



Financial Services & Products ADVISORY ■

DECEMBER 4, 2020

State Regulators Enact Guidance Allowing Remote Work for Licensees Even After COVID-19

by [Lisa Lanham](#) and [David McGee](#)

As the COVID-19 pandemic continues to persist across the nation, some state regulators have begun to consider, or have adopted, measures to allow employees of licensed entities to work from home, both during the pandemic and permanently thereafter.

On October 11, 2020, the Washington Department of Licensing filed [emergency rules](#), effective October 20, 2020, that allow employees of licensed collection agencies to work from home. The emergency rules both amend a current section of the Washington Revised Code and add a new section, which details operational requirements to allow employees of licensed collection agencies to work from home.

The emergency rules amend Wash. Admin. Code § 308-29-010 to add a definition of “remote work,” which is defined as “the practice of working from home or other alternative location through the use of technology which allows the employee to access normal work material (email, telephone, electronic documents, etc.)” on either a scheduled or “ad hoc basis.” Further, the emergency rules clarify that an employee of a licensee working from home is not deemed a collection agency or a branch office for purposes of licensure while engaged in remote work.

The emergency rules also add a new section to the Washington Administrative Code, § 308-29-085, which details requirements a collection agency must follow to allow an employee to engage in remote work. A collection agency must ensure the following requirements are met:

1. If the collection agency allows remote working, a record of which employees have been assigned to working remotely must be maintained and kept current.
2. Remote working employees must comply with all applicable laws and regulations as outlined in chapters 19.16 and 18.235 RCW and chapter 308-29 WAC.
3. Collection agencies and their employees must have a written IT security policy that outlines the security protocols in place safeguarding the company and customer data, information and electronic and physical records, to protect them against unauthorized or accidental access, use, modification,

This alert is published by Alston & Bird LLP to provide a summary of significant developments to our clients and friends. It is intended to be informational and does not constitute legal advice regarding any specific situation. This material may also be considered attorney advertising under court rules of certain jurisdictions.

duplication, destruction or disclosure. Physical records must be stored and maintained at the business location and may not be stored at the remote working location.

4. The IT security policy requirements must include provisions for the remote working employee to access the collection agency's secure system from any out-of-office device the employee uses through the use of a virtual private network "VPN" or other system that requires passwords, frequent password changes, identification authentication authorization, multifactor authentication, data encryption, and/or account lockout implementation. The collection agency is responsible to maintain any updates or other requirements in order to keep information and devices secure.
5. Collection agencies must record and monitor all calls initiated or received by their employees while employees are working remotely and must maintain copies of these recordings and make them available for inspection upon request.
6. Neither the employee nor the collection agency shall conduct any activity that would indicate or tend to indicate the employee is performing collection agency business from an unlicensed location. Such acts include, but are not limited to:
 - (a) Advertising in any form, including business cards and social media, an unlicensed address or personal telephone or facsimile number associated to the unlicensed location;
 - (b) Meeting consumers at, or having consumers come, to an unlicensed location;
 - (c) Holding out in any manner, directly or indirectly, by the employee or collection agency, an address that would suggest or convey to a consumer that the location is a licensed collection agency or branch, including receiving official mail directly, or permanently storing books or records at the remote location.

The Department of Licensing intends to release a permanent rule by the end of the year, with a notice and comment period, that will permanently allow employees of Washington licensed collection agencies to work from home as long as the collection agency follows all requirements to allow employees to engage in remote work contained in the emergency rules.

Similar to the Washington Department of Licensing, the New Mexico Regulation and Licensing Department, Financial Institutions Division, released new [guidance](#) on working-from-home arrangements on November 23, 2020 that is permanent unless withdrawn. The Financial Institutions Division authorized remote work for employees of all entities licensed, registered, or certified with the Financial Institutions Division, unless otherwise prohibited by law, as long as the licensed financial institution adheres to the following guidelines:

1. The company shall not advertise, promote, or otherwise publicly hold out the unlicensed location as a place of business;
2. The market area for the business shall be based upon licensed locations, not the physical location of the employees who are working remotely;
3. Only activities that can be safely accomplished (in full compliance with all provisions of this guidance) while working remotely will be performed;
4. In-person customer interactions will not be conducted at the remote location;

5. The company must have established security protocols in place for employees to securely access systems through a virtual private network (VPN) or other secure system(s);
6. Companies and employees must exercise due diligence in the safeguarding of company and customer data, information, and records, whether in paper or electronic format, and to protect them against unauthorized or accidental access, use, modification, duplication, destruction, or disclosure;
7. Sensitive customer information will be protected consistent with strict cybersecurity protocols and best practices;
8. Risk-based monitoring and oversight processes will be followed; and
9. Information regarding the specific activities conducted via telework/remote work will be maintained and available upon request.

As regulators across the country continue to grapple with COVID-19, we expect that other regulators may follow Washington's and New Mexico's examples and promulgate rules and guidance for working from home even after the COVID-19 pandemic has ceased. We will continue to monitor state regulators for further developments into allowing employees of licensed entities to work from home.

You can subscribe to future *Financial Services & Products* advisories and other Alston & Bird publications by completing our [publications subscription form](#).

If you have any questions or would like additional information, please contact your Alston & Bird attorney or any member of our [Financial Services & Products Group](#).

Nanci Weissgold
202.239.3189
nanci.weissgold@alston.com

Morey Barnes Yost
202.239.3674
morey.barnesyost@alston.com

Anoush Garakani
202.239.3091
anoush.garakani@alston.com

Stephen Ornstein
202.239.3844
stephen.ornstein@alston.com

Ross Speier
404.881.7432
ross.speier@alston.com

David McGee
202.239.3795
david.mcgee@alston.com

Brian Johnson
202.239.3271
brian.johnson@alston.com

Rinaldo Martinez
202.239.3205
rinaldo.martinez@alston.com

John C. Redding
213.576.1133
john.redding@alston.com

Lisa Lanham
212.210.9527
lisa.lanham@alston.com

ALSTON & BIRD

WWW.ALSTON.COM

© ALSTON & BIRD LLP 2020

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
 BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86.10.85927500
 BRUSSELS: Level 20 Bastion Tower ■ Place du Champ de Mars ■ B-1050 Brussels, BE ■ +32 2 550 3700 ■ Fax: +32 2 550 3719
 CHARLOTTE: Bank of America Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
 DALLAS: Chase Tower ■ 2200 Ross Avenue ■ Suite 2300 ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
 FORT WORTH: 3700 Hulen Street ■ Building 3 ■ Suite 150 ■ Fort Worth, Texas, USA, 76107 ■ 214.922.3400 ■ Fax: 214.922.3899
 LONDON: 5th Floor ■ Octagon Point, St. Paul's ■ 5 Cheapside ■ London, EC2V 6AA, UK ■ +44.0.20.3823.2225
 LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
 NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
 RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ 919.862.2200 ■ Fax: 919.862.2260
 SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ 415.243.1000 ■ Fax: 415.243.1001
 SILICON VALLEY: 1950 University Avenue ■ Suite 430 ■ East Palo Alto, California, USA 94303 ■ 650.838.2000 ■ Fax: 650.838.2001
 WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333