Protecting Your Business From Fraud

Smart Tips and MB&T Tools

Fraud continues to be one of the most pressing threats facing small and mid-sized businesses. Even tech-savvy companies are increasingly vulnerable as fraudsters evolve their tactics. Understanding how fraud occurs and the common ways criminals target businesses is the first step toward prevention.

Common Business Fraud Scenarios

Business Email Compromise (BEC)

Fraudsters impersonate executives, vendors, or employees to trick your team into sending payments or sharing confidential information. These scams often appear legitimate and exploit urgency.

In the U.S. in 2024

21,442 complaints → **$2.77B losses**

CA reports the highest volume and losses[1]

Tips for preventing BEC:

1. **Verify requests by phone:** For payment changes, wire transfers, or sensitive data requests, confirm the request by calling a known number for the individual or company.
2. **Be skeptical of urgency:** Train staff to pause if an email pressures them to act quickly or secretly, especially from a "CEO" or vendor.
3. **Train staff to detect red flags:** Look for misspellings in the sender address, unusual names in the CC line, or errors in tone, spelling, or grammar.

Check Fraud

Check fraud occurs when criminals alter, forge, or counterfeit checks to divert funds from your account. *Check mail fraud* happens when criminals steal checks from the mail, alter them, and attempt to cash them as their own.

In 2024

1,458

BSA reports filed by CA banks

CA banks reporting a steep increase in 2025[2]

Tips for preventing check fraud:

1. **Hand-deliver checks to the post office:** avoid leaving them in outdoor mailboxes.
2. **Use ACH payments whenever possible:** electronic payments keep account info secure.
3. **Enroll in Positive Pay:** match presented checks or ACH debits against issued items to catch fraud.
4. **Use high-security checks:** watermarks, microprinting, and heat-sensitive ink can deter criminals.
5. **Review the cleared check image:** this ensures the payee information hasn't been altered.

Businesses that combine strong internal processes, employee training, and banking tools significantly reduce their exposure to fraud.

Remember, prevention is always more cost-effective than remediation!

Check out MB&T's tools inside!

[1] FBI IC3 Annual Report 2024. [2] FINCEN Check Fraud Report.

Easy, Everyday Steps to Protect Your Business

Businesses don't need to be IT experts to build strong fraud defenses. Simple, consistent habits can significantly reduce exposure.

Cybersecurity Checklist

- ✓ Use strong, unique passwords and change them regularly.
- ✓ Limit admin access to essential personnel & update as necessary.
- ✓ Never approve payments based on emails alone—always verify.
- ✓ Install antivirus software and update systems frequently.
- ✓ Reconcile bank accounts daily or weekly.

NEVER give your password or one-time passcodes to ANYONE

Smart Banking Habits

- Be cautious of urgent payment requests, especially from new vendors.
- Keep checks, company stamps, and sensitive paperwork in a secure location.
- Always log out of online banking portals when not in use.
- Train staff to recognize and report suspicious activity.

Built-in Security Features in MB&T Business Banking

At MB&T, all business clients can activate and tailor **free built-in fraud protections** that work together to reduce risk and increase control over finances.

Online Banking Protections

- **Multi-Factor Authentication (MFA):** Extra verification when logging in from unrecognized devices.
- **Real-Time Alerts:** Immediate notifications when transactions post.
- **User Permissions:** Assign custom roles so personnel can only access what they need.
- **Dual Approvals:** Require two users to authorize sensitive transactions like wires or ACH transfers.

Next Step: Connect with your Business Banker to review your fraud protections and ensure your accounts are secure.

MB&T’s Secure Tools That Streamline Your Business Operations

Managing payments efficiently while staying protected is possible when you use the right tools. Here’s how Montecito Bank & Trust’s **Cash Management Solutions** can help you improve both security and cash flow.

Remote Deposit Capture (RDC)

RDC allows you to scan and deposit checks from your office—saving you trips to the branch and giving you faster access to funds. You can control who has deposit access and enable dual control settings for added security.

→ RDC reduces fraud risk:

By depositing checks from your office, you reduce the risk of lost or stolen items during transit to the bank. The digital transmission is encrypted, and you maintain physical control of checks until they’re securely destroyed.

ACH (Automated Clearing House) & Wire Transfers

ACH is great for recurring payments like payroll, rent, or vendor bills. Wire transfers are ideal for large, time-sensitive payments. Both services give you the ability to manage cash flow securely and efficiently. Using dual approvals and user permissions minimizes the risk of fraudulent transactions.

→ Electronic transactions are safer than writing checks:

ACH and wire payments are transmitted electronically, eliminating the risk of paper checks being stolen, altered, or counterfeited. Check fraud often occurs because account and routing numbers are printed right on the check. With ACH and wires, your payment information is encrypted and transmitted securely, reducing opportunities for fraud.

Positive Pay for Checks & ACH

Positive Pay helps stop fraud before it happens by comparing the checks or ACH debits presented against the ones you’ve authorized. If something doesn’t match, you’ll be notified and can approve or reject the item.

→ Positive Pay enhances security:

Positive Pay acts as a real-time filter, flagging suspicious items before funds leave your account. This extra layer of review stops fraudulent checks and ACH debits before they clear, protecting your business from losses.

Learn more about MB&T’s Cash Management Solutions:
Trusted Resources for Business Fraud Prevention

Trusted Resources for Business Fraud Prevention

Agency	Website	Resources Available
CISA	cisa.gov	Practical steps to strengthen cybersecurity, protect online banking, secure networks, and defend against phishing and ransomware.
FTC	ftc.gov	Guidance on safeguarding customer data, preventing fraud, and complying with federal data security requirements.
FBI / IC3	ic3.gov	Alerts on emerging cyber threats, tips to prevent payment fraud, and instructions for reporting incidents.
U.S. Secret Service – Cyber Fraud Task Force	secretservice.gov	Investigates and prevents financial cybercrime, including account takeovers and wire fraud.
FDIC	fdic.gov	Educational resources on protecting account credentials, avoiding phishing scams, and securely managing online banking.

If you suspect fraudulent activity (scam emails, texts or calls), notify us:
(805) 963-7511 | fraud@montecito.bank

If you suspect a scam, report it to your **local law enforcement**.

If you suspect an internet-based crime, report it to the **IC3**.

For additional fraud prevention resources, visit **montecito.bank/fraud**

Montecito Bank & Trust®

Member FDIC