2023 DFS Law Compliance Checklist

The following questions represent the core components necessary for DFS compliance. Please check off as applicable to self-evaluate your practice or organization.

Do you have a designated Chief Information Technology Officer (CISO) or Board of Directors?

- ☐ Yes
- ☐ They have adequate authority and independence to manage risks
- ☐ They have implemented a written cybersecurity program

Have you conducted the required annual Audits/Assessments?

- ☐ Yes
- ☐ Bi-Annual Security Risk Assessment by a Third-Party
- ☐ Yearly DFS Portal Attestation
- ☐ Asset and Device Audit including Assets and Devices for Remote Employees

Do all of your devices utilize Multifactor Authentication?

- ☐ Yes
- ☐ Including remote employees and personal devices able to access work documentation

Have you created remediation plans to address deficiencies for the following?

- ☐ Security Risk Assessment
- ☐ Privacy Assessment
- ☐ Security Standards Audit
- ☐ Asset and Device Audit
- ☐ Physical Site Audit

Do you have a defined process in the event of incidents or breaches?

- ☐ Do you have the ability to track and manage the investigations of all incidents?
- ☐ Are you able to provide the required reporting of minor or meaningful breaches or incidents within 24/72 hours?
- ☐ Do your staff members have the ability to anonymously report an incident?

Have you performed regular data backups?

- ☐ Yes
- ☐ Have you regularly tested your ability to restore systems from your backups?
- ☐ Do the restores work properly?

Do you have Policies and Procedures relevant to the annual DFS Privacy, Security, and Breach Notification Rules?

- ☐ Have all staff members read and legally attested to the Policies and Procedures?
- ☐ Do you have documentation of their legal attestation?
- ☐ Do you have documentation for annual reviews of your Policies and Procedures?

Have all staff members undergone annual DFS Cybersecurity training?

- ☐ Do you have documentation of their training?
- ☐ Are staff responsible for incident response, business continuity, and disaster recovery regularly tested against social engineering and other common hacking techniques?

Have you identified all Business Associates (and Confidentiality Vendors?)

- ☐ Do you have Business Associate Agreements in place with all Business Associates?
- ☐ Have you audited your Business Associates to ensure that they are DFS compliant?
- ☐ Are you tracking and reviewing your Business Associate Agreements annually?
- ☐ Do you have Confidentiality Agreements with those who are not considered Business Associates?

AUDIT TIP: If audited, you must provide all documentation in an eligible format to auditors.

DFS Cybersecurity Compliance can be overwhelming. Work with Motiva to make sure you have everything in place. Contact us at 646-374-1820 or info@motiva.net

motiva NETWORKS