PROTECTING YOUR BUSINESS

Tips & Tools for Guarding Against Fraud

Bank of Marin

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 $125,000. 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 fraud prevention and the security of our customers' information and finances. The tips and tools we've provided in this guide will help you identify potential gaps in your fraud prevention activities and take actionable steps to protect yourself and your business.

As a business bank, we are committed to making sure all of our customers have the right tools and information to be secure. With the proper protections in place, you can sleep comfortably at night knowing that your business, and your money, are safe and sound.

*2020 Report to the Nation on Occupational Fraud and Abuse.

Bank of Marin

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 everyone 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.

*2020 Report to the Nation on Occupational Fraud and Abuse.

Occupational Fraud

Internal billings schemes are one of the most common types of occupational fraud. Taking the greatest impact are small businesses, which account for 26% of all occupatonal fraud cases at a median loss of $150,000. For small businesses who may have fewer anti-fraud controls in place, billing schemes are easier to pull off and take longer to detect.* We've highlighted some common billing schemes and provided a list of actions you can take to detect and prevent fraud from happening to your business.

Types of Billing Schemes:

Shell Companies

A fictitious company set up as a vendor by a dishonest employee. The employee submits invoices from this vendor to collect payment. In a lot of cases, the person submitting the invoice is also the same person paying the invoice.

Pay & Return Schemes

An employee intentionally pays a vendor twice. The employee then calls the vendor and requests that they send one of the checks back to them. The returned check is then deposited into the employee's bank account.

Personal Purchases

An employee makes purchases using the company credit card or submits bogus expense reports to be reimbursed. This is very common as most managers and owners generally do not closely monitor expense reports and company credit card statements.

What to Look For:

- Unfamiliar vendors
- Vendors that have only a post office box address
- Invoices from vendors who are not on the company-approved vendor list
- Changes in vendor billing account information
- Vendors with company names consisting only of initials - many such companies are legitimate, but fraudsters commonly use this naming convention
- Vendor addresses that also match an employee's address
- Large billings broken into smaller payments

*2020 Report to the Nation on Occupational Fraud and Abuse.

Occupational Fraud (continued)

Prevention Tips:

- Establish an approved vendor list.
- Conduct due diligence on new vendors to make sure they are legitimate.
- Review payments to vendors and look for abnormalities like an excess in payments to one particular vendor.
- Require that detailed receipts are turned in for all credit card purchases and expense report items.
- Set up dual control or create separation of duties so the employee entering invoices is not the same person who also pays the invoices. If this is not an option due to staffing, then the manager should audit the accounts payable list monthly.
- Conduct random audits of paid invoices, company credit card purchases and expense reports.
- Establish a call-back procedure to vendors when they request a change to billing or account information.
- Educate your employees on what to look for, as they are your eyes and ears in an organization.
- Set-up a fraud hotline. Losses from fraud were nearly 50% less at organizations with a hotline.*

Beginning on page 7 of this guide, you will find the Fraud Prevention Tools that Bank of Marin offers to help you take an active role in preventing fraud in your business.

*2020 Report to the Nation on Occupational Fraud and Abuse.

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 reconnaissance 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 requests will sometimes 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.

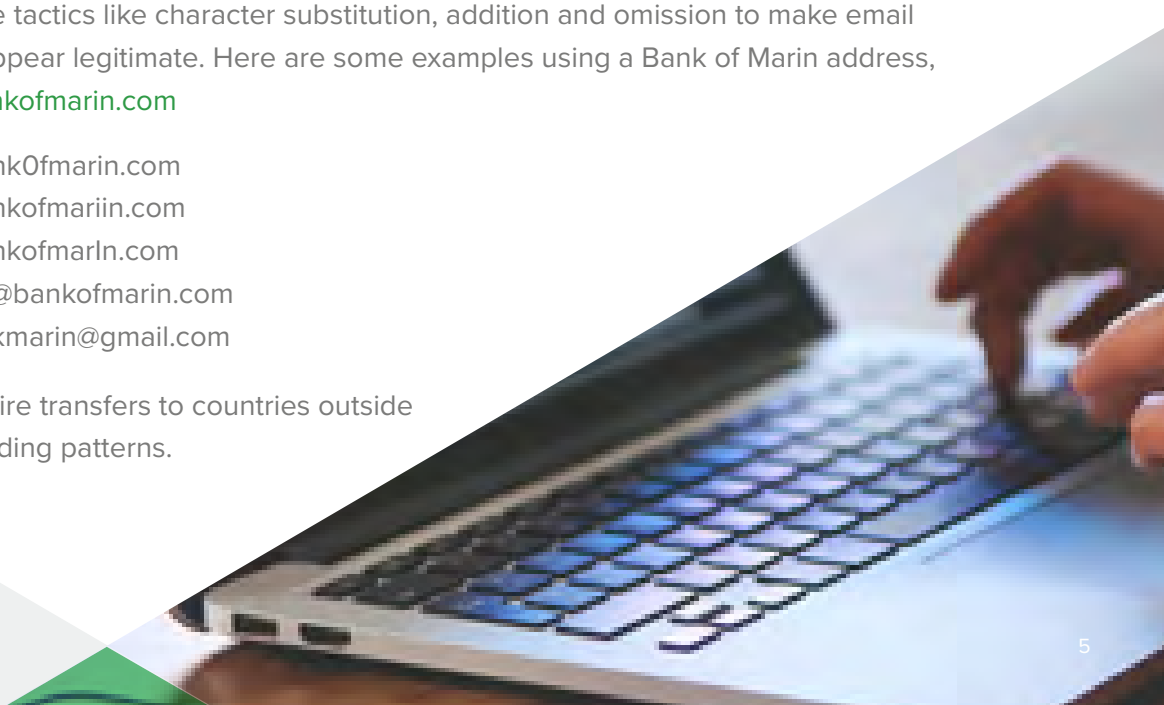
Business Email Compromise (continued)

How to protect against it:

1. Limit the number of employees with authority to handle wire transfers. Mobile authorization tools help limit the number of approvers required.
2. Have a second employee designated as an approver for any wire transfer requests.
3. Implement a callback process in order to have dual authentication from two different communication streams.
4. 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.
5. Look out for emails that contain significant changes in grammar, sentence structure and spelling compared to previous communications.
6. Look out for 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.
7. 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.
8. 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, johnroe@bankofmarin.com

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

9. Be wary of wire transfers to countries outside of normal trading patterns.



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:

1. Always keep your phone with you, and lock it when it's not in use.
2. If you lose your phone, call your bank promptly and have your password changed or disable your banking application.
3. Choose your password and personal verification questions carefully and never share them with anyone - not even family or friends.
4. Don't keep your password or other sensitive information stored on your smartphone, where it could be discovered if your phone is stolen.
5. Don't send your banking credentials by email or text, which could be intercepted.
6. Review your banking statements frequently and report any errors promptly.
7. Install the most current anti-virus software on your phone, such as Avast, Bitdefender, Kapersky, Lookout, McAfee and Norton.
8. Be aware of the actual URL in links and don't visit sites that you don't know.
9. 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).
10. 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 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, and that's what sets Bank of Marin apart. We are here to assist you every step of the way. Our dedicated team of business banking professionals helps you identify and implement the fraud prevention tools that are appropriate for your business.

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

Account Monitoring

With our account monitoring tools, Bank of Marin helps you keep tabs on your finances to identify any unusual activity.

Mobile Banking

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

Online & Mobile Banking Alerts

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

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 online 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 cash management tools to approve your transactions, even while on the go, and identify fraudulent attempts before they occur.

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.

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.

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.

G-PYB 10/20

Bank of Marin