UNIBANK **Company Name:** **CIF:**

Online Banking Security Best Practices Checklist – Cash Management

UniBank will assist in creating a secure online banking experience driven by a range of security layers.

Computer Security

- ☐ Network / computer firewall installed
- ☐ Dedicated computer for electronic banking (ie, NOT used for email nor web browsing), for primary and backup users only
- ☐ Automated Operating System updates
- ☐ Commercial anti-virus software (not freeware), with automated updates and regular regularly scheduled anti-virus scans
- ☐ Automated updates for third party software such as Microsoft Office, Java, Adobe Reader, Adobe Flash, etc.
- ☐ Limited administration rights on the computer
- ☐ Install Trusteer Rapport malware protection

Administration

- ☐ Dual control (ie, one user creates/edits users, another user approves)
- ☐ Administrators and users with "least privilege" – access to the minimal set of accounts and functions to do their jobs
- ☐ Establish IP Address restrictions (UniBank administers)
- ☐ Establish day / time access restrictions

ACH

- ☐ Dual control (ie, one user creates a transaction, another user approves/transmits
- ☐ Transaction Limits
- ☐ Daily Limits
- ☐ Email alerts, to multiple users (ensure @unibank.com is whitelisted by your company's email admin)

Wires

- ☐ Dual control (ie, one user creates a transaction, another user approves/transmits
- ☐ Transaction Limits
- ☐ Daily Limits
- ☐ Email alerts, to multiple users (ensure @unibank.com is whitelisted by your company's email admin)
- ☐ One-Time Passcode process for transmitting wires

Daily Operations

- ☐ Daily reporting/reconciliation of transactions and account balances
- ☐ Train all users on security, safe computer usage and online banking – examples:
  - Change password every 60-90 days
  - Different passwords for each website
  - Passwords of at least 8 characters
  - Passwords with letters, numbers and special characters
  - NEVER share passwords with anyone!
    ** UniBank staff will not ask for passwords **
  - Do not write password on desk notes
  - Don't click on suspicious email links
  - Don't select "Save My Password" option
- ☐ Train all users on social engineering: hackers gathering information via phone calls, etc, to be used in fraud attempts later

Reviewed

UniBank Rep: _____ Date: _____

Client Rep: _____ _____

Position: _____ Signature: _____