

KU: Submitted to Julie K 9-28-20

AMENDATORY SECTION (Amending WSR 01-11-132, filed 5/22/01, effective 6/22/01)

WAC 308-29-010 Definitions. (1) Words and terms used in these rules have the same meaning as each has under chapter 19.16 RCW unless otherwise clearly provided in these rules, or the context in which they are used in these rules clearly indicates that they be given some other meaning.

(2) "Remote work" is the practice of ~~working~~ conducting activity meeting the criteria of a collection agency or out-of-state collection agency as defined in RCW 19.16.100, 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.). Remote work may be scheduled or on an ad hoc basis.

(3) "Branch office" is any location physically separated from the principal place of business of a licensee where the licensee conducts any activity meeting the criteria of a collection agency or out-of-state collection agency as defined in RCW 19.16.100.

Commented [KU1]: As with the definition of branch office in sub-(3), remote working rules should apply only to work that qualifies as "collection agency" activity.

~~((3))~~ An employee of a licensee shall not be deemed a "collection agency" or a "branch office" as defined in RCW 19.16.100 (5)(a) and the employee need not have a license to perform collection activities on behalf of the collection agency, whether working in the collection agency office, or working remotely.

(4) "Repossession services" conducted by any person shall not be deemed a collection agency as defined in RCW 19.16.100, unless such person is repossessing or is attempting to repossess property for a third party and is authorized to accept cash or any other thing of value from the debtor in lieu of actual repossession.

~~((4))~~ (5) "Managing employee" is an individual who has the general power to exercise judgment and discretion in acting on behalf of the licensee on an overall or partial basis and who does not act in an inferior capacity under close supervision or direction of a superior authority (as distinguished from a nonmanaging employee who is told what to do and has no discretion about what he or she can and cannot do and who is responsible to an immediate superior).

[Statutory Authority: [RCW 19.16.410]. WSR 01-11-132, § 308-29-010, filed 5/22/01, effective 6/22/01; Order PL-123, § 308-29-010, filed 5/17/72.]

NEW SECTION

WAC 308-29-085 Remote work requirements. Collection agencies that allow remote working must ensure that 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 ("[Covered Data](#)"), to protect them against unauthorized or accidental access, use, modification, 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. The IT security policy shall include, but not be limited to, measures taken to ensure:

- (a) The safe and secure storage of physical and electronic Covered Data;
- (b) Computers and other electronic devices that have access to Protected Data contain reasonable security measures such as updated antivirus software and firewalls;
- (c) Covered Data that is transferred to a remote worker is transferred securely through the use of encryption or other secure transmission sources;
- (d) An action plan has been developed and communicated with relevant employees on how to handle a data breach arising from remote access devices in accordance with applicable laws, which shall include any required disclosures of such breach;

(e) A disaster recovery plan has been developed and communicated with relevant employees on how to respond to emergencies (e.g. fire, natural disaster, etc.) that have the potential to impact the use and storage of Covered Data; and

(f) The secure and timely disposal of Covered Data as required by applicable laws and contractual requirements.

(g) An annual internal or external risk assessment is performed on the collection agency's protection of Covered Data from reasonably foreseeable internal or external risks. Based on the results of the annual risk assessment, the collection agency shall make adjustments to its data security policy if warranted.

(5) Collection agencies must ~~record and have the ability to~~ monitor all calls with debtors initiated or received by their nonmanaging employees while employees are working remotely and a policy for monitoring or reviewing calls~~must maintain copies of these recordings and make them available for inspection upon request.~~

Commented [KU2]: There is no current requirement of recording calls in a physical office. Recording calls as an added compliance tool addresses collector behavior in general; it is not specific to remote-collector behavior. The hallmark of an office environment is the ability to monitor collectors for compliance, and that's what should be required in a remote environment.

(6) All calls must comply with RCW19.16.250 (13)(c), (18), and (19).

(7) Neither the employee nor the collection agency shall represent to debtors that ~~conduct any activity that would indicate or tend to indicate~~ the employee is performing collection agency business

Commented [KU3]: in some instances we will have to represent that the employee is working remotely, like in the record required under sub-(1). Presumably we will have to furnish the record to the CAB if requested, which would then be a violation of sub-(6) as the WAC is originally written. Another example would be advising clients that we work remotely—that would be a violation.

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 employee's home ~~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.

It shall not be considered a violation of this subsection (7) if, in response to an inquiry about the remote worker's location, a remote worker responds that the worker is working remotely or working from home, or words to that effect.

[]

Commented [KU4]: Prohibiting meeting at an "unlicensed location" is a problem. E.g., the courthouse becomes a remote work location if you access the debtor's account via VPN; so in-house attys could not conduct court hearings. Or an agreed repo of a car—how would you do that if every place is a remote work location? Or a non-consensual repo?