TREASURY SOLUTIONS
FRAUD PROTECTION CHECKLIST

As your partner, Independent Financial is here to help your business mitigate payment fraud, scams, hacks, social engineering, cyber-enabled fraud and more. We have created this checklist to guide you through the process of assessing your business processes and identifying practical applications to strengthen your company's fraud protection controls**.**

Bank Accounts and Service

- ❒ Limit the number of business accounts and monitor account balances and account activity daily. Keep authorized bank account signers and their contact information up to date.
- ❒ Review and update signature cards annually and immediately after any changes with signers occur.
- ❒ Manage suspected check and ACH fraud using bank-provided Positive Pay services by uploading issue files, reviewing presented exceptions daily and decisioning exceptions after verifying transaction details.
- ❒ Determine which accounts will be used only for electronic transactions and block non-electronic debits such as checks.
- ❒ Manage ACH debits with blocks and filters to prevent unauthorized transactions. Only give approved companies account access.

Paper Check Controls

- ❒ Use a reputable supplier when ordering checks, be sure check stock includes security features and monitor check orders to ensure receipt of exact quantity and selected styles.
- ❒ Securely store check stock and printing equipment and ensure associated applications use dual control and authorization.
- ❒ Avoid handwritten checks and never sign checks in advance without completing amount and recipient information.

Information Security

- ❒ Keep your software, including operating systems, applications and anti-virus programs, up to date on all electronic devices to protect against the latest security vulnerabilities.
- ❒ Use complex, unique passwords for all devices, accounts and networks. Consider using a password manager.
- ❒ Enable two-factor authentication (2FA) wherever possible to add an extra layer of security beyond just a password.
- ❒ Use caution when downloading, installing and opening software, applications and documents. Always use reputable software vendors and verify third-party sources.
- ❒ Avoid using unsecure means of communication to send sensitive information such as account numbers and instead use secure email and encrypted file transfer software or other encrypted communications. Only use secure websites leading with **https://**.
- ❒ Beware of any emails, phone calls and text messages urging you to click a link, download or open an attachment, run an application or provide your credentials such as username and password.
- ❒ Avoid using public Wi-Fi and other untrusted networks and use a virtual private network (VPN) whenever possible.

Internal Controls

- ❒ Monitor accounts daily and inform us of any potential unauthorized activity.
- ❒ Regularly review access and privileges and limit administrator rights. Consider a dedicated workstation for online banking.
- ❒ Set policies around using strong, unique passwords and require passwords to change regularly.
- ❒ Activate transaction notification features in Online Banking.
- ❒ Use dual control and secondary authorization for all payment transactions.
- ❒ Implement a security education, training and awareness program to bolster your organization's security culture and address common threats such as business email compromise, social engineering and fraud.
- ❒ Regularly educate employees on the importance of safeguarding sensitive information and following established policies and procedures to avoid behaviors that can expose your organization to fraud.
- ❒ Ensure processes are established to immediately deactivate or remove accounts and accesses for departed employees.

Operational Controls

- ❒ Consider using electronic payment capabilities to reduce the potential for check payment fraud.
- ❒ Validate all emailed requests for payment by calling the requestor.
- ❒ Always verify vendor legitimacy for unexpected or suspicious invoices, address change requests or other communications.
- ❒ Create a policy for document retention and safekeeping and destroy documents that are no longer necessary to retain.
- ❒ Protect sensitive Information and use extreme caution when being asked to provide an account number or bank credentials or other financial information.
- ❒ Institute a Clean Desk Policy ensuring employees lock their workstations when they are away from their computer, leaving no sensitive information available to unauthorized personnel. Shred all appropriate documents when no longer needed.
- ❒ Do not log in and access financial information and applications via an unsecure public internet connection.