

## Business eDeposit Self-Assessment

Landmark Credit Union would like to thank you for taking the time to complete this Business eDeposit Self-Assessment. This document should be used to evaluate the processes your company uses in conjunction with Landmark Credit Union's Business eDeposit service, and ensure that your company's financial information and the information of your customers remain secure. This assessment should be used as an internal tool to help identify potential security concerns, or areas where improvements could be made within your company. If you have any questions regarding the assessment, please contact your business relationship manager at 262-796-4500.

Business Name:

Date:

Completed by:

Yes

No

### AGREEMENTS

Have you reviewed your eDeposit agreement(s) recently?

Are you in compliance with the agreement(s)?

Yes

No

### OPERATIONAL CONTROLS

Is your payment equipment and designated computer physically secure?

Do you have business continuity plan(s) for your payment product(s)?

Is your depository account activity reviewed daily for accuracy?

Yes

No

### BUSINESS OPERATIONS

Do you utilize: anti-virus, anti-spyware, and anti-malware programs?

Do you keep this software updated and install security patches promptly?

Are firewalls in place?

Do you monitor for unauthorized system activity or scan for vulnerabilities?

Does each eDeposit user have a unique user name and password?

Are strong passwords required of all users?

Do users "log off" or lock computers when not in use?

Do you have a computer dedicated for online banking functions?

If No, is web browsing restricted on the computer used?

- Do you use dual control for administrative online banking functions?  
(new users added, new payee accounts added/changed, password changes, disabling of security features, etc.)
- Do you use dual control for external transfer transmissions?  
(ACH transfers, wire transfers, remote deposits, etc.)
- Are security procedures reviewed annually and adjusted?

### STAFF CONTROLS

- Are background checks required on staff involved with payment processing?
- Does staff receive initial and periodic product training?
- Are written procedures maintained on electronic payment products?

Yes      No

### BUSINESS eDEPOSIT

- Do you keep scanned checks physically secure?
- Do you retain scanned checks for the required retention time of 60 Days?
- After the retention timeframe, do you destroy the scanned checks by cross-cut shredding so that they cannot be reconstructed?
- Is your daily deposit limit still set suitably for your business?
- Are scanners maintained as recommended to ensure proper function?  
(e.g., covered when not in use, cleaned regularly)