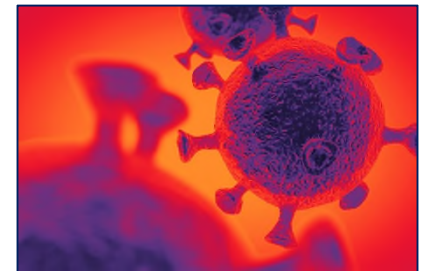


**SECTION 03**

**INCREASED THREATS DUE TO GROWING  
RELIANCE ON ONLINE ORDERING AND  
DELIVERY, AND HOW THIS AFFECTS  
COVERAGE**

# VARIOUS NEW VULNERABILITIES

- Unsecure connections and networks
- Access controls
  - Authentication
  - Weak password security
- Unencrypted devices and data
- Loss of data
- Lost devices
- External access to internal resources
- Lack of physical security controls



# KEY SECURITY ISSUES

## ➤ **Secure Connections**

- No public wi-fi or open internet connections
- VPN / Encrypted connections
- Password-protected connections
- Multi-Factor Authentication (MFA)

## ➤ **Secure End Points (Data At Rest)**

- Encryption
- Endpoint Protection Platforms
- Endpoint Detection and Response

## ➤ **BYOD**

- Layers of control on access to data
- Mobile device management

## ➤ **Strong Passwords or Passphrases**

- Computers, devices
- Network access

## ➤ **Secure Documents**

- Secure, locked storage
- Return for cross-shredding

## ➤ **Training**

- Alert and aware to new risks
- Promote culture of cybersecurity

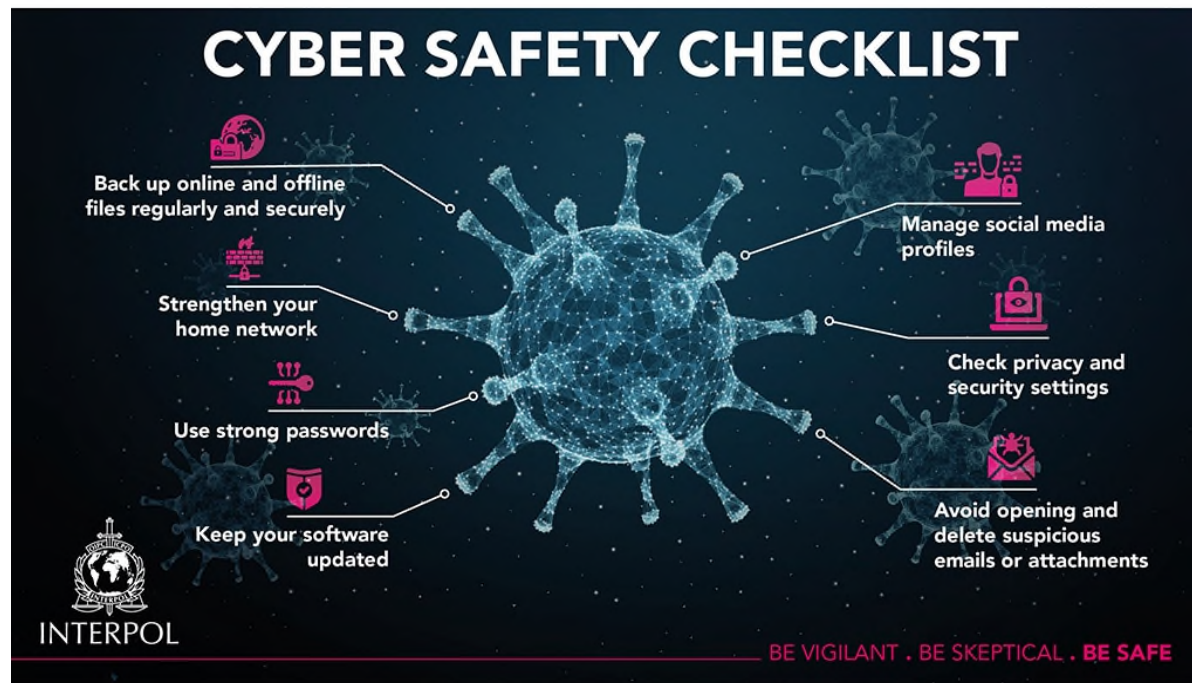
## ➤ **Company Policies**

- Telework Security Policy
- Company Confidential Information Policy
- BYOD (Bring Your Own Device to Work) Policy

## ➤ **Test Incident Response Plan**

- Are you prepared for an incident?
- Emergency contact information
- Business continuity issues

# SAFETY CONSIDERATIONS





## DOJ TIPS

- Independently verify the identity of any company, charity, or individual that contacts you regarding COVID-19.
- Check the websites and email addresses offering information, products, or services related to COVID-19. For example, they might use "cdc.com" or "cdc.org" instead of "cdc.gov."
- Be wary of unsolicited emails offering information, supplies, or treatment for COVID-19 or requesting your personal information for medical purposes.
- Do not click on links or open email attachments from unknown or unverified sources. Doing so could download a virus onto your computer or device.
- Make sure the anti-malware and anti-virus software on your computer is operating and up to date. Keep your operating system up to date as well.
- Ignore offers for a COVID-19 vaccine, cure, or treatment. Remember, if a vaccine becomes available, you will not hear about it for the first time through an email, online ad, or unsolicited sales pitch.
- Check online reviews of any company offering COVID-19 products or supplies.
- Research any charities or crowdfunding sites soliciting donations in connection with COVID-19 before giving any donation.
- Be wary of any business, charity, or individual requesting payments or donations in cash, by wire transfer, gift card, or through the mail. Do not send money through any of these channels.

# BASICS OF CYBER COVERAGE

**Typically provides first and third party coverages**

**First-party coverages:** Protect the insured's property, assets and income

- **Data Recovery:** Pays reasonable and necessary costs of the insured to regain access to, replace or restore data and any reasonable and necessary costs incurred by the insured to determine that its data cannot be accessed, replaced or restored.

# BASICS OF CYBER COVERAGE

## Cyber Extortion: Two possible coverages:

The policy will cover an extortion payment, made with insurer consent, in response to a threat to (a) alter or destroy data; (b) perpetrate unauthorized access to systems; (c) prevent access to systems and or/data; (d) steal or misuse personally identifiable information; (e) introduce malware into the system; (f) interrupt or suspend the system.

Or the policy will cover reasonable and necessary expenses, incurred with insurer consent, to prevent or respond to an extortion threat.

## BASICS OF CYBER COVERAGE

- **Business Interruption:** Pays income loss and specified expenses (including forensic) sustained during a “period of restoration,” and following a “waiting period,” resulting from the suspension of normal business operations caused by the insured’s system failure.
- **Dependent Business Interruption:** Pays income loss and specified expenses (including forensic) sustained during a “period of restoration,” and following a “waiting period,” resulting from the suspension of normal business operations caused by a system failure at a business that provides necessary services or products to the insured.

## BASICS OF CYBER COVERAGE

### Additional Coverages – Usually provided in small amounts:

- **Crisis Management:** Pays public relations expenses incurred in response to negative media coverage necessary to avert or mitigate material damage to the insured's reputation following a cyber event.
- **Consequential Reputation Loss:** Pays documented financial losses resulting from negative media coverage following a cyber event.
- **Telecommunications Fraud:** Pays losses when a third-party gains unauthorized access to the insureds' telecommunications system.

## BASICS OF CYBER COVERAGE

- **Funds Transfer Fraud:** Pays losses when a third-party delivers fraudulent instructions via telephone, electronic mail or other electronic means to a financial institution directing the institution to transfer money from the insured's account to an unauthorized account without the insured's knowledge or consent.
- **Fraudulent Instructions:** Pays losses when a third-party purporting to be a vendor, client or authorized employees provides fraudulent instructions to the insured via electronic mail, the telephone or via the web to transfer money to an unauthorized account.
- **Criminal Reward Fund:** The insurer will a specified amount of money for information that leads to the arrest of individuals committing or attempting to commit any illegal act related to coverage provided under the policy.

# BASICS OF CYBER COVERAGE

Third-Party coverages: Protects the insured against liability claims:

**Privacy Liability and Information Security:** Covers the insured's liability for damages because of a claim for:

- The theft, loss or unauthorized disclosure of personally identifiable information;
- The alteration, corruption, deletion or damage of data stored on the insured's system;
- The failure to prevent the transmission of malicious computer code from the insured's system to a third-party system;

## BASICS OF CYBER COVERAGE

- The participation of the insured's system in a denial of service attack against third-parties.
- The failure to provide timely notice of a breach event in violation of a data breach notice law.
- The failure to comply with the insured's written privacy policies.
- The failure to administer an identity theft program.



# BASICS OF CYBER COVERAGE

## Regulatory Defense and Penalties

- Pays the costs of responding to a request for information, a civil investigative demand or civil proceeding initiated by a governmental entity alleging a potential violation of a privacy law. Some policies will also pay resulting penalties to the extent permitted by the relevant jurisdiction.

# BASICS OF CYBER COVERAGE

## Privacy Notification Costs

- Pays the costs of the insured's obligation to comply with a breach notice law following a breach event. Payable cost include computer expert services, legal services, call center services, credit monitoring and identity theft monitoring.

# BASICS OF CYBER COVERAGE

Other Liability Coverages – Usually provided on an “as needed” basis:

- **PCI Fines, Expenses and Costs:** Pays assessments, fines or penalties imposed by banks or credit card companies due to non-compliance with the Payment Card Industry Data Security Standard (PCI DSS) or payment card company rules.
- **Multimedia and Advertising Liability:** Covers defamation, trade libel, invasion of privacy, misappropriation of likeness, misappropriation of trade secrets, plagiarism, invasion of copyright, infringement of trade dress, false arrest, etc.
- **Technology Errors and Omissions**
- **Technology Products Liability**



**SECTION 04**

**COVERAGE IMPLICATIONS WHEN LARGE PARTS OF THE WORKFORCE WORK AT HOME INSTEAD OF THE OFFICE**

## DOES CYBER INSURANCE COVER EMPLOYEES WORKING AT HOME?

At its most basic level, coverage under a cyber policy is triggered by a “security breach.” Coverage is typically afforded for losses the insured suffers directly (loss of data, damaged hardware, damaged software, business interruption, extortion) and against third-party claims (privacy)

### **Definitions of “Security Breach”:**

- “Unauthorized Access or Use of Computer Systems”
- “Infection of Computer Systems by malicious code or transmission of malicious code from Computer Systems”

## DOES CYBER INSURANCE COVER EMPLOYEES WORKING AT HOME?

**Definition of “Computer System”:** “Computers, any software residing on such computers and associated input and output devices, data storage devices, networking equipment and back up facilities (1) operated by and either owned by or leased to the Insured Organization”

**Definition of “Computer Security”:** “Software, computer or network hardware devices . . . the function of which is to prevent Unauthorized Use Access or Use . . . infection of Computer Systems by malicious code or transmission of malicious code from Computer Systems.”

## DOES CYBER INSURANCE COVER EMPLOYEES WORKING AT HOME?

Some companies previously provided, or provided in anticipation of or in response to shelter-in-place orders, company “owned” or “leased” laptops and/or mobile devices to employees to facilitate working at home.

Other companies, however, may have been forced by circumstances to require employees to use their own computers or mobile devices to work from home.

- Coverage may not be afforded for a “Security Breach” that happens at, or originates from, a home working employee that was not using a company “owned” or “leased” device.
- Cyber insurers usually require companies to maintain certain security measures as a condition of purchasing and maintaining coverage. Those measures likely did not extend to employee-owned devices at the inception of the policies, and companies likely did not think of attempting to comply with insurer imposed security measures, and amending their policy, while quickly seeking to ensure that employees could work at home.

## BASICS OF CYBER COVERAGE

Issues resulting from a “Security Breach” originating from an employee-owned device can potentially different coverage grants in a cyber policy:

- Data Recovery Costs: The costs the insured incurs to regain access to, replace, or restore data resulting from a “Security Breach”
- Business Interruption Loss: Lost income or gross profits resulting from a “System Failure.” A “System Failure” is an unintentional and unplanned outage of “Computer Systems”
- Privacy Liability: Coverage for third-party claims resulting from the insured’s failure to prevent a “Security Breach,” including the failure to “prevent transmission of malicious code” to third-party systems.



## DOES CYBER INSURANCE COVER EMPLOYEES WORKING AT HOME?

Can an argument that a cyber policy does not cover a breach originating with an employee-owned device be defeated? Perhaps:

The insured can argue that it nevertheless exercises control over the employees' personal computing devices and that connectivity to the company's "networking equipment" satisfies the definition of "Computer System" in connection with a covered "Security Breach." This may be a technical, forensic-based argument tracing the cause of the "Security Breach" and the role played by the insured's "networking equipment."

## DOES CYBER INSURANCE COVER EMPLOYEES WORKING AT HOME?

- Better solution: Fix the policy by amending the definition of “computer system” so that it reaches the business use of employee-owned devices at remote locations. Companies now have the time, and the opportunity, to seek to ensure that employee-owned devices comply with insurer-imposed security protocols, and that employees are instructed in best practices in using their personal devices for business purposes.
  - Better definition of “Computer System”: “Computers and related peripheral components, including Internet of Things (“IoT”) devices . . . related communication networks . . . *mobile devices . . . by which electronic data is transmitted, processed, stored, backed-up, retrieved and operated by you.*”
    - The intent is to cover claims resulting from a “security breach,” a “security failure” or “security event” sourced to any computer, related peripheral component or mobile device through which the insured company “transmits” or “retrieves” electronic data.
- The insurer whose policy contains this definition of “Computer System” says on the cover of its cyber policy: “We cover BYOD devices, IoT usage and social media.”

## POTENTIAL IMPACT OF COVID-19 ON CYBER CLAIMS RESOLUTION

- COVID-19 may be the most expensive event in the history of insurance.
- Increased exposure to claims in one area can affect the resolution of claims in other areas.
- Remote working increases the risk of data breaches, and provides a fertile ground for cyber extortion.
- Increased on-line retail transactions increases the risk of data breaches, including for businesses such as restaurants that probably never previously worried about a data breach.
- Criminals love chaos and crisis.

## POTENTIAL IMPACT OF COVID-19 ON CYBER CLAIMS RESOLUTION

- Expect increased insurer scrutiny and fly-specking of cyber claims, particularly on the question of whether a “security breach” resulted from a covered “computer system.”
- Expect increased insurer scrutiny of compliance with security protocols, whether explicitly written into policies or disclosed by the insured as part of the underwriting process. It is highly unlikely that massive remote working was contemplated at the time of contracting.
- All of this means that companies seeking coverage will likely need to increase the amount of money they spend on forensics when seeking coverage. The costs of investigating a remote breach or a remote malware attack can be expensive. Policies could have small sub-limits for these items, and they will erode coverage an insured might need to remedy a problem and/or defend against third-party claims.

# BASICS OF CYBER COVERAGE

Cyber coverage is a relatively small, but growing and profitable “niche” insurance market.

- Overall premium growth was 12% in 2019, up from an 8% increase in 2018.
- “Standalone” cyber premium growth in 2019 was 14%.

## PROJECTED MARKET AND CLAIM TRENDS

- Fitch: “2020 segment premium growth will be tempered by reductions in underwriting exposures from the recent sharp economic contraction tied to the coronavirus pandemic. Cyber coverage purchase practices may change meaningfully in the near term with mounting strain on corporate budgets and profits.”
- Largest growth in new policies and first-time cyber coverage purchases is projected to be in the retail & manufacturing sectors as business increasingly moves on-line, and supply chain management becomes increasingly digital.

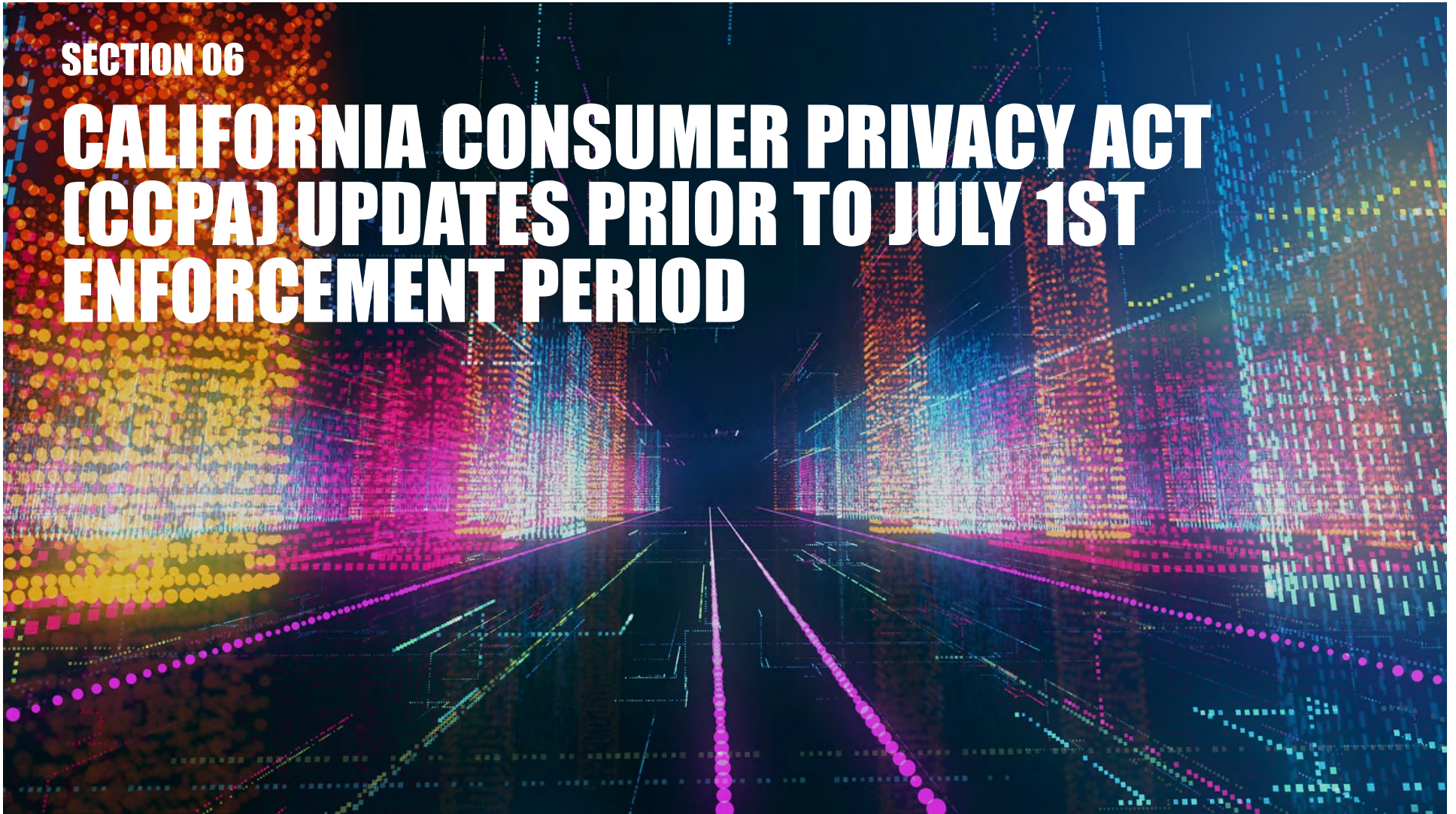
# PROJECTED MARKET AND CLAIM TRENDS

**Insurer exposure to cyber claims will increase for several reasons:**

- Expanding coverage, and the liberalization of policy terms to meet demand
- Remote working as a consequence of COVID-19.
- Consumer protection statutes such as the California Consumer Privacy Act

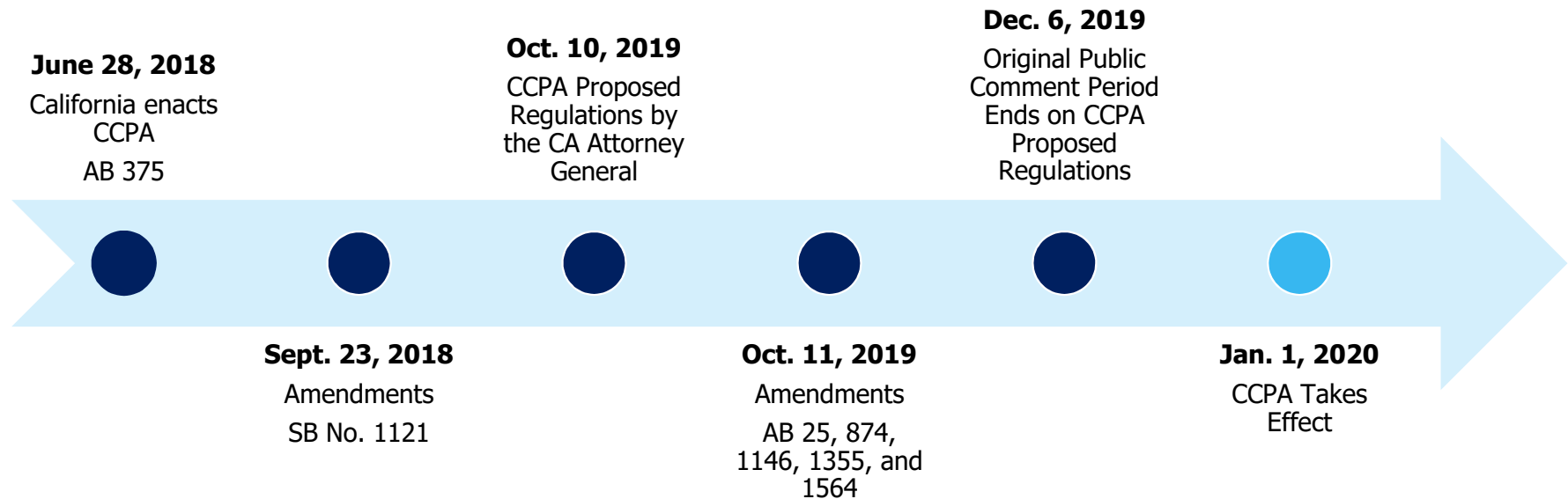
**SECTION 06**

# **CALIFORNIA CONSUMER PRIVACY ACT (CCPA) UPDATES PRIOR TO JULY 1ST ENFORCEMENT PERIOD**

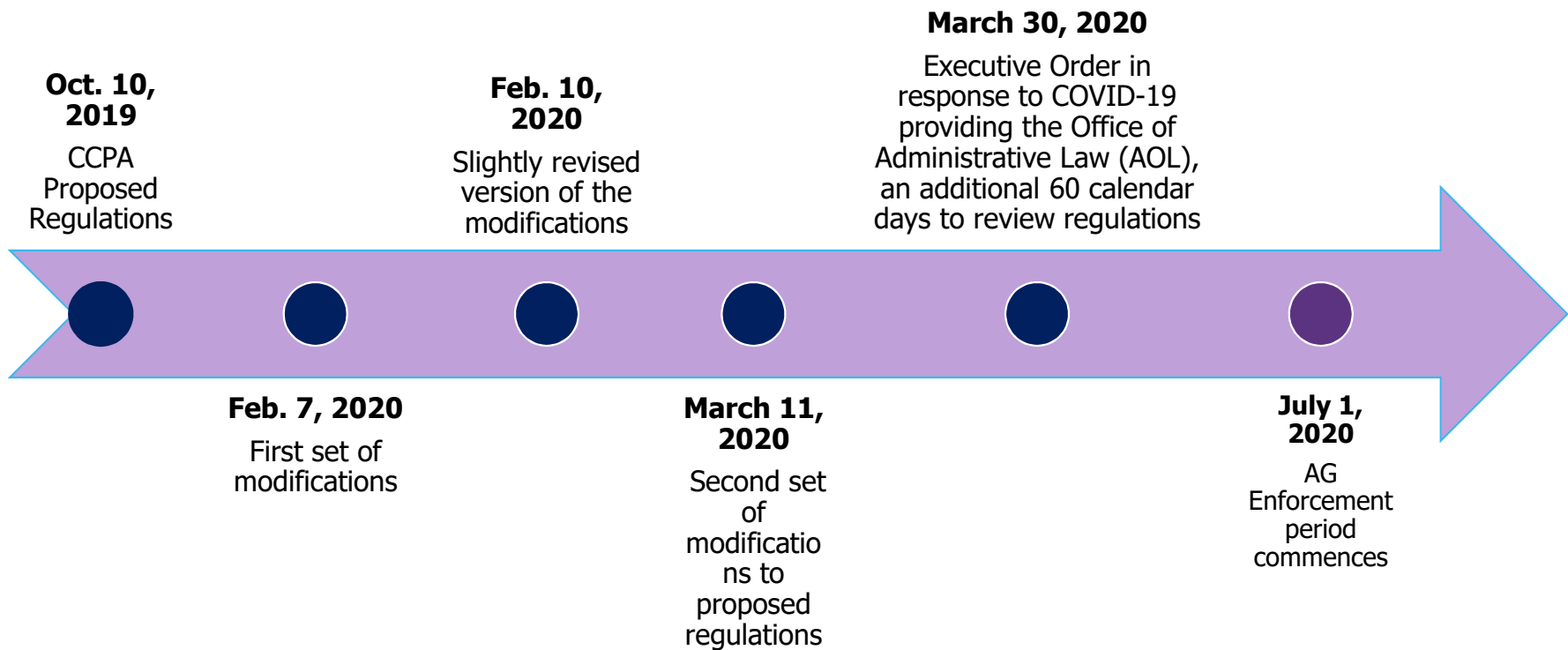




# CCPA TIMELINE



# CCPA REGULATIONS TIMELINE



# ATTORNEY GENERAL ENFORCEMENT

- **Attorney General Civil Enforcement Action**

- Not more than \$7,500 for each intentional violation of the CCPA
- \$2,500 for unintentional violations that the company fails to cure within 30 days of notice
- Injunctive relief
- New Consumer Privacy Fund
  - 20 percent of the collected UCL penalties allocated to a new fund to “fully offset any costs incurred by the state courts and the Attorney General”
  - 80 percent of the penalties allocated “to the jurisdiction on whose behalf the action leading to the civil penalty was brought”

# PRIVATE RIGHT OF ACTION

- **Limited Consumer Private Right of Action**

- Individual consumer or classwide basis
- Only to data breaches, but proposed legislation looks to expand the private right of action to violations of the privacy requirements.

- (1) Nonencrypted or nonredacted **personal information**\*
- (2) “subject to an unauthorized access and exfiltration, theft, or disclosure
- (3) as a result of the business’s violation of the duty to implement and maintain **reasonable security** procedures and practices appropriate to the nature of the information to protect the personal information”

# STATUTORY DAMAGES RANGE

- Court imposes the **greater of statutory or actual damages**
- **Statutory Damage Range**
  - Statutory damages are “not less than” \$100 and “not greater than” \$750 “per consumer per incident”
- **Statutory Damages Factors**
  - Nature and seriousness of the misconduct
  - Number of violations
  - Persistence of the misconduct
  - Length of time over which the misconduct occurred
  - Willfulness of the defendant’s misconduct
  - Defendant’s assets, liabilities, and net worth
  - Other “relevant circumstances presented by any of the parties”

# CCPA NEW ERA IN CYBERSECURITY LITIGATION

- **Key Questions**

- What measures are in place to protect personal information?
- Can you redact and encrypt where possible?
- Can you demonstrate there are reasonable security procedures and practices appropriate to the nature of the information to protect the personal information?
- Are you prepared to respond to an incident?

## CYBER POLICIES SHOULD BE REVIEWED ENFORCEMENT UNDER THE CALIFORNIA CONSUMER PRIVACY ACT BEGINS JULY 1

- Insurers offered new coverages coinciding with the enforcement of the European Union's General Data Protection Regulation.
- New coverages are being offered to address issues arising from the California Consumer Privacy Act ("CCPA"), as well.
- The most effective coverage will include verbiage stating specifically that the policy responds to regulatory proceedings initiated under the CCPA and any lawsuit alleging a violation of the CCPA.

## REGULATORY COVERAGE ENHANCEMENT ENDORSEMENT – CCPA AND GDPR

“The definition of Regulatory Proceeding . . . is deleted and replaced with the following. ‘Regulatory proceeding means a request for information, civil investigative demand or civil proceeding commenced by service of a complaint or similar proceeding:

(1) brought by or on behalf of [a governmental entity] in such entity’s regulatory or official capacity, in connection with such proceeding arising from a security failure or data breach, or

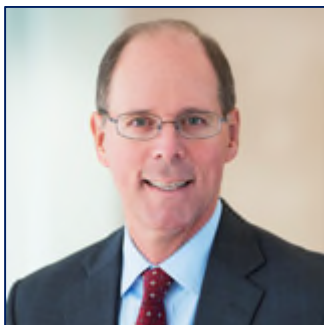
(2) brought for a violation of the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), or other similar federal, state, local or foreign regulation arising from a privacy liability”



## REGULATORY COVERAGE ENHANCEMENT ENDORSEMENT – CCPA AND GDPR

- The insurer that promulgated this endorsement has written that the coverage pays “on your behalf claim expenses and regulatory penalties from a regulatory proceeding, or class action, arising from a security failure or data breach. This includes the associated costs to defend yourself and damages resulting from a class action lawsuit or alleged violation of the CCPA.”

## Mark L. Krotoski



**Mark L. Krotoski**

Silicon Valley

+1.650.843.7212

mark.krotoski@morganlewis.com

**Morgan Lewis**

- Litigation Partner, Privacy and Cybersecurity and Antitrust practices with more than 20 years' experience handling cybersecurity cases and issues.
- Co-Head of Privacy and Cybersecurity practice
- Advises clients on mitigating and addressing cyber risks, developing cybersecurity protection plans, responding to a data breach or misappropriation of trade secrets, conducting confidential cybersecurity investigations, responding to regulatory investigations, and coordinating with law enforcement on cybercrime issues.
- Experience handling complex and novel cyber investigations and high-profile cases
  - At DOJ, prosecuted and investigated nearly every type of international and domestic computer intrusion, cybercrime, economic espionage, and criminal intellectual property cases.
  - Served as the National Coordinator for the Computer Hacking and Intellectual Property (CHIP) Program in the DOJ's Criminal Division, and as a cybercrime prosecutor in Silicon Valley, in addition to other DOJ leadership positions.

# Jeffrey S. Raskin



**Jeffrey S. Raskin**

San Francisco

+1.415.442.1219

[jeffrey.raskin@morganlewis.com](mailto:jeffrey.raskin@morganlewis.com)

- Jeffrey is the head of Morgan Lewis’s Insurance Recovery Practice in the San Francisco office. He advises clients in litigation, mediation, and arbitration around insurance coverage matters, and intellectual property, commercial, real estate, and environmental disputes. Head of Morgan Lewis’s Insurance Recovery Practice in the San Francisco office, Jeffrey counsels clients seeking recovery for catastrophic losses in securities, environmental, asbestos, silica, toxic tort, product liability, intellectual property, and employment practices cases.
- Jeffrey has written on a variety of topics about insurance, as well as discovery of email in civil litigation. His most recent writings discuss the emerging fields of “cyber” insurance, with a particular focus on the types of first- and third-party coverages available to companies to protect themselves against the financial consequences resulting from various types of data breaches.

**Morgan Lewis**

## Our Global Reach

Africa

Asia Pacific

Europe

Latin America

Middle East

North America

## Our Locations

Abu Dhabi

Almaty

Beijing\*

Boston

Brussels

Century City

Chicago

Dallas

Dubai

Frankfurt

Hartford

Hong Kong\*

Houston

London

Los Angeles

Miami

Moscow

New York

Nur-Sultan

Orange County

Paris

Philadelphia

Pittsburgh

Princeton

San Francisco

Shanghai\*

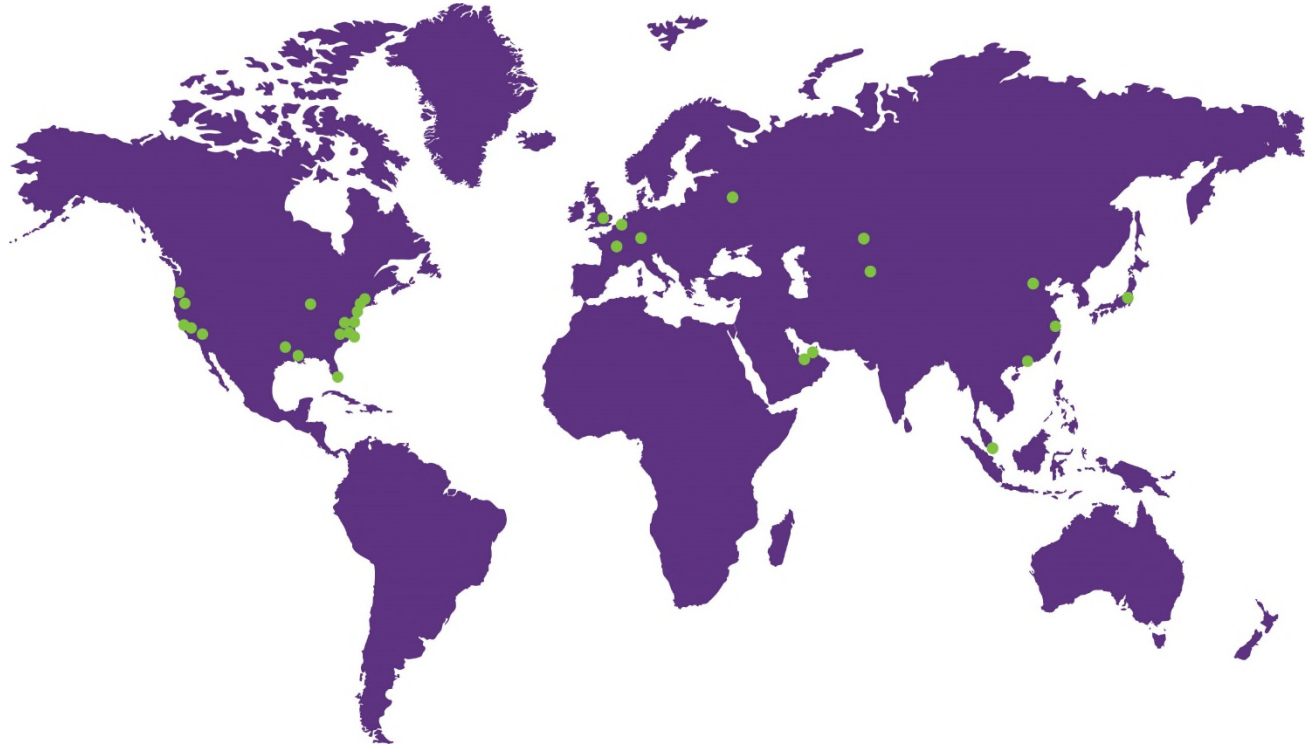
Silicon Valley

Singapore\*

Tokyo

Washington, DC

Wilmington



# Morgan Lewis

\*Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan Lewis operates through Morgan, Lewis & Bockius, which is a separate Hong Kong general partnership registered with The Law Society of Hong Kong as a registered foreign law firm operating in Association with Luk & Partners. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.

# THANK YOU

© 2020 Morgan, Lewis & Bockius LLP  
© 2020 Morgan Lewis Stamford LLC  
© 2020 Morgan, Lewis & Bockius UK LLP

Morgan, Lewis & Bockius UK LLP is a limited liability partnership registered in England and Wales under number OC378797 and is a law firm authorised and regulated by the Solicitors Regulation Authority. The SRA authorisation number is 615176.

Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan Lewis operates through Morgan, Lewis & Bockius, which is a separate Hong Kong general partnership registered with The Law Society of Hong Kong as a registered foreign law firm operating in Association with Luk & Partners. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.

This material is provided for your convenience and does not constitute legal advice or create an attorney-client relationship. Prior results do not guarantee similar outcomes. Attorney Advertising.

**Morgan Lewis**