MEMORANDUM

October 26, 2026

To: MSB Industry

Re: Critical PHP Vulnerabilities

The Department of Banking and Consumer Finance (DBCF) is providing notice due to the disclosure of two potential significant vulnerabilities and widespread use of PHP, a programming language used in websites, enterprise applications, and other software.

These vulnerabilities, which are cataloged as CVE-2026-109618 and CVE-2026-109619, pose significant risk to institutions operating PHP-based applications. Customer-facing applications, sensitive financial information, operational continuity, and third-party technology dependencies are potentially at risk. These vulnerabilities may allow unauthenticated attackers to remotely execute malicious code or access sensitive information. These vulnerabilities affect PHP versions dating back to PHP 5.

A patch to address these vulnerabilities, released on October 21, 2026, should be prioritized, with the following recommended actions based on exposure, business criticality, and potential consequences of compromise:

- Identify and prioritize vulnerable assets
- Apply emergency security updates
- Implement temporary compensating controls
- Enhance monitoring and incident response
- Assess third-party and operational dependencies

More information on the PHP vulnerabilities and recommended actions is below:

- CISA Alert: Critical Vulnerabilities in PHP Require Immediate Patching
- NSA Advisory: Critical Patches Recommended for PHP Vulnerabilities
- PHP.net Security Advisory

Please send any questions to Adam Martino at msb@dbcf.ms.gov.

Sincerely,

Rhoshunda G. Kelly

Rhoshunda G. Kelly, Commissioner