

The Fraud Prevention Checklist: Protecting Your Business in Six Steps

By Rockland Trust Treasury Management



ROCKLAND
TRUST
BANK

Where Each Relationship Matters®

Member FDIC

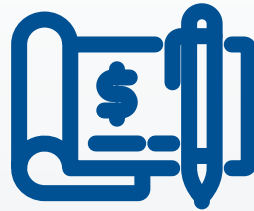
The last several years have not gone as planned. Many businesses anticipated that by now, they would be back to “normal” circumstances. However, as we all know, this has not been the case for many businesses. Hybrid working environments and operational business changes, among other things, have led to an increase of fraudulent activity specifically targeting businesses.

Did you know?

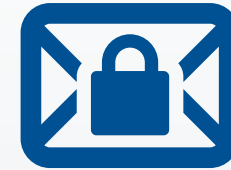
In recent years, it was reported that:



Median loss per business fraud case: \$120,000*



80% of organizations were victims of either attempted or actual fraud†



63% of organizations experienced Business Email Compromise†

What can you do?

Here's the Rockland Trust Fraud Prevention Checklist to help you better protect your business. We break this into six parts:

- ✓ Check Payment Controls
- ✓ Reconciliation Reminders
- ✓ Online Overview
- ✓ Payment Processing
- ✓ Deposit Diligence
- ✓ Layer Your Strategy

*Association of Certified Fraud Examiners Occupational Fraud 2024: A Report to the Nations
†The Association for Financial Professionals (AFP) Payments Fraud and Control Survey 2024

ROCKLAND
TRUST
BANK

Where Each Relationship Matters®

Member FDIC

Check Payment Controls

- Keep it Safe** – Locking up your checks is the easiest way to secure them.
- Have a System** – Who creates them, who signs them, who reorders them. Review this often and ensure the right internal controls are in place.
- Get a Style** – If you have multiple accounts, choose a different style for each checkbook to limit confusion for your team.
- Give Updates** – Be sure to notify your financial institution if you have a change in authorized signers.
- Implement Tools** – Most financial institutions have tools that help guard against fraudulent check activity. Positive Pay will compare your issued checks against checks presented for payment, and flag any differences for review.
[Click here to view a demo.](#)

Payment Processing

- Securing Bill Payments** – Replicate your internal controls as you would for paper checks. Ask your financial institution if dual approval, user access and limits are available.
- ACH Payments** – Practice dual control and verify ACH account information with a pre-note. Always secure recipient authorization for all payment types and be sure to follow [NACHA guidelines](#).
- Positive Pay** – Use tools such as Positive Pay to filter and/or block unauthorized ACH transactions in addition to check payments. Payee Match also verifies the payee name on presented checks before they get paid.
- Wires** – Utilize dual control and validate account information over the phone before wire payments are sent.
- Recipient Data Changes** – Set up phone procedures (secret code, verbal confirmation, etc.) with your recipients to validate new account information. Validate changes to financial data by phone with a trusted contact every time!



IMPORTANT REMINDER:

ALWAYS verify payment change instructions **OVER THE PHONE** with a contact who you know and trust!

ROCKLAND
TRUST
BANK

Where Each Relationship Matters®

Member FDIC

Reconciliation Reminders

- Check Accounts Daily** – There are several channels that will allow you to review your accounts – text, online, mobile. We recommend reviewing your accounts daily.
- Alerts** – **Alerts** are a good way to manage balance, activity, payments and security of your accounts. Create a system that makes it easy for you to monitor your account activity.
- Match Payments** – Make sure your payments are posted correctly.
- Reconciliation Tools** – Generate daily/weekly/monthly reconciliation reports for full account, deposit, and check activity. Contact Rockland Trust to set up Account Reconciliation.
- Sound the Alarm** – If something doesn't look right, report it immediately.

Deposit Diligence

- Remote Deposit** – By depositing checks directly from your location, you can keep your deposited items secure, save time and avoid employee travel expense and liability.
- Consider Lockbox** – Centralize, automate and expedite a secure collection of your receivables with a lockbox service.
- Go Mobile** – Deposit checks directly via your **mobile device**.
- Account Segregation** – It is recommended to segregate certain transactions from your operating account, such as credit card processing, payroll and incoming wire activity, to avoid unnecessary fraud exposure.

ROCKLAND
TRUST
BANK

Where Each Relationship Matters®

Member FDIC

Online Overview

- Sharing is Not Caring** – Use strong user credentials (passwords) that are unique and only available to you.
- Dual Control** – Set up company-wide dual control for ACH and wire transactions, bill payment and Positive Pay services.
- Designate User Authorities** – Assign user access appropriately based on the responsibility of that user. Designate administrator rights wisely, as this user will typically have full rights to add users, send payments and assign other user rights.
- Banking Access Computer** – Designate a secure computer without email, for your financial transactions.

The presence of fraud is increasing year over year. Since many incidents are due to human error, the human element and behavior modification are key factors for keeping your company safe. Ongoing training of every employee and implementing these simple steps can help to better protect your reputation, business and assets.

As a final reminder, it is important to validate financial changes by phone with a trusted contact – every time!

If you have questions or would like more information, please reach out to us: RTCCashManagement@RocklandTrust.com

Layer Your Strategy

- Training** – Train all employees on a consistent basis. Simulated phishing tests are one example of a way to test the knowledge of your teams.
- Email Safeguards** – Be aware of emails that note a change of financial data, attachments, links, unusual content and requests. Validate this information by phone with a trusted contact every time!
- Incident Response Plan** – Create an incident response plan, train your employees and practice it.
- Internet Usage Policy** – Create a strong Internet usage policy to include social media etiquette and enforce it for all employees from the front desk to the CEO.
- Technical Support** – Enlist your IT team or hire a cybersecurity provider to set up protections such as firewalls, security patches, and data backup. Consider how long your business can operate if systems are down or data is lost when selecting a cyber security plan.
- Insurance Coverage** – Contact your insurance provider to evaluate options for cyber security coverage.

ROCKLAND
TRUST
BANK

Where Each Relationship Matters®

Member FDIC