partners bank of california

PRIORITIZE THE SAFETY AND SECURITY OF YOUR FINANCIAL ASSETS

Online Banking Security Best Practices for Businesses

Overview

Partners Bank of California prioritizes the safety and security of your financial assets. This guide outlines best practices and risk mitigation strategies to empower you when using our online banking services. It's crucial to act promptly if you suspect a security breach. Contact Partners Bank of California immediately at (866) 323-2741 (Monday-Friday, 9 AM - 5 PM PST) or tm@pbofca.com to report any suspicious activity.

Layered Security: Your Defense in Depth

Effective security is a combination of safeguards, working together to protect your information. The best practices explore various controls categorized as:

- **General Controls and Best Practices:** Foundational measures applicable to all online banking activities.
- **ACH Best Practices:** Specific guidelines for using the Automated Clearing House (ACH) network for payments.
- **Mobile Deposit Capture (MDC) /Remote Deposit Capture (RDC) Best Practices:** Secure procedures for depositing checks electronically.
- **Wire Transfer Origination Best Practices:** Practices and recommendations for processing irrevocable payments in a safe manner.

By considering your risks and implementing these controls, you significantly reduce the risk of fraud and errors.

General Controls and Best Practices

1 **Dual Control:** Enforces verification by a second authorized user for all outgoing payments, minimizing accidental mistakes and deterring internal fraud. The Bank's online banking system fully supports Dual Control when originating payments; settings can offer protection against accidental errors and can also be a strong deterrent to internal and intentional fraud. Do not assign daily account reconcilement to those who are also processing and authorizing payments.

2 **Software Tokens and One-Time Passcodes:** Always activate two-factor authentication (2FA) for enhanced security. Partners Bank's software tokens provide a more secure alternative to passwords alone, requiring physical possession of the device to generate a unique OTP.

3 **Segregation of Employee Duties:** Separate responsibilities for processing payments and reconciling accounts to prevent conflicts of interest and potential fraud.

4 **Positive Pay:** Utilize this automated service to closely monitor and control debits and credits to your account. Positive Pay allows you to define filters that block unauthorized transactions.

Request a 'Block Checks' or 'Block ACH' on all accounts that don't have regular transaction activity such as savings and Money Market accounts.

5 **Validate Payment Instruction Changes Independently:** Never rely solely on emails, even those seemingly from trusted sources. Always confirm changes to wire instructions or ACH account information directly with the requestor via phone call, never using contact details provided in the email itself.

6 **Prepare to Handle a Serious Error or Fraud:** Treat payments like cash. Understand that recovering funds sent in error or to incorrect accounts may be difficult. Develop a plan to handle situations like duplicate ACH file reversals, wire fraud, identity theft, email account takeovers, or encountering altered or counterfeit checks.

7 **Report Suspicious Activity:** Train employees to recognize common scams and report them promptly. Ensure your team knows who to contact internally for assistance. Report suspected email hacks, data breaches, or unusual banking activity to Partners Bank immediately.

8 **Maintain Consistent Internal Practices:** Document internal procedures for processing payments to ensure consistency during employee transitions.

9 **Review User Security Periodically:**

- Conduct regular reviews to ensure users have appropriate system access levels, aligned with their specific roles. Promptly remove access for terminated employees, including mobile banking app access.

- Reiterate the importance of never sharing usernames and passwords. Do you know how to review and disable users, such as for employees who are no longer employed or authorized to use the online service.

10 **Practice Safe Data Transmission, Storage and Destruction:** Securely store documents containing sensitive information like account numbers, voided checks, electronic ACH files, and reports. Implement a secure destruction method for all such materials.

Never transmit sensitive data via unencrypted email, even to seemingly trusted addresses.

11 **Maintain Strong Network Security, Equipment and Software:**

- Install firewalls with automatic updates.
- Subscribe to anti-virus and anti-malware software, and promptly address update notifications.
- Utilize a web filter to regulate employee internet browsing.
- Avoid opening unsolicited emails or attachments.
- Only install programs and files from trusted sources.
- Patch your computer operating systems regularly.
- Monitor your network activity for unauthorized access.
- Do not open unsolicited email messages.
- Do not open a program or file attachment unless you know it is legitimate.
- Install published patches to your computer operating systems
- Monitor your computer network for unauthorized access and system activity.

12 **Train Your Employees to Recognize Fraud:** Regularly educate (and frequently test) your employees on data security, safe banking practices, email fraud and other schemes including:

- Ignoring requests to share one-time passcodes.
- Questioning requests to click on links in text messages.
- Recognizing Business Email Compromise (BEC) scams.
- Identifying phishing attempts designed to steal credentials or personal data.
- Avoiding responses to emails or phone calls requesting personal information.
- Validating email links by hovering over them to preview the URL before clicking. If suspicious, delete the email immediately.
- For suspicious emails from companies or banks, open a new browser window, navigate directly to the organization.
- Use security software that interacts with your web browser to help identify websites that are generally known to be unsafe and used in phishing attacks.

13 **Isolate Banking from Other Potentially Infected Systems or Equipment:** Dedicate a separate computer exclusively for online banking activities, physically securing it and preventing access for web browsing, online shopping, gaming, personal email, downloading attachments, clicking internet search links, or public use.

ACH Origination Best Practices

Your responsibilities with regard to processing payments using the ACH network are described in the NACHA rules and under the Master Treasury Management Services Agreement.

1 **Know The Rules and Responsibilities:** Familiarize yourself with the National ACH Association (NACHA) Operating Rules and Partners Bank Master Treasury Services agreement. 2024 Nacha Operating Rules & Guidelines Online Resource | Nacha. https:nachaoperatingrulesonline.org

2 **Notifications of Change and Returned Payments:** Address NOCs within three business days and understand the implications of excessive returns or recurring NOCs, which may indicate process issues.

3 **Data Accuracy and Validation:**

- **Data Quality:** Ensure the accuracy of all ACH file data, including account numbers, routing numbers, and dollar amounts.
- **Data Validation:** Implement robust data validation processes to catch errors before file submission.
- **Record Retention:** Maintain accurate records of ACH transactions and customer authorizations for at least two years.

Mobile Deposit and Remote Deposit Capture Best Practices

1 **Secure Scanned Checks:** Store processed checks in a locked location, limiting access to authorized personnel.

2 **Destroy Scanned Checks on a Regular Schedule:** Implement a destruction process for checks and documents containing account information after 30 days.

3 **Third Party Checks:** Only process checks payable directly to your company through mobile or remote deposit systems. Contact the bank for approval if processing other types of checks.

4 **Keep a Control Log:** Maintain a control log to log your daily deposits until you have been credited; wrap your daily RDC report around each scanned day's work; and label the daily work with the deposit date, batch number and deposit total. This process will also help you to maintain your deposit destruction schedule.

5 **Endorse Checks Properly:** All checks deposited remotely must state "For Mobile Deposit Only to Partners Bank of Ca". Failure to endorse these restrictively can cause you to be at the center of a legal dispute surrounding whether a check image is valid when items are accidentally or on purpose deposited multiple times.

6 **Prepare for a Power Outage:** Maintain a contingency plan to handle a Hardware/Software/Power failure. Options to consider include scanning next day, delivering to the branch, send to bank via mail or overnight delivery.

7 **Know Your Daily Limit:** If the value of check deposited exceeds your daily limit for the service, include a brief explanation for the over-limit condition along with amount of transaction or deposit, and if it's a check deposit include a copy of largest item within that deposit. Send the information using encrypted email (SECURE) to tm@pbofca.com.

8 **Steps to Take When Receiving a Returned Deposit:** Redeposit NSF returned checks once but contact the bank for guidance on other return reasons.

9 **Know the Clearing Deadlines:** Service processing deadlines for Remote Deposit is 6 PM PST. Mobile Deposit is 4 PM; ACH 3 PM; Wires 2 PM. Transactions submitted on non-banking days will be processed the next business day.

Online Wire Origination Best Practices

Wire transfers are a critical payment method, but they also carry significant risk due to their irreversible nature. Implementing robust controls is essential to protect your funds.

1 **Use Templates:** Lock in the beneficiary's name and account number by using a template. Prevents users from making inadvertent changes to your pre-approved payment instructions.

2 **Verification Process:** Implement a rigorous verification process for all wire transfer requests, including:
- Calling the recipient using a previously known phone number, not the one provided in the request.
- Verifying account information independently.
- Implementing a callback verification process for new vendors or changes to existing payment instructions.

3 **Employee Training:** Conduct regular training on wire transfer fraud prevention, emphasizing red flags and suspicious activity indicators.

4 **Wire Transfer Confirmation:** Obtain written confirmation of all wire transfers, including the recipient's name, account number, and bank information.

5 **Review and Reconciliation:** Regularly review wire transfer activity and reconcile it with accounting records.

6 **Secure Computer:** Use a dedicated computer for wire transfers, free from personal use or internet browsing.

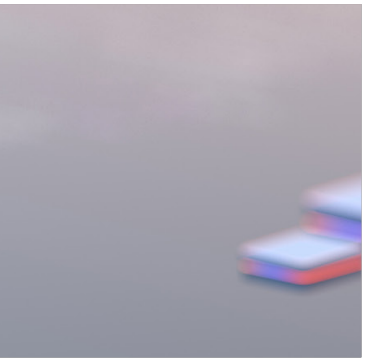
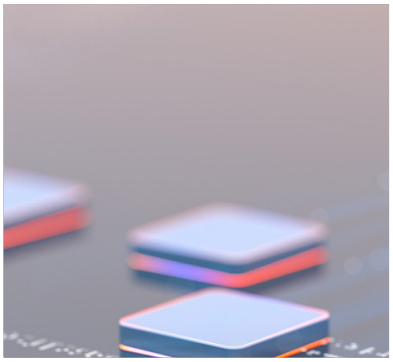
7 **Wire Fraud Insurance:** Consider purchasing wire fraud insurance to mitigate potential losses.

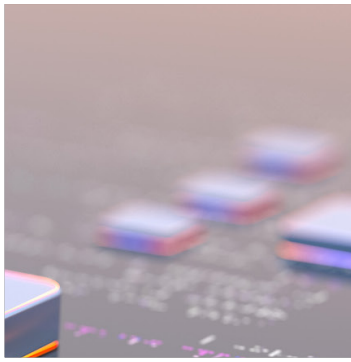
8 **Limit Wire Transfer Access:** Restrict access to online wire transfer functionality to authorized personnel only.

Interested in Learning More?

For more information about online banking security best practices and fraud prevention, please visit our Resource Center on pbofca.com or contact support@pbofca.com.

If you have any questions or need assistance regarding online banking or any of our products and services, please give us a call at (949) 732-4000 or (323) 556-6544, or email us at onlinebanking@pbofca.com.



MISSION VIEJO

Corporate Headquarters
27201 Puerta Real, Suite 160
Mission Viejo, CA 92691

(949) 732-4000

BEVERLY HILLS

8484 Wilshire Blvd., Suite 520
Beverly Hills, CA 90211

(323) 556-6544

pbofca.com

Member FDIC EQUAL HOUSING LENDER