consumer relations consortium
connect | collaborate | advance

COMMENT TO NOTICE OF PROPOSED RULEMAKING
Re: Definition of "Branch office"

The Consumer Relations Consortium (CRC) is submitting its comment to Notice of Proposed Rule Making (NPRM), released by the California Department of Financial Protection and Innovation (DFPI) on April 23, 2021. The entirety of this comment pertains to the definition of "Branch office" as set forth in Article I, §1850(c) of the proposed rules.

Article I, §1850(c) defines "Branch office" as "a location other than the applicant's principal place of business identified in a license application or an amended application." A plain reading of this definition indicates that California debt collection workers would not be able to work remotely from home without a Branch office license. Instead, licensees would be required to apply for a Branch office license for each home location of the licensee's employees, thus in the event of another health crisis, delaying the licensee's ability to protect employees and inundating the DFPI with Branch office license requests.

Further, although a health crisis hastened the process of having call center employees work remotely, this model now appears to be good business, providing benefits to call center employees and consumers. For example, employees report greater job satisfaction by reducing their hours commuting to/from work, allowing employees to spend more time with their families, and reducing workplace distractions. Additionally, allowing a work from home model helps consumers by enabling licensees to retain quality workers and hire the best people instead of those that are just within the immediate geographic proximity to a call center.

To meet the needs of a modern workforce and provide flexibility during any future public health crisis, the CRC recommends that the definition of "Branch office" be updated and/or clarified to explicitly exempt a licensee's employee's home so long as specific criteria are met. The state of Maryland recently took this approach, and the American Financial Services Association has issued guidance on the topic, each of which may be helpful examples for the California DFPI.

Maryland's Work From Home Regulations:

Armed with the evidence of the successful work from home initiatives shown throughout the Covid-19 health crisis, in an effort to modernize its workforce, Maryland enacted a rule allowing a licensee's employees to work from home so long as specific operational and security requirements are met. Although published as an emergency regulation, the Maryland Commissioner of Financial Regulation has proposed filing the regulation on a final basis in substantially the same form. It should be noted that the text of the Maryland rule is not tied to a public health crisis. Instead, a licensee's ability to allow its employees to work from home will depend upon the licensee's ability to meet the rule's operational requirements and security criteria.

The Maryland Rule is attached to this comment, but the highlights of the regulation include the following:

- Employee Location requirements and prohibitions (Section D), including but not limited to the following:
    - The location cannot be:
        - owned or leased by the licensee or its affiliates;
        - included as temporary office space or held out to the general public for use;
        - a place where the employee will receive or dispense cash or negotiable instruments;
        - used for receipt of the licensee's business mail or the storage of books or records of the licensee's business.
    - The location must be:
        - secure for the appropriate protection of personal information and have proper technology safeguards; and
        - used by a single employee.

- A licensee must adhere to specific Security Standards (Section E), including but not limited to:
    - development, implementation, and maintenance of a security program meeting particular criteria, which is part of the licensee's data and cybersecurity program;
    - creating a monitoring process, which must meet specific requirements;
    - completing a comprehensive remote access and security risk assessment;
    - performing periodic testing and monitoring of the security program, which must include specific requirements.

- A licensee must adhere to specific Employee Supervision requirements (Section F), including but not limited to:
    - Reasonably and adequately supervising employees at all times;
    - maintaining written records regarding working locations and retain those records for two years.

American Financial Services Association White Paper

The COVID-19 pandemic caused many State regulators of financial services companies to seek guidance on allowing the employees of regulated entities to work safely from home while also ensuring stringent protection of sensitive consumer data. The American Financial Services Association (AFSA) created a widely-regarded white paper setting forth standardized data security and similar requirements allowing employees of licensed financial institutions to perform their jobs remotely while adhering to current regulatory requirements. Like the Maryland regulations, the attached guidance also includes security standards, location requirements, and training protocols.

consumer relations consortium
connect | collaborate | advance

Allowing Work From Home is Good for Both the Industry and Consumers

In 2020, faced with the public health crisis of Covid-19, debt collectors were for the first time permitted to work from home. Debt collectors quickly established controls and security protocols that allowed collectors to perform their job duties while adhering to established regulatory requirements. It has been over a year since collectors began working from home, and none of the doomsday predictions have come to fruition. Instead, the ability to offer a licensee's employees the ability to work from home has important positive implications, including the following:

- Criteria for agent selection will be more those best suited to collections, not just those who live within commuting distance from the office. The ability to allow agents to work from home means that collection agencies can recruit nationwide and can hire those best suited to the job, not just those who live in the right place, including those in areas with high unemployment.

- It will increase employment opportunities for those who are unable to travel, or cannot leave the home, or can do so only on a limited basis. In addition, many who might be best suited to collections but are either physically unable to travel or are restricted due to child or elder care or similar issues will have increased opportunities for employment due to this recruiting flexibility.

- Higher retention is better for all, especially consumers - Collections is historically a high-turnover industry; most collection call centers experience annual turnover in the range of 100%. Because of the regulatory complexity and overall stress associated with collections, clients, agencies, and consumers alike would benefit significantly from happier, more tenured agents who are better suited to their role.

Addressing This Now Will Prevent Emergency Rulemaking

In 2020, to protect the health of their citizens, states were tasked with creating emergency regulations to allow employees of licensees to work outside the licensee's business offices. State regulatory bodies were forced to quickly come up with ways to meet the health needs of their citizens yet continue to protect consumers. In addition to the practical considerations for a modern work environment discussed above, at the current juncture, there is an opportunity to give thoughtful contemplation to these issues and draft regulations that protect consumers and allow a state to protect its citizens from a future health crisis. Detailing the circumstances in which an employee can work from home will provide clarity to licensees and prevent the California DFPI from being forced to address this issue via emergency order should we suffer a future pandemic or other public health crisis.

MARYLAND COMMISSIONER OF FINANCIAL REGULATION

INDUSTRY ADVISORY REGULATORY NOTICE

January 22, 2021

Emergency Regulations for State-Regulated Entities: Permitting Remote Work for Employees at Certain Locations

The Commissioner of Financial Regulation has promulgated, under emergency status, new Regulation .08 under COMAR 09.03.02 – General Regulations pertaining to certain licensees regulated by the Office of the Commissioner of Financial Regulation ("OCFR"). Specifically, the regulation will immediately permit remote work for employees working at certain locations if the remote work arrangement complies with certain standards and conditions.

This Regulation balances appropriate consumer protections with a recognition of today's workforce needs and the progression towards more consistent remote work and work location flexibility. Currently, Maryland has regulations in place regarding remote work for Mortgage Loan Originators that provide flexibility for those employees to originate loans outside the Office based on compliance with certain standards and conditions. This Regulation extends similar flexibility to other licensed workers and reflects changes in practices and procedures that have been facilitated by advances in communication and interactive technologies, as well as the mandatory protocols that have been put in place pursuant to the COVID-19 pandemic.

See Exhibit A (below) for new Regulation .08 as it will be published in the Maryland Register on January 29, 2021. As the emergency status is valid for only 6 months, the Commissioner will also be proposing, after seeking public comments, these regulations on a final basis, in substantially the same form as the emergency ones.

If you have any questions, you may contact Jedd Bellman, Assistant Commissioner for Non-Depository Supervision, by e-mail at jedd.bellman@maryland.gov, or by telephone at (410) 230-6390.

The Office of the Commissioner of Financial Regulation, a division of the Maryland Department of Labor, is Maryland's banking and financial services regulatory agency. For more information, please visit our website at www.labor.maryland.gov/finance.

EXHIBIT “A”

.08 Remote Work for Employees of Licensees.

A. Scope.

(1) This regulation governs the conduct of any employee operating from a location other than that which appears on the employer’s license or licenses.

(2) Notwithstanding §A(1) of this regulation, this regulation does not apply to the conduct of an employee if:

(a) The employer is licensed under Financial Institutions Article, Title 11, Subtitle 5, Annotated Code of Maryland;

(b) The employee is licensed under Financial Institutions Article, Title 11, Subtitle 6, Annotated Code of Maryland; and

(c) The employee is taking a loan application or offering or negotiating the terms of a loan in compliance with COMAR 09.03.09.07.

(3) Nothing contained in this regulation shall be deemed to prohibit an employee of a licensee from conducting any business for which a license is required at a location other than the locations set forth on the employer’s license or licenses if applicable law or regulation does not limit that conduct to the location shown on the license.

(4) A licensee may not use this regulation to evade the requirements of any applicable law or regulation.

B. Definitions.

(1) Terms Defined.

(2) In this regulation, the following terms have the meanings indicated.

(a) “Affiliate” means a person that directly or indirectly, through one or more intermediaries, controls, is controlled by, or is under common control with another person.

(b) “Authorized delegate” has the meaning stated in Financial Institutions Article, §12-401, Annotated Code of Maryland.

(c) “Board” has the meaning stated in Business Regulation Article, §7-101, Annotated Code of Maryland.

(d) “Breach of the security of a system” has the meaning stated in Commercial Law Article, §14-3504, Annotated Code of Maryland.

(e) "Consumer" means an individual who resides in Maryland.

(f) “Employee” means an employee of a licensee who is not an independent contractor or an authorized delegate.

(g) “Independent contractor” has the meaning stated in Financial Institutions Article, §11-601, Annotated Code of Maryland.

(h) “License” means any of the following:

(a) A license issued by the Board under Business Regulation Article, Title 7, Annotated Code of Maryland, to do business as a collection agency;

(b) A license issued by the Commissioner under Commercial Law Article, Title 14, Subtitle 19, Annotated Code of Maryland, to engage in the business of a credit services business;

(c) A license issued by the Commissioner under Financial Institutions Article, Title 11, Subtitle 2, Annotated Code of Maryland, to make loans under the Maryland Consumer Loan Law;

(d) A license issued by the Commissioner under Financial Institutions Article, Title 11, Subtitle 3, Annotated Code of Maryland, to make installment loans;

(e) A license issued by the Commissioner under Financial Institutions Article, Title 11, Subtitle 4, Annotated Code of Maryland, to engage in business as a sales finance company;

(f) A license issued by the Commissioner under Financial Institutions Article, Title 11, Subtitle 5, Annotated Code of Maryland, to engage in business as a mortgage lender;

(g) A license issued by the Commissioner under Financial Institutions Article, Title 12, Subtitle 1, Annotated Code of Maryland, to provide check cashing services;

(h) A license issued by the Commissioner under Financial Institutions Article, Title 12, Subtitle 4, Annotated Code of Maryland, to engage in the business of money transmission; or

(i) A license issued by the Commissioner under Financial Institutions Article, Title 12, Subtitle 9, Annotated Code of Maryland, to provide debt management services.

(i) "Licensee" means a person issued a license or licenses for the purpose of conducting the business for which the license or licenses are issued.

(j) "Personal information" has the meaning stated in Commercial Law Article, §14-3501, Annotated Code of Maryland.

(k) "Records" has the meaning stated in Commercial Law Article, §14-3501, Annotated Code of Maryland.

(l) "Security program" means a written program created by or on behalf of a licensee for the purpose of allowing the licensee's employees to safely and securely access the licensee's information technology systems, other systems, and data from a location authorized by this section.

C. Certain Remote Work Permitted. An employee of a licensee may work remotely and is not considered conducting business for which a license is required at a location other than the address that appears on the license or licenses of that licensee if the conditions set forth in this regulation are met.

D. Locations. The location from which the employee is working:

(1) May not be owned or leased by the licensee or an affiliate of a licensee, or for the benefit of the licensee or an affiliate of the licensee;

(2) May not be a location that offers temporary office space unless the employee is using the location on a temporary basis due to the unavailability of the employee's regular work location;

(3) May not be held out to the public by use of signage, advertisement, or other means, as a location at which the licensee conducts business for which a license is required;

(4) May not provide work space, telephone service, or internet service maintained in the name of the licensee or an affiliate and that is not intended primarily for the purpose of conducting business for which a license is required;

(5) May not be a location where the employee will meet in person with nonemployees in connection with the business for which a license is required;

(6) May not be a location that will receive or dispense cash, negotiable instruments, or other monetary value in connection with the business for which a license is required, other than compensation paid to the employee by the licensee;

(7) May not be used for the receipt of mail relating to business for which a license is required;

(8) May not be used for storage of books or records, in any form, relating to business for which a license is required unless:

(a) The records were produced or used in the normal course of employment by the employee working at that location and the licensee maintains and administers procedures for the employee to promptly and securely transmit those records to its location for the storage of books and records; or

(b) The licensee is permitted by applicable law or regulation to store the books or records of the licensee at that location;

(9) Shall provide a workspace that is secure, provide for appropriate protection of personal information as required under applicable law, and have the appropriate technological security measures and physical safeguards in place to protect personal information;

(10) Shall be a location used only by a single employee unless:

(a) Other employees using the location maintain a common household with each other; or

(b) The location is used for a period not exceeding 2 weeks every calendar quarter to facilitate business or nonbusiness travel;

(11) May not be used to conduct a specific act that applicable law or regulation requires be conducted only at specified locations; and

(12) Shall be authorized by the licensee as a location from which the employee may work.

E. Security Standards.

(1) A licensee that allows any employee to work at a location authorized by this section shall develop, implement, and maintain a security program that is consistent with all applicable laws and regulations, meets or exceed standards of the industry in which the licensee conducts its business, addresses known vulnerabilities, and is commensurate with the licensee’s size and complexity.

(2) The licensee’s security program may be part of the licensee’s comprehensive data and cyber security program.

(3) A licensee’s security program shall consider the following objectives:

(a) Allowing employees working at locations authorized by this section to access the licensee’s information technology system, other systems, and data needed to perform the employee’s job functions in a safe and secure manner;

(b) Ensuring the security and confidentiality of the licensee’s data containing personal information and other sensitive information;

(c) Protecting the licensee’s information technology systems, other systems, and data against security breaches and unauthorized access, including unauthorized access by employees;

(d) Identifying the types of devices an employee may use to access the licensee’s information technology systems, other systems, and data, and protecting those devices from security breaches and unauthorized access; and

(e) Providing training and support of the licensee’s employees necessary to ensure compliance with the security program and establishing appropriate sanctions for failures to comply.

(4) A licensee shall have an established governance process in place to control and monitor the security program which shall include, as appropriate for the size and complexity of the licensee and its information technology systems, other systems, and data:

(a) The approval of the security program by the board of directors, ownership, or most senior level of management; and

(b) A management structure that encompasses:

(i) Assigning responsibilities and authorities for ensuring adherence to the security program;

(ii) Documenting accountability for functions to ensure compliance with the security program; and

(iii) Reporting to the board of directors, ownership, or most senior level of management, no less than annually, regarding the effectiveness of the security program.

(5) In connection with the security program, a licensee shall complete a comprehensive remote access and data security risk assessment, including:

(a) Identification and assessment of risks and vulnerabilities created by allowing employees to work at locations authorized by this section and to access the licensee’s information technology systems, other systems, and data from such locations; and

(b) Identification of the devices, data, information technology system, and other systems that need to be protected.

(6) A licensee shall perform periodic testing and monitoring of the security program as appropriate for the size and complexity of the licensee's information technology and other systems, including:

(a) Evaluating the effectiveness of the security program;

(b) Evaluating employee compliance with the security program;

(c) Taking corrective action to address any significant deficiencies identified during the course of licensee's evaluation of the effectiveness of the security program;

(d) Monitoring of external sources for new vulnerabilities;

(e) Updating, as appropriate, its remote access and data security risk assessment; and

(f) Developing and implementing additional control frame works for any new or changed threats or risks identified by the licensee.

(7) A licensee shall review the security program at least annually and make changes necessary to achieve the objectives of the security program.

(8) A licensee that adequately demonstrates compliance with standards issued by the National Institute of Standards and Technology, United States Department of Commerce, relating to remote workers and remote access, as such may be revised from time to time, shall be deemed to be in compliance with this section.

F. Supervision of Employees.

(1) A licensee shall at all times reasonably and adequately supervise the work-related activities of each employee working at a location authorized by this section.

(2) If the Commissioner determines that the licensee does not provide reasonable and adequate supervision of the employee, after written notice from the Commissioner, and within 5 business days of receiving such notice, the licensee will terminate the employee's eligibility to work at a location provided for under this regulation.

(3) A licensee shall maintain and update, as appropriate, written records with respect to an employee working from locations provided for in this section, including the initial authorization to work from any such location, any updated authorization, and information regarding the location and any due diligence the license has undertaken to ensure compliance with this regulation.

(4) The licensee shall retain the records required by §F(3) of this regulation for the greater of 2 years from the date the employee ceases using such location in connection with the business for which a license is required or any retention period required by applicable law or regulation.

G. Identification of Licensee. The employee may not, in connection with the business for which a license is required, conceal, misrepresent or otherwise mislead any person with respect to the identity of the licensee.

H. Principal Executive Office. The licensee shall, at a minimum, maintain a principal executive office.

I. Security Breach. If a breach of the security of a system occurs at a location provided for in this regulation, the following steps shall be taken:

(1) Upon learning of the breach of the security of a system, the employee shall immediately notify the licensee;

(2) Upon learning of the breach of the security of a system, the licensee shall within 72 hours notify the Commissioner and make any other notifications that may be required under applicable law or regulation;

(3) The licensee shall investigate the breach of the security of a system and document its findings, including the remedial steps, if any, that have been undertaken by the licensee to remediate any harm to consumers and to update policies, procedures, and processes as a result of the findings; and

(4) If requested by the Commissioner, the licensee shall provide a copy of the documentation of the investigation required in this section.

ANTONIO P. SALAZAR
Commissioner of Financial Regulation

WORK FROM HOME

- **Advancement driven by necessity**: The COVID-19 pandemic has necessitated technology-enabled remote working. Though many companies invested in VPNs and other advanced technology before 2020, the pandemic pushed a cultural shift forward years or arguably even decades. AFSA members have demonstrated—out of necessity—that nearly all critical operational functions for many financial service business models can take place through remote working.

- **Paradigm shift is twofold:** The investment in technology and procedures have rapidly evolved on what CAN be done from home and simultaneously the professions—which office workers and what jobs—have also evolved. Where working from home was previously embraced by some professions, all manner of workers have now had to learn new ways for them to do their jobs from locations other than the commercial workplace.

- **Identical customer experience**: COVID-19 has shown us that working from home works. For business models that support it, and with the right technology and training in place, consumers have the exact same experience with the financial institution employee working from home as in a commercial office. Authorizing remote working merely allows licensed financial services providers to be more flexible in employment practices, while still providing the same secure services to the public.

- **How it works**: In consumer credit, a work from home approach involves employees being permitted to conduct licensable activities from home—including loan servicing, credit decisioning, funding and collections.
    - Employees are not meeting customers in their homes
    - Employees are not keeping records in their homes.
    - Employees are performing the same telephone / internet-based functions they would have performed if they were sitting in the licensed location.
    - Regulatory supervision, oversight, and licensing fees do not change. All records are available to the regulator as mandated by state law.

919 18th Street NW, Washington, DC, 20006 ▲ 202.296.5544 ▲ www.afsaonline.org ▲ @AFSA_DC

- **Supervision**: Employees are supervised as they would be at the licensed location, and the licensee's records are stored at the licensee's premises without compromising the need for strong data protections.

- **Revenue shortfalls**: The industry is receptive to modifying branch licensing fee structures to mitigate the risk of a negative financial effects on states.

- **COVID and the foreseeable future**: Nobody knows how long the pandemic will last, but it's here for the foreseeable future. Employees cannot tell from looking at someone if they are in a high-risk category. Remote work allows businesses to make critical safety accommodations for employees who may be higher risk or who care for higher risk individuals. Permitting licensees to choose remote work is also the best way to ensure the safety of employees and customers alike while maintaining continuity of operations and critical access to credit.

- **Competition**: National companies and other companies with offices in multiple states have a difficult time justifying the health and safety of workers in one state versus another merely on grounds of state decisions. Particularly when (so far, at least) some states with significantly higher transmission rates have significantly lower safety requirements.

- **Benefits:** The benefits of letting financial institutions choose whether to permit remote work are numerous.
    - **Reducing existing commercial real estate costs**, particularly at a time when so much consumer relief is being voluntarily granted. When less money is coming in, costs have to be reduced one way or another.
    - **Not increasing existing commercial real estate costs.** Another side of the commercial real estate coin is the need in some cases to significantly increase spacing or otherwise costly reconfigure commercial real estate to create more space for existing employees. Remote work helps offset potential increased commercial real estate costs.
    - **Safety for employees**. Remote work allows companies to addressing health concerns for all employees, especially those in high-risk health categories and employees with household members in higher risk categories.

919 18th Street NW, Washington, DC, 20006 ▲ 202.296.5544 ▲ www.afsaonline.org ▲ @AFSA_DC

- **Diversity**. While workplace accommodations can and have always been made for differently-abled employees, remote work creates opportunities for individuals who have trouble commuting and geographically diverse employees who can't reasonably travel to a central commercial office on a daily basis. Working from home also enhances existing inclusivity and allows us to create new avenues to attract and retain diverse talent.
- **Employee satisfaction**. Many of our members report increased employee satisfaction with remote work. And happy employees = happy customers.

- **Urgent**: The industry needs flexibility and consistency now as it has a direct impact on who must leave their home work sites and return to commercial facilities, when that will occur, and what site infrastructure changes must be made to safely accommodate personnel.

- **Not appropriate for all business models:** To be clear, AFSA does not advocate working from home unless it's appropriate for the business model. For employees of companies with the right business model, it should be an option without regulatory interference—as long as all state oversight and consumer protection standards are addressed.

- **Mortgage crisis:** There is now advanced, comprehensive oversight technology that did not exist during the mortgage crisis. Consumer complaint tracking by institutions is now robust, and institutions have the ability to track calls and transactions to the individual employee level. Compensation structures have also been overhauled since the mortgage crisis to mitigate the risk of non-compliant behavior.

- **Best practices.** Financial services providers should be able to identify and implement their own home-working protocols and procedures to protect their businesses and employees and keep the wheels of commerce moving. Some standards of remote work are common across our member companies.
  - ✓ In-person customer interactions will not be conducted at the remote location;
  - ✓ Sensitive customer information will be protected consistent with the licensee's existing cybersecurity protocols for on-site operations;
  - ✓ Employees will utilize virtual workspaces and VPNs, where appropriate;
  - ✓ Risk-based monitoring and oversight processes will be followed;
  - ✓ Physical records will not be maintained at the remote location;

919 18th Street NW, Washington, DC, 20006 ▲ 202.296.5544 ▲ www.afsaonline.org ▲ @AFSA_DC

- ✓ information regarding the specific activities conducted via telework will be maintained and available upon request;
- ✓ Conversations about consumers will be kept private, and remote employees will work in an environment conducive and appropriate to that privacy;
- ✓ Regulatory oversight exams will be unhindered by remote work;
- ✓ Quality monitoring will take place just like in the commercial business center;

Ask: It is critical that government embraces widespread remote working as a way to mitigate the economic impact of the pandemic on workers, businesses, and the economy.

1) Regulators should extend Covid work from home waivers for as long as possible, for as many roles as possible, for as many licensees as possible.
2) Regulators should interpret existing statutes to permit permanent work from home for as many licensees as possible.
3) Regulators should support legislative changes where necessary to accommodate remote work.

919 18th Street NW, Washington, DC, 20006 ▲ 202.296.5544 ▲ www.afsaonline.org ▲ @AFSA_DC

AN ACT permitting work from home for state licensees, under certain circumstances.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF [STATE]:

Notwithstanding anything to the contrary under the laws of the state of [STATE], nothing in [this chapter] shall be interpreted to interfere with employees of a state licensee working from home, or another location selected by the employee ("Remote Location"), provided the licensee:

(a) Ensures all in-person customer interactions will not be conducted at the Remote Location, and will not designate the Remote Location to consumers or customers as a business location;
(b) Maintains appropriate safeguards for licensee and consumer data, information, and records, including the use of secure virtual private networks ("VPNs") where appropriate;
(c) Employs appropriate risk-based monitoring and oversight processes of work performed from a Remote Location, and maintains records of the same;
(d) Ensures consumer information and records are not maintained at a Remote Location;
(e) Ensures consumer and licensee information and records remain accessible and available for regulatory oversight and exams;
(f) Provides appropriate employee training to keep all conversations about, and with, consumers conducted from a Remote Location confidential, as if conducted from a commercial location, and to ensure remote employees work in an environment conducive and appropriate to that privacy.