

PROTECTING YOUR BUSINESS

Tips and tools for
guarding against fraud.



Bank of Marin

BANKOFMARIN.COM

Protecting Your Business

How would you like to boost your revenue by 5%?

According to the Association of Certified Fraud Examiners (ACFE), 5% of revenue is what the average business loses in any given year due to fraud, with a median loss of \$117,000. And, small businesses with less than 100 employees had the highest median loss of \$150,000. If you're not taking active steps to detect and prevent fraud, you may be opening yourself up to that 5% loss and potentially much more.*

Bank of Marin is dedicated to educating you about how to prevent fraud on your accounts and to keeping your information and finances secure. The tips and tools we've provided in this guide will help you identify potential gaps in your fraud prevention activities and the steps you can take to protect yourself and your business.

As a business bank, we are committed to ensuring you have the right tools to keep your information and accounts secure. With the proper protections in place, you can sleep comfortably at night knowing that your business, and your money, are safe and sound. Much trust in their employees, there are clear opportunities for small businesses and nonprofit organizations to increase their protection against fraud.*

Best Practices for Business Owners

Fraud can be especially devastating to small businesses and nonprofit organizations. Whether it's due to resource limitations, a lack of awareness, or a tendency to place too much trust in their employees, there are clear opportunities for small businesses and nonprofit organizations to increase their protection against fraud.*

1 Establish Internal Controls

- Limit electronic access to financial information or sensitive documents.
- Create strong and secure passwords, and change them frequently.
- Develop company policies that control how financial transactions are made.
- Implement review and authorization procedures.
- Conduct daily review and reconciliation of transactions by a third party not involved in the payables process.

2 Secure and Maintain Computer Systems

- Be cautious when utilizing wireless networks. Avoid doing business on public wireless networks, and use encryption on your own wireless network.
- Ensure up-to-date firewalls, anti-virus software and spyware prevention software are in place for all computers.
- Maintain the physical security of computers and limit access to computers that are used for sensitive functions.
- If possible, use a computer dedicated to banking and financial transactions only, with no internet browsing.
- Do not download or install software from unknown third parties.
- Do not open email or email attachments from an unknown source.

3 Supervise and Monitor Financial Transactions

- Use an automated monitoring system and/or continually review wires, transfers, payroll and business checks.
- Provide ongoing training and adequately supervise anyone who takes part in business finances.
- If appropriate based on business size, consider utilizing CPAs to conduct audits, and conduct your own regular and unscheduled audits of inventory and finances.

Electronic Vendor Payment Fraud

Vendor fraud occurs when fraudsters gain access to documentation to change the bank routing and account numbers for electronic vendor payments. In an attempt to disguise the fraudulent activity, they may compromise email or use a fake email domain to make themselves look like the legitimate representative of a vendor. Here are some important strategies and tips to help protect your business against electronic vendor payment fraud:

General Strategies

- Carefully review and confirm information using a known, reliable source BEFORE making any changes to vendor information, particularly payment addresses and/or bank account information.
- Coordinate with your information technology team to establish and maintain up-to-date system security and e-mail spam filters.
- Address payment questions as quickly as possible because they may expose vendor or payment fraud.

Staffing Considerations

- When changing vendors involve more than one staff member in the process. Proper separation of duties helps ensure that the individual who enters information into the system and the person who approves the change is not the same person.
- Have the accounts payable vendor manager or their supervisor review all vendor changes for a given day, week, or month. Provide the paperwork for vendor changes to the manager, along with a system report. Use this review process as a training tool to make your vendor staff more aware of risk.

Electronic Vendor Payment Fraud

Process Tips

- Never rely on e-mail to confirm changes to vendor payment information.
- Call the vendor using information you already have in your records. Do not call a new phone number to verify changes; you may be talking to the fraudster.
- Provide a script to staff to use when confirming changes. Remind staff not to provide vendor information, instead always ask vendors to provide both old and new account information. The vendor should provide the information without assistance.
- Conduct an online search or validate the vendor's street address and phone numbers using reputable databases.

Follow-Up Strategies

- Notify your local branch and law enforcement if you become aware of fraudulent account numbers and/or account routing information.
- After notifying the branch and law enforcement, scrub your vendor file data for other vendor accounts that might use the same bank routing number or account number.
- Deactivate any questionable vendor accounts, until you are satisfied that the vendor has resolved the issue.



Business Email Compromise

What it is:

- Business email fraud compromises email accounts through phishing, social engineering or malware used to obtain the user's password. Once an email account is compromised, fraudsters begin accessing and reviewing emails, including meeting and calendar information, contact lists and information concerning business partners, vendors and customers.
- This activity enables criminals to interject themselves into normal business communications masquerading as the person whose account was compromised. This stage lasts until the fraudster feels comfortable enough to send wire transfer instructions using either the victim's email or a spoofed email account. Emails are typically sent to an employee with the ability to wire funds.
- A common tactic is to wait until the victim is away on legitimate business travel to send new wire instructions, making it more likely that individual would use email to conduct business and making it more difficult to verify the transaction as fraudulent because the victim is in transit. The request may state that the wire transfer is related to urgent or confidential business matters and must not be discussed with other company personnel.
- For this type of fraud, there is a relatively easy fix: all wire information received via email should be verbally verified using established business telephone numbers.
- Another type of business email compromise is the diversion of payroll funds, where a company's human resources or payroll department receives spoofed emails appearing to be from employees requesting to update their direct deposit information. The new information provided to HR or payroll representatives generally leads to a pre-paid card account. In some cases, prior to the change request, multiple employees have received an email with a spoofed log-in page. When employees enter their usernames and passwords, the hacker gathers and uses employee credentials to access the employees' personal information. This helps make the direct deposit requests appear legitimate.

Business Email Compromise (continued)

How to protect against it:

- Limit the number of employees with authority to handle wire transfers. Mobile authorization tools help limit the number of approvers required.
- Split the duties of initiating and approving transactions like ACH and wire payments into two steps: People who can initiate payments, and those who can approve them. This is often referred to as dual controls.
- Be wary of wire transfers to countries outside of normal business patterns.
- Be careful opening attachments and clicking on links even if the email appears to be from a legitimate source, particularly if you believe wire instructions may be included in the communication.
- Watch for emails that contain significant changes in grammar, sentence structure and spelling compared to previous communications.
- Scrutinize suspicious communications, particularly toward the end of the week or the end of a business day; as the fraudsters will have more time to access and divert funds.
- Maintain a file, preferably in non-electronic form, of existing vendor contact information including telephone numbers to ensure that the invoice or payment you are reviewing is for a vendor you know.
- Look out for “spoofed” email addresses that are made to look like the real addresses. Criminals use tactics like character substitution, addition and omission to make email addresses appear legitimate. Here are some examples using a Bank of Marin address.


The correct email should be **johnroe@bankofmarin.com**.

Examples of “spoofed” addresses:

- roe@bank0fmarin.com
- roe@bankofmariin.com
- roe@bankofmarln.com
- johnroa@bankofmarin.com
- roe.bankmarin@gmail.com

Mobile Banking Security

Mobile banking is convenient and popular, but some customers still have concerns about paying bills and transferring funds by phone. Staying informed on developments and best practices for mobile banking is the most powerful deterrent to mobile banking fraud. By following these easy steps, you can take precautions to safeguard your business and personal banking information:

- Always keep your phone with you, and lock it when it's not in use.
 - If you lose your phone, call your bank promptly and have your password changed or disable your banking application.
 - Choose your password and personal verification questions carefully and never share them with anyone - not even family or friends.
 - Don't keep your password or other sensitive information stored on your smartphone, where it could be discovered if your phone is stolen.
 - Don't send your banking credentials by email or text, which could be intercepted.
 - Review your banking statements frequently and report any errors promptly.
 - Install the most current anti-virus software on your phone, such as Avast, Bitdefender, Kapersky, Lookout, McAfee or Norton.
 - Be aware of the actual URL in links and don't visit sites that you don't know.
 - Choose apps wisely. Obtain them from the official app store for your phone type, since fraudsters may email links to apps that contain malware (software designed to gain unauthorized access to your remote device).
 - Don't follow links in any emails that claim to be from your financial institution. Go directly to your bank's website to do your banking.
- 

Bank of Marin's Fraud Prevention Tools

Our security and fraud prevention tools are designed to keep your business, and your money, safe. From access to authorization, identity to approval, we offer a host of solutions for your security and fraud prevention needs.

These tools are only effective when used properly. We are here to assist you every step of the way. Our dedicated team of banking professionals helps you identify and implement the fraud prevention tools that are appropriate for your business, and that's what sets Bank of Marin apart.

Please contact your local branch with any questions about our Fraud Prevention Tools.

Account Monitoring

Using your account monitoring tools will help to identify any unusual activity.



Digital Banking

Monitor, manage and access your Bank of Marin accounts quickly and securely from your mobile phone or tablet.



Digital Banking Alerts

Personalized daily alerts help you track your accounts and transactions with email alerts customized to your individual requirements.

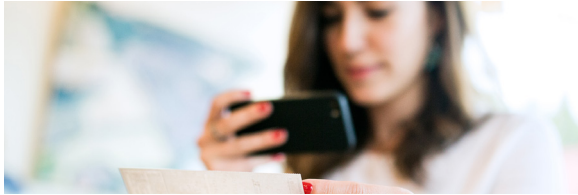
You can also test the effectiveness of your organization's fraud prevention measures by completing the **checklist** found at the end of this guide.

Additional resources and tools for managing organizational fraud risk can be found at [ACFE.com/fraudrisktools](https://www.acfe.com/fraudrisktools)

Bank of Marin's Fraud Prevention Tools (continued)

Account Controls

With multiple controls in place, we put the power to protect your finances right at your fingertips.



Remote Deposit Capture (RDC)

As an alternative to in-branch or ATM check deposits, RDC offers you the flexibility to manage your business on your schedule, under your control, at your location.



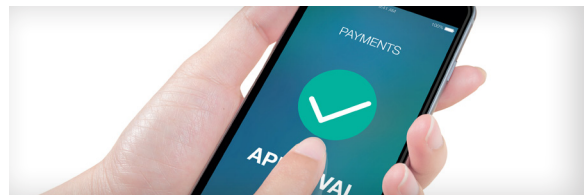
Symantec™ VIP Soft Tokens

Two-factor authentication provides extra security by verifying your device identity through a PIN and then delivering a unique, frequently changing code to your device to verify it is in your possession - keeping remote identity thieves and fraudsters out of your bank account.



Credit Card Controls

Your Bank of Marin business account allows you to set Visa® Payment Controls that limit or restrict employee transactions based on category, location, spending or time. All of these are backed by the Visa Liability Waiver Program, which insures you for up to \$100,000 against eligible losses that might be incurred through card misuse by a terminated eligible card member. No other payment tool offers this level of protection from embezzlement or employee fraud.



Tiered Authorization

Control who has the authority to initiate wires or transfer funds out of your account, and who has access to other banking and account management functions. By managing the number of authorized users, you are better able to keep a handle on outgoing payments.

Bank of Marin's Fraud Prevention Tools (continued)

Transaction Approvals

The best way to avoid fraud is to stop it before it occurs. That's why we offer multiple treasury management tools to approve your transactions, even while on the go, and identify fraudulent attempts before they occur.



Check Positive Pay & Reverse Positive Pay

You provide a list of company-issued checks and Bank of Marin will match to all checks presented, ensuring only approved transactions are completed.

ACH Positive Pay

You establish pre-authorized ACH transaction criteria and review any exceptions before they post to your account, avoiding any unauthorized ACH debits.



Mobile Wire & ACH Approval

Now you can review and approve wire transfers remotely, right from the Bank of Marin mobile app, protecting you from wire fraud.

Fraud Prevention Checklist

1 Provide ongoing anti-fraud training to all employees of the organization.

- ☐ Do employees understand what constitutes fraud?
- ☐ Have the costs of fraud to the company and everyone in it—including lost profits, adverse publicity, potential job loss, and decreased morale and productivity—been made clear to all employees?
- ☐ Do employees know where to seek advice when faced with uncertain ethical decisions, and do they believe that they can speak freely?
- ☐ Has a policy of zero-tolerance for fraud been communicated to employees through words and actions?

2 Create an effective fraud reporting mechanism.

- ☐ Have employees been taught how to communicate concerns about known or potential wrongdoing?
- ☐ Are one or more reporting channels (e.g., a third-party hotline, dedicated email inbox, or web-based form) available to employees?
- ☐ Do employees trust that they can report suspicious activity anonymously and/or confidentially (where legally permissible) and without fear of reprisal?
- ☐ Has it been made clear to employees that reports of suspicious activity will be promptly and thoroughly evaluated?
- ☐ Do reporting policies and mechanisms include vendors, customers, and other outside parties?
- ☐ Do reporting mechanisms include multilingual capabilities and provide access to a trained interviewer 24 hours a day, 7 days a week?

3 Increase employees' perception of detection, using the following proactive measures taken and publicized to employees.

- ☐ Is possible fraudulent conduct aggressively sought out, rather than dealt with passively?
- ☐ Are surprise fraud audits performed in addition to regularly scheduled audits?
- ☐ Are data analytics techniques used to proactively search for fraud and, if so, has the use of such techniques been made known throughout the organization?
- ☐ Do managers actively review the controls, processes, accounts, or transactions under their purview for adherence to company policies and expectations?

4 Ensure the management climate/tone at the top is one of honesty and integrity.

- ☐ Are employees periodically surveyed to determine the extent to which they believe management acts with honesty and integrity?
- ☐ Are performance goals realistic and clearly communicated?
- ☐ Have fraud prevention goals been incorporated into the performance measures that are used to evaluate managers and to determine performance-related compensation?
- ☐ Has the organization established, implemented, and tested a process for oversight of fraud risks by the board of directors or others charged with governance (e.g., the audit committee)?

Fraud Prevention Checklist

- 5** Perform fraud risk assessments to proactively identify and mitigate the company's vulnerabilities to internal and external fraud.
 - ☐ Are fraud risk assessments updated regularly (e.g., annually), as well as following times of notable organizational or environmental changes?
 - ☐ Are the results of the fraud risk assessment shared with appropriate levels of management and used to update the organization's anti-fraud program and controls?
- 6** Instill that the following anti-fraud controls are in place and operating effectively.
 - ☐ Proper separation of duties
 - ☐ Use of authorizations
 - ☐ Physical safeguards
 - ☐ Job rotations
 - ☐ Mandatory vacations
- 7** Ensure the hiring policy includes the following (where permitted by law).
 - ☐ Past employment verification
 - ☐ Criminal and civil background checks
 - ☐ Credit checks
 - ☐ Drug screening
 - ☐ Education verification
 - ☐ References checks
- 8** Ensure the internal audit department, if one exists, has adequate resources and authority to operate effectively and without undue influence from senior management.
- 9** Provide an employee support program to assist employees who may be struggling with addiction, mental/emotional health, family, or financial problems.
- 10** Conduct regular, anonymous surveys to assess employee morale.



Bank of Marin is here to help you protect your business from fraud and cyber-threats.

For more information or to ask a question, contact your local branch or visit www.bankofmarin.com for more helpful tips.



Bank of Marin

BANKOFMARIN.COM | MEMBER FDIC