Protecting Your Business from Fraud

A guide for business customers of Martha's Vineyard Bank.

Running a business means moving money every day, which can make companies a frequent target for fraud. This guide covers common threats and the habits that help keep your account more secure.

Why business fraud is different

Most people know to guard passwords, think twice before clicking a link, and monitor accounts closely. Businesses face a separate set of risks because larger sums move through business accounts, more people may have access, and payments often go out by wire or ACH on tight timelines. The federal protections that limit a consumer's liability for unauthorized electronic transactions generally do not extend to business accounts in the same way, which is why prevention deserves real attention.

The most common threats

- **Business email compromise.** A scammer poses as an executive, employee, or vendor and asks for a payment or a change to banking details. Messages can look convincing, sometimes coming from an address that's similar to a real one.
- **Invoice and vendor fraud.** A fake or altered invoice arrives, or a real vendor's payment instructions appear to change. Funds get routed to a criminal's account.
- **Wire and ACH fraud.** These channels get targeted because they move money quickly and in larger amounts. Once a wire leaves, recovering it can be difficult.
- **Check fraud.** Checks can be stolen, altered, or counterfeited. Businesses that write and receive checks in volume carry more exposure here.
- **Internal fraud.** When several people can access accounts and approve payments, there's more risk, whether deliberate or through a compromised login.

What you can do

- **Verify before you pay.** For any request to send funds or change payment details, confirm it through a known phone number, not the contact information in the message itself. Treat urgency and secrecy as warning signs.
- **Set up dual controls.** Require a second person to approve wires, ACH batches, and new payees. A single approval is a single point of failure.

- **Limit and review access.** Give each user only the permissions their role requires and remove access promptly when someone leaves. Review the list of users regularly.
- **Reconcile often.** Check accounts daily during busy stretches. The sooner an unauthorized transaction is caught, the better the odds of stopping it.
- **Protect your devices and logins.** Use strong, unique passwords and turn on multifactor authentication. Keep software current and be cautious on shared or public networks.
- **Guard your checks.** Store checks securely and use the fraud prevention tools available to you.

If you suspect fraud

Act quickly. Time matters, especially with wires and ACH transfers. Contact us right away so we can help review the activity and take the appropriate steps. Keep any suspicious emails, invoices, or messages, since the details can help. We would rather hear from you about a false alarm than learn of a problem too late, so if something feels off, reach out.

Need more help? Call us at 508-627-4266 or stop by any office for in-person support.