Bank of Marin

PROTECTING YOUR BUSINESS

Tips & Tools for Guarding Against Fraud

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 $150,000. And that median loss amount was similar whether the organization was a large company or had fewer than 100 employees. 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, much more.*

Bank of Marin is dedicated to fraud prevention and the security of our customers' information and finances. The tips and tools contained 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.

*2014 Report to the Nation on Occupational Fraud and Abuse.

Bank of Marin

Anti-Fraud Best Practices for Business Owners

1 Establish Internal Controls

- Limit electronic access to financial information or sensitive documents.
- Create strong and secure passwords, and change them regularly.
- 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.

Billing Fraud Schemes

Billing schemes account for 28.7% of all fraud and is one of the most common types we see. In smaller organizations, billing schemes are easy to pull off due to lack of separation of duties or management oversight. The average time to detect a billing scheme is 24 months, with an average loss of $150,000.*

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
- Vendors with company names consisting only of initials - many such companies are legitimate, but dishonest employees commonly use this naming convention
- Vendor addresses that also match an employee's address
- Large billings broken into smaller payments

*2014 Report to the Nation on Occupational Fraud and Abuse.

Billing Fraud Schemes

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.
- Separate duties so the employee entering invoices into the system is not the same person who also pays the invoices. If this is not an option due to staffing, than the manager should audit the accounts payable list monthly.
- Conduct random audits of paid invoices, company credit card purchases and expense reports.
- Educate your employees on what to look for, as they are your eyes and ears in an organization.

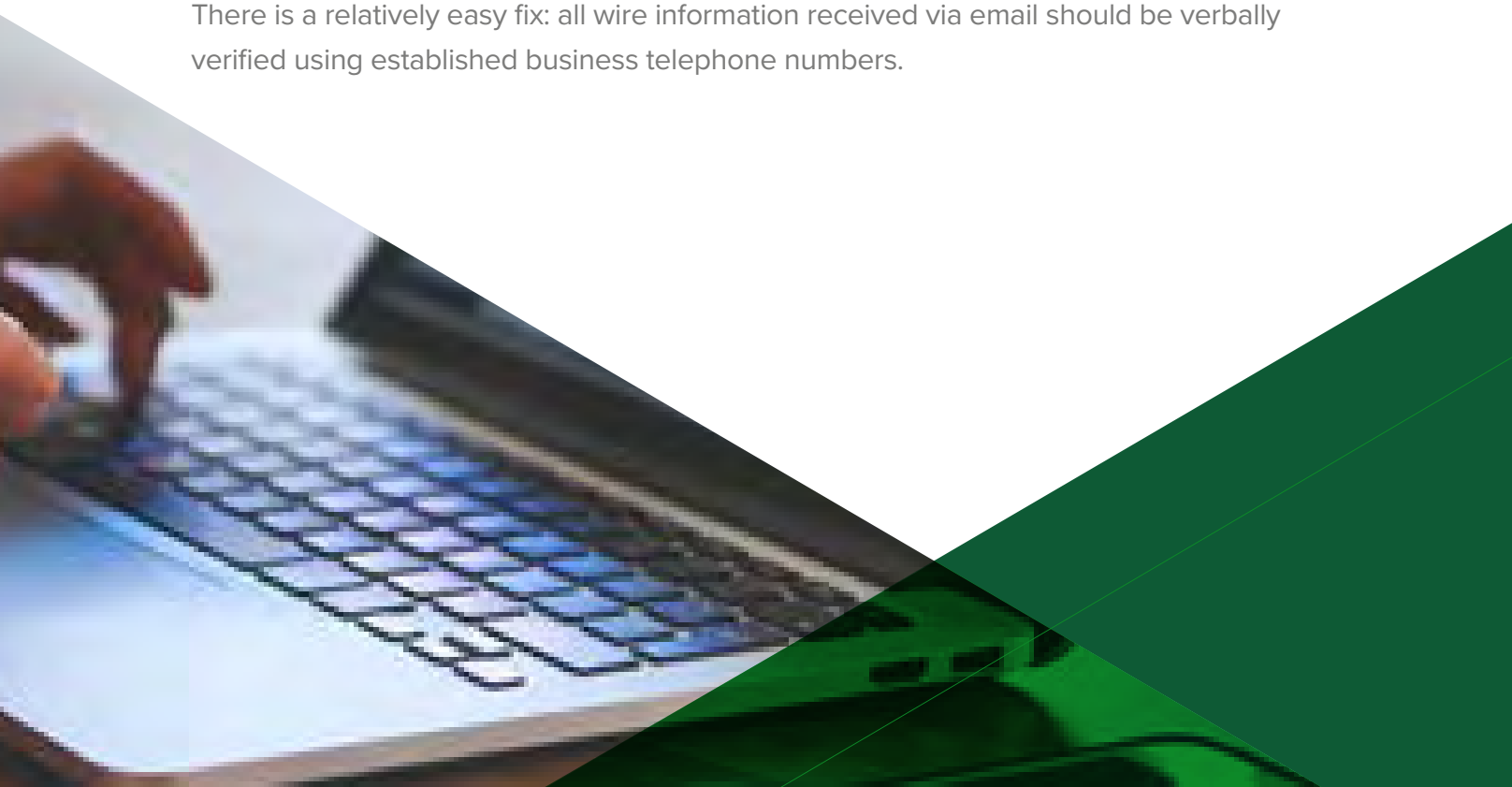
Business Email Compromise

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.

There is a relatively easy fix: all wire information received via email should be verbally verified using established business telephone numbers.



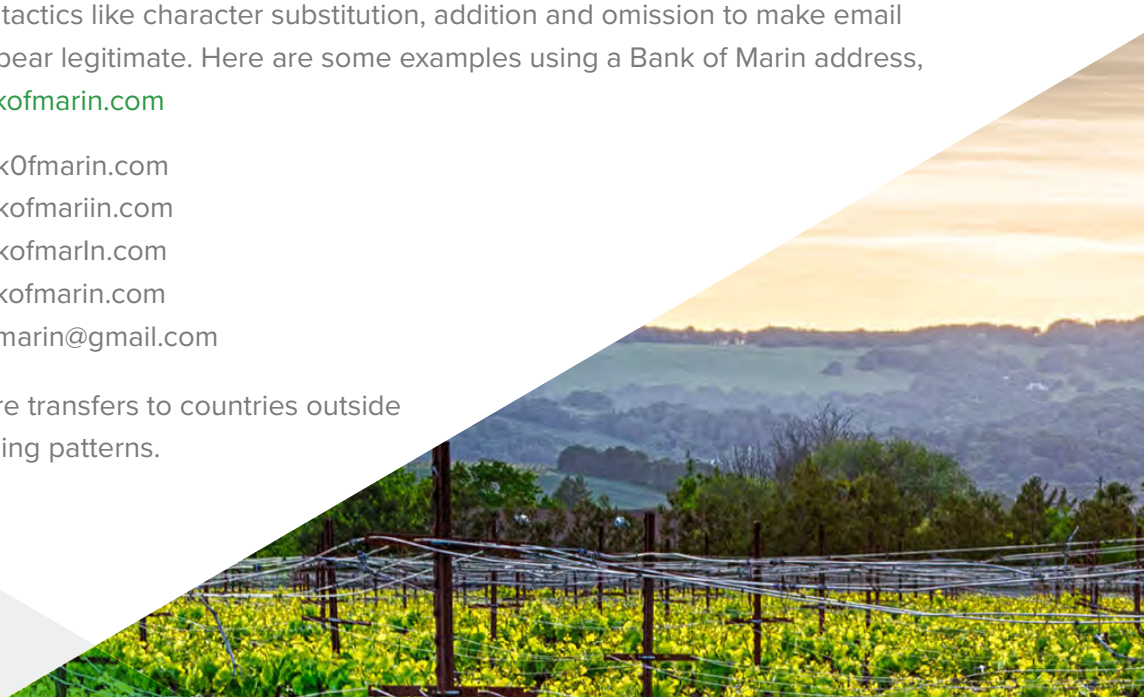
Business Email Compromise

To guard against this type of fraud, here are some suggestions:

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; 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@bankofmarln.com
    - roa@bankofmarin.com
    - roe.bankmarin@gmail.com

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



Mobile Banking Security Tips

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.

FRAUD PREVENTION TOOLS

Bank of Marin 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.

But these tools are only effective if 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 determine the best protections for you and your business, identify the fraud protection tools that are appropriate for you and help you implement and learn to use them.

Monitor

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

Mobile Banking

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

Online Banking Alerts

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

FRAUD PREVENTION TOOLS

Control

With multiple controls in place, Bank of Marin puts the power to protect your finances right at your fingertips.

Remote Deposit Capture (RDC)

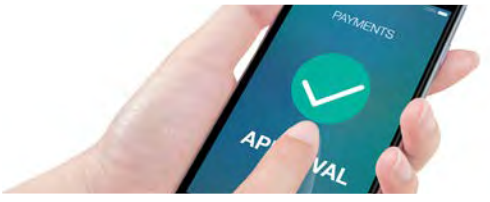
As an alternative to in-branch or ATM deposits, RDC offers you the flexibility to manage your business on your schedule, under your control, at your location.

Security 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 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 tight handle on outgoing payments.

FRAUD PREVENTION TOOLS

Approve

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

Positive Pay & Reverse Positive Pay

You create a file of legitimately issued checks that are reviewed and validated prior to payment, 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 one of the most prevalent types of business fraud.

Bank of Marin

Member FDIC

EQUAL HOUSING LENDER