



## Fraud Awareness & Risk Management

### Fraud Prevention Best Practices

Use this checklist as a guide to protect your business.

- Check before you click – be on the alert for business email compromise or malware.
- Reconcile accounts frequently (preferably daily).
- Ensure that adequate procedures are defined and followed for all types of payments (paper, electronic, and digital).
- Provide ongoing training to employees on detecting and preventing electronic fraud.
- Ensure that disaster recovery plans are in place and tested annually.
- Hire and consult IT and cybersecurity experts.
- Have a comprehensive information security policy, and test and review practices annually.
- Conduct periodic risk assessments.
- Validate internal controls through phishing and malware testing, training, and internal audit team tests.
- Review insurance policies to ensure that your company has business crime insurance in place to protect itself from fraud-related losses.
- Establish an alert system to quickly identify fraud.
- Ensure that digital and paper documents are disposed of securely.
- Use contact info (i.e., email addresses and phone numbers) from your files, not that were sent to you in an email.
- Use dedicated and protected computers for payments origination (restricting and/or limiting access to personal email, web browsing, and social networks).
- Restrict organization network access to company devices only, preferably via secured environment (i.e., Citrix or VPN).
- Adopt a Dual Control environment requiring multi-level approvals for all payment types.
- Consider fraud control services such as ACH, Payee or Reverse Positive Pay.
- Use encryption for sensitive information.
- Utilize tamper-resistant features on checks.
- Segregate duties at all levels, especially in the accounting department.

In 2023, **80% of organizations** experienced attempted or actual payments fraud.<sup>1</sup>

### In addition to potential monetary loss, additional costs may be incurred from:

- ✓ Investigating the fraud, including fees paid to outside consultants
- ✓ Closing compromised accounts and establishing replacement accounts
- ✓ Replacing compromised financial instruments such as check stock
- ✓ Legal fees associated with losses
- ✓ Staff time and mailing costs associated with notifying vendors and/or customers of changes
- ✓ Staff time spent dissecting the fraud and analyzing or reconstructing records
- ✓ Distraction and impact to morale at all levels after an attempted or actual fraud incident



**Want more information on  
Fraud Awareness?**  
Connect with Webster Bank.

<sup>1</sup> <https://www.afponline.org/training-resources/resources/survey-research-economic-data/details/payments-fraud>  
The opinions and views herein are for informational purposes only and are not intended to provide specific advice or recommendations. Please consult professional advisors with regard to your situation.