CALIFORNIA BANK & TRUST

ANTI-FRAUD AND CYBERSECURITY BEST PRACTICES CHECKLIST

Help Strengthen Your Defense Against Fraud and Cyber Threats

As digital transactions become standard, the risk of fraud and cybercrime continues to grow. Businesses must proactively implement safeguards to help protect against both internal and external threats.

Account Structure

- ☐ Create separate accounts for payroll and operations.
- ☐ Establish dual account audit/reconciliation processes..

Transaction Protection

- ☐ Review and reconcile all accounts daily and monthly.
- ☐ Formalize policy and procedures for the destruction of private documents.
- ☐ Establish employee transition and termination procedures that include login credentials and passwords.
- ☐ Implement daily ACH and wire transfer limits.
- ☐ Verify any changes in payment instructions through a known associate, using a phone number you have on record.
- ☐ Implement dual control for initiating and approving transactions.
- ☐ Enter the security token at payment release, in addition to entering it when accessing the system.

Device Best Practices

- ☐ Keep operating system and other software up to date. Don't forget programs like Java®, Adobe®, and web browsers (Firefox®, Chrome®, Safari®).
- ☐ Establish guidelines to help secure password utilization. (strong password design, privacy, and periodically updated)
- ☐ Understand the risks of using "cloud" based applications.
- ☐ Uninstall programs that are not used or unnecessary.
- ☐ Require auto-locking computers after a period of inactivity.
- ☐ Implement a firewall.
- ☐ Back up servers (real time if possible).
- ☐ Install Anti-Virus, Anti-Malware and Anti-Spyware software. Keep these systems up to date, and scan for issues regularly.
- ☐ Install an Anti-Malware browser plug-in.
- ☐ Enable SIM Protection: This added layer of security helps prevent SIM swap fraud, which can lead to account takeovers and financial loss.

Internet Browsing Best Practices

- ☐ Do not install software from unknown sources.
- ☐ Do not click on web advertisements or 'pop-ups'.
- ☐ Do not open attachments on unsolicited e-mails. Contact the sender to verify before opening the attachment.
- ☐ Access the bank's website by typing the URL in the address bar; avoid clicking search result links to prevent accessing spoofed sites.
- ☐ Verify domain names on emails before clicking links.
- ☐ Log off online accounts that are not currently being utilized.
- ☐ Implement policies restricting internet access based on need and content.

Internal Operations

- ☐ Use dual authorization for all bank transactions, including wire transfers, online ACH originations, and ACH direct transmissions.
- ☐ Set policies regarding passwords that include: alphanumeric passwords, different passwords for different applications, change often.
- ☐ Require system administrators to have different accounts/passwords from their regular user accounts.
- ☐ Conduct surprise audits.
- ☐ Separate employees to initiate/approve transactions and audit the monthly bank statement.
- ☐ Train employees on fraud detection, payment approvals, and phishing awareness.
- ☐ Review cybersecurity insurance to confirm coverage requirements.
- ☐ Maintain a disaster contingency and incident response plan addressing potential data breaches.

Banking Services*

- ☐ Require dual authorization when utilizing bank services.
- ☐ Adopt Check Positive Pay with Payee Match to strengthen check fraud prevention.
- ☐ Help stop fraudulent ACH transactions by using our ACH Positive Pay service. With this service, you can control electronic withdrawals from your account.
- ☐ Predetermine amounts authorized ACH originators can debit accounts by using ACH debit filters.
- ☐ Use alerts to be notified of account changes and transaction activity.
- ☐ Disconnect immediately if contacted by an unfamiliar banker offering transaction assistance; verify by calling us directly.

Reporting Fraud

Notify us immediately if you suspect that your account information has been hijacked and misused to commit fraud or theft.

- If you suspect your account or sensitive information has been compromised, such as missing checks or online banking credentials, and may be used for unauthorized or fraudulent activity, please contact us immediately at 800-840-4999 (Mon - Sat, 6:00 a.m. - 9:00 p.m. MT).
- If you believe you have received or responded to a fraudulent email purporting to come from us or one of our bankers, forward the email to abuse@calbanktrust.com.
- Remember, we will never ask you for your RSA token, password, or secured financial information through unsolicited messages or calls.

*Some Treasury Management products are subject to credit approval and agreement. Contract and fees may apply. Contact California Bank & Trust Treasury Management or go to **www.calbanktrust.com.com/business/treasury** for more information on Banking Services offered by California Bank & Trust.

CB TRUST CALIFORNIA BANK TRUST