Remote Deposit Now

Quick Reference Guide

TABLE OF CONTENTS

Remote Deposit Now Overview

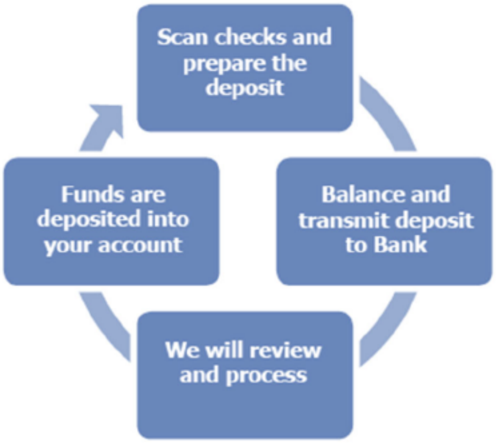
What is Remote Deposit Now?

This quick reference guide was developed to give you an overview of important information you should be aware of as a Remote Deposit Now user. It will assist you with training, compliance and risk associated with using remote deposit technology.

Remote Deposit Now (RDN), also known as Remote Deposit Capture, is the ability to deposit a check into a bank account from a remote location, such as an office or place of business, without having to physically deliver the check to the bank. This is accomplished by scanning a digital image of a check into a computer, then transmitting that image to the bank in an encrypted and safe format.

Flow of deposits made via Remote Deposit Now

You accept check payments from your customers. Using our Remote Deposit Now service and an approved scanner, you can scan and submit those checks securely over the Internet to us. We pick up your Remote Deposit Now and process the checks accordingly.


Scan checks and prepare the deposit
Balance and transmit deposit to Bank
We will review and process
Funds are deposited into your account

Correcting and Balancing Deposits

Once you have scanned your items, a list of the items showing a snippet of each check will appear along with a box displaying what the scanner read as the amount of the check. You will need to review these and verify that it balances. Out of balance conditions can occur when the Declared Amount does not match the scanned amount, the number of Items does not match the number of items scanned when the scanner cannot read information from the deposited items, required information is missing, or items are misidentified.

Laws and Regulations

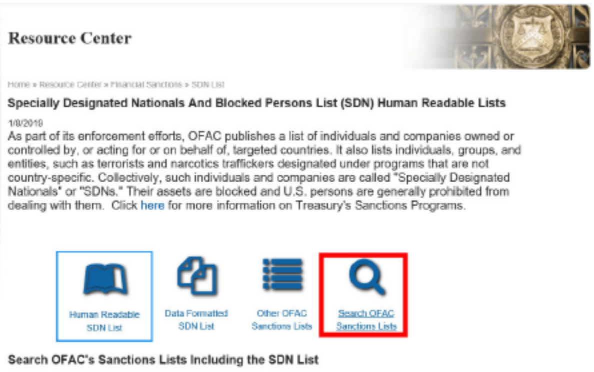
Compliance

Company agrees to abide by all federal and state laws, and rules and regulations applicable to banking transactions, including but not limited to Regulations GG (Unlawful Internet Gambling Enforcement Act.

OFAC Compliance Obligations

Comply with rules of Office of Foreign Asset Control. You should not be acting on behalf of, or transmitting funds to or from, any blocked party subject to OFAC-enforced sanctions. It is your responsibility to check with the OFAC list regularly to determine whether blocked parties have been added to the SDN (Specially Designated Nationals and Blocked Persons) list or whether other modifications to the sanctions programs have taken place.

You may check the OFAC SDN list at: https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx or OFAC's Compliance Hotline may be reached at (800) 540-OFAC.



Resource Center

Home » Resource Center » Financial Sanctions » SDN List

Specially Designated Nationals And Blocked Persons List (SDN) Human Readable Lists

1/8/2019

As part of its enforcement efforts, OFAC publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific. Collectively, such individuals and companies are called "Specially Designated Nationals" or "SDNs." Their assets are blocked and U.S. persons are generally prohibited from dealing with them. Click here for more information on Treasury's Sanctions Programs.

Search OFAC's Sanctions Lists Including the SDN List

Additional Important Information regarding Remote Deposit Now

Federal Holidays - Due to the bank being closed on all federal holidays, no Remote Deposit Now files will be processed on those days, any pending files will be processed on the next business days.

New Year's Day (January 1).
Birthday of Martin Luther King, Jr. (Third Monday in January).
Washington's Birthday (Third Monday in February).
Memorial Day (Last Monday in May).
Juneteenth National Independence Day(June 19)
Independence Day (July 4).
Labor Day (First Monday in September).
Columbus Day (Second Monday in October).
Veterans Day (November 11).
Thanksgiving Day (Fourth Thursday in November).
Christmas Day (December 25).

Daily Cut-Off Times - Deposits submitted through Remote Deposit Now will be posted on the current or next business day depending on when they are received. They will post at the end of the day during nightly processing.

Contingency - If for some reason you are not able to scan your checks using the Remote Deposit Now system, you would then need to bring the checks to your nearest local branch.

Chargeback of Return Items (IRDs) – In the event you are not able to process a deposit through Remote Deposit Now for any reason, the deposit can also be made at any of our branches

Periodic Audit by Bank - As part of our ongoing review, we will contact you periodically concerning your Remote Deposit Now service. This will include a questionnaire and possibly other documentation that will need to be completed, signed and returned to the Bank.

Staff Training and Staff changes

- Inform Digital Banking team of any staff changes (additions and deletions) as soon as possible.
- Please let us know if you wish for us to retrain your staff on how to use the Remote Deposit Now system.

Daily Limits - Any deposit in excess of the agreed upon limit established in the Remote Deposit Now Agreement (Schedule F) must be approved by both the Bank, as well as, the Primary and Secondary Contact before the deposit can be completed.

Duplicate items / double feeds – please contact the Digital Banking Department bank for assistance.

Error Reporting – report errors, if any, no later than 40 days after the date of transaction

Image Quality – We recommend to keep cell phones, printers, and other electronic equipment out of reach of the check scanner as it could result in a poor check image quality and the item could ultimately be returned by the receiving bank.

Online Security

Recommendations include but are not limited to the following:

- Monitor computer operating system vulnerabilities and apply vendor patches and upgrades promptly.
- Run reliable computer virus, malware and spyware detection programs regularly in order to detect and remove computer viruses and other malware.
- Protect your computer by using a ***'firewall".***
- Implement ***appropriate restrictions*** on functions from ***computer workstations and laptops*** that are used to conduct Online Banking and to initiate payments. For example, a

computer used for Online Banking should not be used for general Web browsing, e-mail or for social media.

- Set up Security Alerts (including but not limited to the below listed alerts) and review them carefully to detect unexpected activity, such as alerts in connection with login activity.
- Periodically ***review*** the ***access rights*** of individuals authorized to access your Commercial Online Banking service and have your Company Online Banking Master User make the necessary adjustments. The Company Online Banking Master User and its authorized Sub-User Administrator is solely responsible for designating and administering access to its designated Authorized Sub-Users and for the protection against unauthorized access to the administrative features of the Online Banking system. Please notify the Bank's Digital Banking Department immediately at 866-227-7775 if you change or terminate your Company Online Banking Master User.
- It is imperative to secure and maintain your ***username and password confidentially***.
- ***Clear cache and reboot occasionally*** – to improve system performance.

Additional Security Resources

- For more information, please visit the Security Resource section on our website.
- Create a custom Cybersecurity Planner for your business at http://www.fcc.gov/cyberforsmallbiz.
- Perform a risk assessment on your business to evaluate your existing controls ***(see attached for Business Digital Banking Risk Assessment and Controls Evaluation).***

Frequently Asked Questions

What items can be processed through Remote Deposit Now?

All personal and business U.S. checks and Postal money orders can be processed through Remote Deposit Now. Foreign Checks, food stamps, substitute check images as well as poor image quality checks must be deposited traditionally.

What should we do with the original checks after deposits are made?

Original checks should be retained for 45 days per the Remote Deposit Now Agreement. These items need to be retained in the event that the Federal Reserve requests the original item. Your company will need to set policies for the proper storage and methods (cross cut shredder / shredding service) for securely destroying the original items after the required retention period.

We also recommend downloading the images of your deposit file for future reference and retention purposes. Please contact one of our Digital Banking Specialists for assistance, if applicable.

Is there any maintenance needed for the machine?

Cleaning Cards 5 Count Pack

Please remember to clean your check scanner on a weekly basis to maintain good image quality. We recommend using a Compressed Gas Dust Remover to remove any dust or small particles from the track. Cleaning cards from the machine vendor is also suggested. The customer will be responsible for purchasing additional cleaning cards. These can be purchased at https://paninionlinestore.com/ and can be used on Panini and Canon Scanners. For Canon scanner users, you can go to [Device Cleaning Guide - Canon Solutions America]() for information on cleaning your device. This will ensure that your scanner will continue to operate properly.

How do we prevent checks from being scanned and deposited twice?

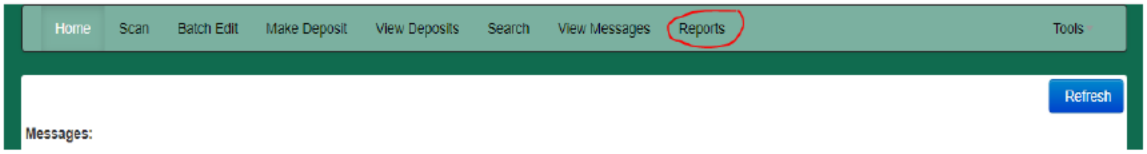
The software has duplicate detection tools that can detect if an item is a possible duplicate. These items will be flagged for review.

Can foreign items be scanned through the service?

Foreign items cannot be scanned thru Remote Deposit Now and have to be deposited manually. These items must be deposited at any of our branches.

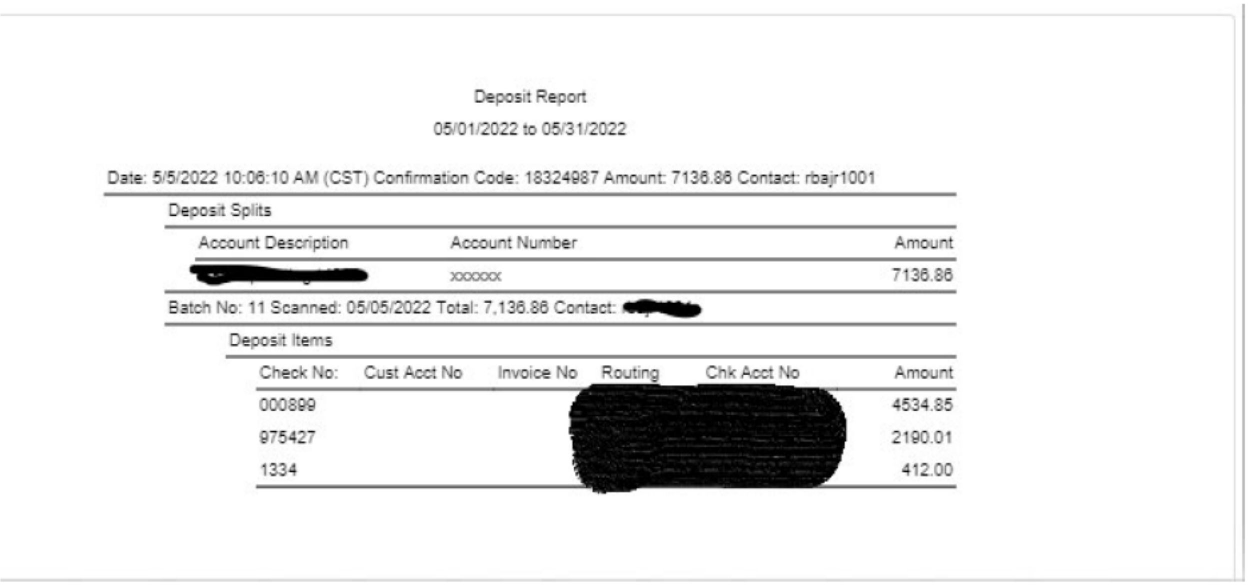
Reports

If you would like to review previous deposits or download a report you can do so by going to the "Reports" tab within "Remote Deposit Now" screen, as shown below.



For the reports, you will just need to select the report you want to download, the date option from the stop and start calendars, and the account you want to run the report for.

Deposit Report- This will list each check included in a deposit and the date of the deposit.



Deposit Report
05/01/2022 to 05/31/2022

Date: 5/5/2022 10:06:10 AM (CST) Confirmation Code: 18324987 Amount: 7136.86 Contact: rbajr1001

Deposit Splits

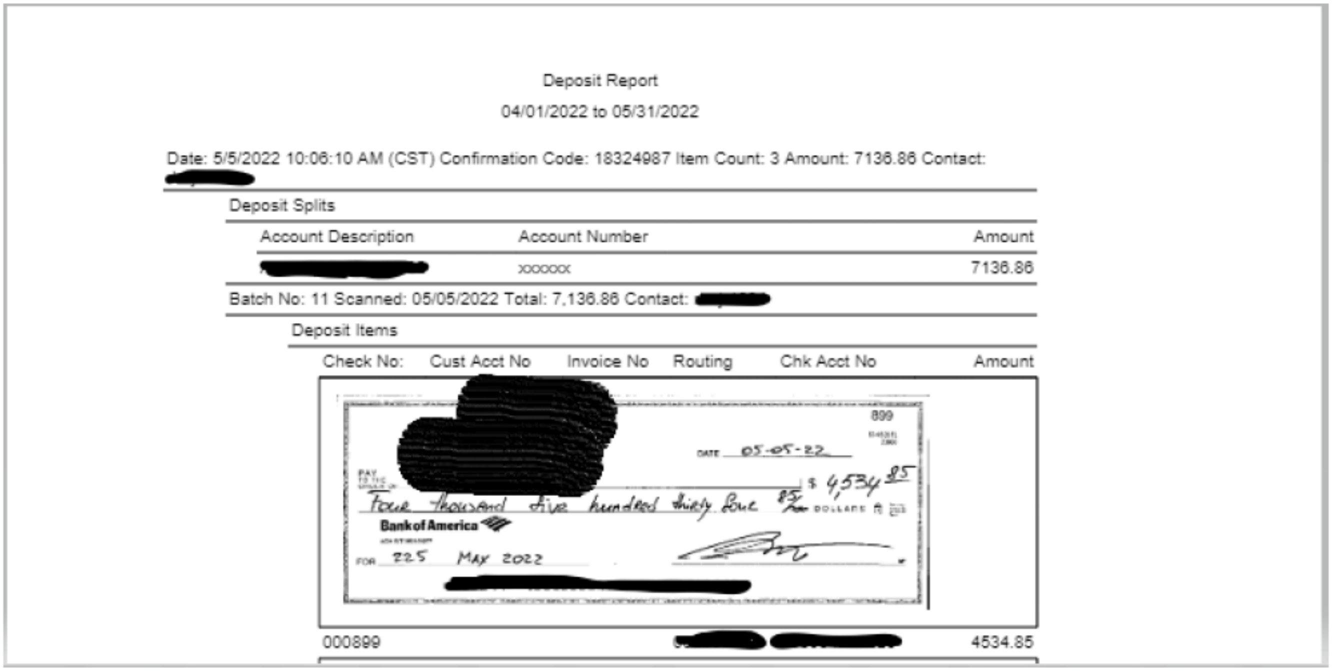
Account Description	Account Number	Amount
[redacted]	xxxxxx	7136.86

Batch No: 11 Scanned: 05/05/2022 Total: 7,136.86 Contact: [redacted]

Deposit Items

Check No:	Cust Acct No	Invoice No	Routing	Chk Acct No	Amount
000899			[redacted]	[redacted]	4534.85
975427			[redacted]	[redacted]	2190.01
1334			[redacted]	[redacted]	412.00

Deposit Report with Images – This will list each check deposited individually with the date, check number and amount along with the account number it was deposited into.



Deposit Report
04/01/2022 to 05/31/2022

Date: 5/5/2022 10:06:10 AM (CST) Confirmation Code: 18324987 Item Count: 3 Amount: 7136.86 Contact: [redacted]

Deposit Splits

Account Description	Account Number	Amount
[redacted]	xxxxxx	7136.86

Batch No: 11 Scanned: 05/05/2022 Total: 7,136.86 Contact: [redacted]

Deposit Items

Check No:	Cust Acct No	Invoice No	Routing	Chk Acct No	Amount
000899			[redacted]	[redacted]	4534.85

[redacted]

899

DATE 05-05-22

PAY TO THE ORDER OF $ 4,534 85/100

Four thousand five hundred thirty four 85/100 DOLLARS

Bank of America

FOR 225 May 2022

[redacted]

Business Digital Banking Risk Assessment & Controls Evaluation

Today's businesses are challenged to find ways to ensure the security of their corporate finances and information, and how to implement appropriate controls to reduce these risks. A good starting point is to make sure you have a strong process in place for monitoring and managing who has access to your Business Digital Banking service and how that information is handled. This evaluation will help you assess your current environment, determine your level of risk, and make sure you have the necessary controls in place.

What Are the Benefits? This assessment will:

1. Help you ensure that the greatest risks to your business Digital Banking operations are identified and addressed on a continuing basis.
2. Help your staff better understand the risks associated with your Digital Banking operations; avoid risky practices; and be alert for suspicious events.
3. Help you determine which risks are the greatest and what steps are appropriate for reducing them.

Instructions:

Go through each question and choose the answer that best represents your environment. The numbers that appear after each possible answer will be used in the Risk Rating section called Risk Rating.

At the end of the Risk Assessment, you'll find a section called "Control Evaluation – Best Answers & Tips." From here, you can make any necessary changes to your environment to ensure your Business Online Banking process is secure. ***PLEASE NOTE: This Risk Assessment <u>does not</u> need to be returned to the Bank. It is provided for your reference only.***

Personnel Security:

1. Do you run background checks and pre-employment screening on your staff?
   a. Yes, for all employees (1)
   b. Yes, but only based on position (2)
   c. No (5)

2. Do you have an Acceptable Use Policy (AUP) that your employees must agree to before they are given access to your information systems?
   a. Yes, at least annually or more frequently as needed (1)
   b. Yes, but only when hired (2)
   c. No (5)

3. Do you conduct user security awareness trainings for each employee using Business Online Banking?
    a. Yes, at least annually or more frequently as needed (1)
    b. Yes, but only when hired (2)
    c. No (5)

Computer System Security:

4. Do your computer systems have antivirus tools enabled and are they updated regularly?
    a. Yes, all systems (1)
    b. Yes, but only critical systems (3)
    c. No (5)

5. Do you have a firewall in place to protect your network?
    d. Yes (1)
    e. No (3)

6. Is there a process in place to ensure your machines are regularly updated with the latest software updates and patches (e.g. Microsoft, web browser, Adobe products, etc.)?
    f. Yes, a formal process where updates are applied at least monthly (1)
    g. Yes, but informally as needed (3)
    h. No (5)

7. Do users run as local Administrators on their computer systems?
    i. No (1)
    j. Only those that require it (3)
    k. Yes (5)

8. Do you use SPAM filtering on your email?
    l. Yes (1)
    m. No (5)

9. Does your email system block executable file types as attachments?
    n. Yes, at the gateway (1)
    o. Yes, on clients (1)
    p. No (5)

10. Do you have an Intrusion Detection/Prevention system (IDS/IPS) in place to monitor and protect the network?
    q. Yes (1)
    r. No (3)

11. Do you conduct annual penetration tests on your network to test your defenses?
    s. Yes (1)
    t. No (5)

12. Is Internet content filtering being used?
    u. Yes (1)
    v. No (5)

13. Are users of the Internet banking system trained to manually lock their workstations when they leave them?
    a. Yes, and the systems are set to auto-lock after a period of inactivity (1)
    b. Yes, but it is only manually (2)
    c. No (5)

14. Is wireless technology used on the network with the Internet banking system?
    a. No (1)
    b. Yes, but wireless traffic uses industry-approved encryption (e.g. WPA, etc.) (1)
    c. Yes, but wireless uses WEP encryption (2)
    d. Yes, and wireless traffic is not encrypted (15)

Physical Security:

15. Are critical systems (including systems used to access Internet banking) located in a secure area?
    a. Yes, behind a locked door (1)
    b. Yes, in a restricted area (2)
    c. No, in a public area (5)

16. Do you have a password policy in place?
    a. Yes, we have a written policy, and users are required to create complex passwords that expire periodically (1)
    b. No (15)

17. How are passwords protected?
    a. Passwords are stored securely. (1)
    b. Passwords are written on sticky notes and placed by the computer. (15)

RISK RATING

Once you have completed the questionnaire, add up the numbers next to each answer you have selected. Using your total, note where you fall on the chart below.

Overall Risk Rating	
1-17	LOW
18-27	MEDIUM
28-37	HIGH
Over 37	EXTREME

Control Evaluation – Best Answers & Tips

Compare your answers to the Business Digital Banking Risk Assessment to the “Best Answers” below. Tips are also provided to help you protect your systems and information.

1. The best answer is “a) **Yes, for all employees.”** Companies should verify job application information on all new hires. Background checks encompass all information about a person’s interactions with the law that a company is entitled to consider in making employment decisions. Additional background and credit checks might be performed for individuals holding certain positions. Once employed, companies should remain alert to changes in their staffs’ circumstances that could increase incentives for abuse or fraud.

2. The best answer is **“a) Yes, at least annually or more frequently as needed.”** An Acceptable Use Policy (AUP) is a set of rules that restrict the ways in which the network, website or system may be used, along with the consequences of noncompliance. An AUP includes things like: expected user behavior; acceptable devices which may be used to access the network, purpose and extent of network activity; prohibitions on circumventing controls or disrupting services; accessing the accounts of others, etc.

3. The best answer is **“a) Yes, at least annually or more frequently as needed.”** Security Awareness Training (SAT) for Internet banking users, at a minimum, should include a review of the acceptable use policy, desktop security, log-on requirements, password administration guidelines, a general understanding of malware, phishing scams, social engineering tactics, etc.

4. The best answer is **“a) Yes, all systems.”** Companies should maintain active and up-to-date antivirus protection provided by a reputable vendor. Schedule regular scans of your computer in addition to real-time scanning.

5. The best answer is **"a) Yes."** Use firewalls on your local network to add another layer of protection for all the devices that connect through the firewall (e.g. PCs, smart phones, and tablets).

6. The best answer is **"a) Yes, a formal process where updates are applied at least monthly."** Update your software frequently to ensure you have the latest security patches. This includes a computer's operating system and other installed software (e.g. web browsers, Adobe Flash Player, Adobe Reader, java, Microsoft Office, etc.). In many cases, it is best to automate software updates when the software supports it.

7. The best answer is **"a) No."** Limit local Administrator privilege on computer systems where possible.

8. The best answer is **"a) Yes."** Implementing email SPAM filtering will help eliminate potentially harmful or unwanted emails from making it to end users' inboxes.

9. The best answers are **"a.) Yes, at the gateway or b.) Yes, on clients"** As a security measure to prevent potential viruses, you should block emails containing undesirable file attachments such as executable files (files ending in .exe). Executable files can contain harmful code that might cause malicious software to download to your computer.

10. The best answer is **"a) Yes."** Intrusion Detection/Prevention Systems (IDS/IPS) are used to monitor network/Internet traffic and report or respond to potential attacks.

11. The best answer is "a) Yes." A Penetration Test is the process of attempting to gain access to resources without knowledge of usernames, passwords and other normal means of access. It assesses your overall security and uncovers holes and vulnerabilities before attackers do. The test provides a report highlighting the weaknesses that need attention, along with advice on how to fix them. Pen Tests should be performed at least annually. Microsoft, for example, discovers new vulnerabilities daily. Maintaining a secure network requires constant vigilance.

12. The best answer is **"a) Yes, Internet traffic on the system used for "high risk" Internet Banking activities is completely restricted to only sites specifically needed for business functions."** Filter web traffic to restrict potentially harmful or unwanted Internet sites from being accessed by computer systems. For "high risk" systems, it is best to limit Internet sites to only those business sites that are required.

13. The best answer is **"a) Yes, and the systems are set to auto-lock after a period of inactivity."** Systems should be locked (requiring a password to reconnect) when users walk away from their desks to prevent unauthorized access to the system.

14. The best answer is **"a) No" or "b) Yes, but wireless traffic uses industry approved encryption (e.g. WPA, etc.)."** Wireless networks are considered public networks because they use radio waves to communicate. Radio waves are not confined to specific areas and are easily intercepted by unauthorized individuals. Therefore, if wireless is used, security controls such as encryption, authentication, and segregation are necessary to ensure confidentiality and integrity.

15. The best answer is **"a) Yes, behind a locked door."** Physically secure critical systems to only allow access to approved employees.

16. The best answer is **"a) Yes."** A password policy establishes a standard for the creation of strong passwords, the protection of those passwords, and how frequently passwords are changed. All users should be trained on what constitutes a strong password and how to create them.

17. The best answer is **"a) Passwords are securely stored."** Passwords should never be left out for unauthorized individuals to gain access.

If you should have questions that are not covered in this Quick Reference Guide, please feel free to call the Digital Banking Department at 1-866-227-7775 during regular business hours and we will be happy to assist you.