PROVIDENCE BANK & TRUST

Service, Stewardship and Security

Fraud Exposure Checklist

7 key questions you should ask yourself before you decide you're too busy and "round file" this checklist!

KEY QUESTIONS	Y	N	COMMENTS:
✓ Do bank statements arrive at your desk **unopened**?			
✓ Do you personally review bank statements **every month**?			
✓ Do you personally review **daily account activity** online via your online balance reporting to spot irregular entries? If not, is this done by someone who has **no signing authority** on the account(s)?			
✓ If you utilize ACH transactions or wire transfers, is there a **second level of approval** on all outgoing funds transfers?			
✓ Do you have an **approved vendor list** for your payables, and do you **review it periodically**?			
✓ If you have cash receipts, do you have **dual controls** in place? Can you see that the cash actually was deposited?			
✓ Do you **review** payroll reports and **verify** that payees and amounts are appropriate? Can you put a name and face with each payroll check?			

Did you answer "no" to any of these questions? If so, your company may be at risk for fraud. Are there other areas in which you may have additional fraud risk? Maybe you should continue on...

BANK RECONCILIATIONS:	Y	N	COMMENTS:
✓ Are bank reconciliations prepared: ⤷ **Monthly** for **all** accounts? ⤷ By someone **other than** the person authorized to sign checks or initiate other transfers?			
✓ Are **all items** on the bank account statement **reconciled** and accounted for?			
✓ Do you review bank reconciliations for cancelled checks and especially **for unusual items**?			
✓ Are bank reconciliations reviewed and adjustments of the cash accounts approved by you to underline **dual control**?			
✓ Do you regularly review your Account Analysis statement for bank services you are using to determine their usefulness and/or to see if there are services you are not using but should be?			

A/R & A/P CONTROLS:	Y	N	COMMENT
✓ Do you review accounts receivable aging lists?			
✓ Does someone who is **not involved** in general ledger or accounts receivable make the call for			
✓ Are all sales orders recorded on pre-numbered forms and are all numbers accounted for?			
✓ Are monthly statements for outstanding balances: J Reviewed by you? J Mailed by you or a responsible **employee other than the bookkeeper/accountant**?			
✓ Are checks to trade vendors matched against the invoice as well as proof-of-receipt of the product?			
✓ Other than for tax purposes, do you have **regular outside audits**?			

CASH RECEIPTS	Y	N	COMMENT
✓ Do you, or a responsible employee (**other than the Bookkeeper or A/R clerk**): J Open the mail and pre-list all cash receipts before turning them over to the bookkeeper? J Compare daily pre-listing of cash receipts with: – Cash receipts journal? – Duplicate deposit slip? – Bank statement?			
✓ Are cash receipts deposited intact on a daily basis?			
✓ Are cash receipts posted promptly to appropriate journals?			
✓ Are cash sales controlled by cash registers or pre-numbered cash receipt forms?			

CHECK STOCK	Y	N	COMMENTS
✓ Are you a necessary signatory on all checks?			
✓ Are checks always pre-numbered?			
✓ Do you review cleared checks and ACH items for **missing, out of sequence numbers or fraud**?			
✓ Is your check stock kept in a **secure** (locked) location?			
✓ Are all checks recorded as they are issued?			
✓ Is a mechanical check protector or other fraud protection used as a precaution against alteration?			
✓ If a signature plate is used, is it only under your sole control? If not, is access to the plate **controlled** and used under double custody? Do you use it only when necessary rather than as the norm?			
✓ Are voided checks retained, noted, and then shredded or mutilated?			
✓ Are **supporting documents** (invoices, reports, purchase orders, etc.) presented to you with the payables checks and reviewed by you **prior to** signing the checks or approving ACH credit issuance?			
✓ Are supporting documents for payables checks properly cancelled to avoid duplicate payment?			
✓ Are checks payable to cash prohibited?			
✓ Is signing blank checks prohibited?			
✓ Are signed checks mailed by someone **other than** the person who writes the checks?			
✓ Are outgoing payables checks securely delivered to the Post Office rather than being left in an "out basket" where they might be picked up and misused?			

INFORMATION SECURITY	Y	N	COMMENTS:
✓ Do you have an Information Technology (I.T.) Manager?			
✓ Do you have a **policy** (written or unwritten) that addresses information security?			
✓ Is your workplace secured with an **alarm system** or do you have **access controls**?			
✓ Do you maintain an internet firewall to protect data?			
✓ Do you use and regularly update anti-virus software?			
✓ Are your computer systems and equipment configured to install critical security patches **automatically** when they are released?			
✓ Do you maintain **secure** systems and applications?			
✓ Do you use a **wireless** network, and if so, is it **secure** and are transmissions encrypted?			
✓ Is access control in place for computer and information systems with multiple users to restrict access based on a user's **need to know**, and is it set to "deny all" access unless specifically allowed?			
✓ Is **IBM Trusteer Rapport** software installed on all computers used to access cash management services banking applications?			
✓ Do you regularly **test** security systems and			
✓ Do you have formal information technology **(I.T.) audits** performed by in-house auditors or other third party I.T. auditors?			
✓ Do you have a change management policy in place to revoke user access to systems when necessary?			
✓ Are computer / network passwords changed at least every 90 days?			

ELECTRONIC BANKING	Y	N	COMMENTS:
✓ Do you have complete access to your on-line banking program? Do you use it daily?			
✓ Do you or a trusted administrator safeguard and monitor who can access the system and what they can see/do?			
✓ Does your Network Administrator require complex, hard-to-guess passwords?			
✓ Do you have a policy in place to require that passwords be protected and **never** shared?			
✓ Do you review ACH origination entries/wire transfers (both outgoing and incoming) regularly?			
✓ Do you have a **change management policy** in place to revoke user access to the system when necessary?			
✓ Do you use **Positive Pay** for issued checks and/or **Blocking and Filtering** for electronic entries?			

ACH ORIGINATION	Y	N	COMMENTS:
✓ Have you obtained **signed authorizations** for **all** accounts to which you are sending ACH debits and/or ACH credits?			
✓ Are ACH Debit and/or Credit Authorizations maintained in a secure environment with access limited to authorized personnel?			
✓ Are ACH authorizations retained for at least **2 years** from the date of the last transmission?			
✓ Do you destroy these and other sensitive information documents (by burning, shredding, commercial shredding, etc.) at the end of the retention time?			
✓ Have you restricted access to ACH origination and/or wire transfer origination services on bank systems to specific IP addresses related to computers used by authorized personnel only?			
✓ Have you reviewed your ACH agreement to make sure you are complying with your responsibilities?			

REMOTE DEPOSIT CAPTURE	Y	N	COMMENTS:
✓ Do you retain **original scanned checks** for at least 30 days but not more than 60 days?			
✓ Do you retain all information regarding your digitizing of checks as created by the System for **at least seven (7) years**?			
✓ Do you lock / secure checks and other documents with sensitive information to **protect non-public personal information** from being compromised?			
✓ Do you destroy the checks and other sensitive documents (by burning, shredding, commercial shredding, etc.) at the end of the retention time?			
✓ Do you use the **electronic endorsement** feature of check scanning, and if so, are endorsement settings for each account correctly set?			
✓ Are all scanned checks made payable to the account holder of record as shown on the bank statements (your business or organization)?			
✓ Are you routinely cleaning your scanner equipment as recommended by the scanner manufacturer?			
✓ Have you reviewed your Remote Deposit Capture agreement to make sure you are complying with your responsibilities?			

MISCELLANEOUS	Y	N	COMMENTS
✓ Are annual **one week vacations mandatory** for all employees with access to books, cash, or receivables duties?			
✓ Are employees **cross-trained** so no one individual is always responsible for a specific duty without oversight?			
✓ Have there been any changes in management or the responsibilities of key employees that should be communicated to the bank?			

If you answered "no" to any of these questions, you may need to spend additional time evaluating your internal processes and controls to minimize the risk of fraud in your company.

Please be aware that this is not an "all inclusive" list of potential risk areas. It is intended to alert you to areas of possible weakness in your systems or practices. Fraud is a serious, expensive, and time-consuming matter when it affects your business and we want to help you avoid it if possible!

We urge you to plan a meeting with your staff, your accounting firm, or fraud prevention professionals to further discuss and evaluate these important topics.