HANCOCK WHITNEY®

Avoiding Cybersecurity Threats and Payment Fraud

CHECKLIST TO HELP KEEP YOUR COMPANY SAFE

Fall 2020

Security Review Checklist

Most businesses have been targets of cybercrime or payment fraud. However, you can protect your company by implementing strong internal controls. Cyberthieves not only set their sights on fraudulent wire and ACH transfers, but also other types of financial information, especially checks. Below is a checklist highlighting best practices that make it harder for your company to become a target.

Payments Checklist

ESTABLISH STRICT SECURITY PROCEDURES AND LIMITS.

□ Require dual authorization for all wire and ACH transactions

□ Require dual authorization for check and card purchases over set amounts

□ Independently verify vendor changes and require confirmation before paying a new vendor or changing an address

□ Limit the number of people authorized to sign checks

□ Never sign checks in advance

□ Securely store checks, deposit tickets, check printing equipment, remote deposit scanners and endorsement stamps

□ Give users responsible for payments, such as vendors and payroll or executive assistants, cybersecurity training on fraud schemes and company procedures

□ Develop written payment processing procedures for your organization that all employees (and executives) must follow

□ Void remotely deposited checks and destroy them according to bank retention period

□ **Yes, my payments protections are in place**

Online Banking Checklist

ENSURE THE COMPUTERS USED FOR ONLINE BANKING AREN'T COMPROMISED.

□ Use dedicated computers for online banking access

□ Prohibit email or web access for personal use on dedicated online banking computers

□ For online banking access and internal networks, select trustworthy system administrators

□ Limit network administration privileges to those who absolutely need it

□ Do not allow unidentified or unscreened devices into any computer on your network

□ Prohibit USB drives and external devices (they can deliver malware)

□ Do not open links or download software (unless from a trusted source)

□ **Yes, my online banking protections are in place**

Computers, Tablets and Mobile Devices Security Checklist

SET STRICT RULES, POLICIES AND GUIDELINES TO ENSURE THESE DEVICES DON'T OPEN THE DOOR FOR AN ATTACK.

□ Protect all devices with an internet connection with antivirus software and antimalware tools such as Trusteer Rapport

□ Update all applications and software regularly

□ Update security software automatically (if not set to automatically update, then do so immediately)

□ Turn on automatic updates and patches for operating systems and web browsers

□ Do not use unsupported operating systems

□ Wipe old computers' hard drives before they're disposed of

□ Keep seldom-used programs updated (otherwise, delete them)

□ Do not enter private/secure data online unless you're certain you can trust the site

□ **Yes, my payments protections are in place**

E-mail Tips

- □ Delete spam or emails from unknown parties immediately; do not open the email or click on any links in the email
- □ Avoid emailing confidential data
- □ Be extra cautious when opening emails with external addresses. Do not assume an email is OK just because it displays a corporate logo
- □ Be suspicious of every email and review all attachments warily with caution. Attached files and links may contain hidden malware. Hover over a link with the mouse to reveal the real website address
- □ Do not send confidential or personal information by email outside your company
- □ Use Forward instead of Reply. Reply to suspect emails by forwarding the email and selecting the address from your email address book

Password Tips

- □ Never save passwords on websites or browsers
- □ Use strong passwords with 8–10 characters, upper and lowercase letters, numbers and symbols
- □ Create unique passwords for each account
- □ Change passwords often

Mobile Device Tips

- □ Avoid unsecured Wi-Fi and public Wi-Fi connections
- □ Lost or stolen devices (either belonging to an employee or the company) are a risk; programs such as Find My iPhone® can help
- □ Ensure personal devices are backed up often and encrypted
- □ Do not furnish or confirm personal data in reply to a text or email
- □ Antivirus and protective software must be added to personal devices and cannot be disabled
- □ **Yes, my device protections are in place**

Account Access Checklist

TIGHTER CONTROL OF ACCOUNT ACCESS GIVES CYBERTHIEVES A SMALLER, MORE DIFFICULT TARGET.

- □ Restrict user entitlements and review them at least annually
- □ Remove account access for all former employees
- □ Make sure employees aren't sharing IDs, passwords or login credentials
- □ Set up separate administrator and user IDs
- □ Utilize multiple administrators, with separate duties for each
- □ **Yes, my account access protections are in place**

Transaction Monitoring Checklist

KEEP A CLOSE EYE ON ALL YOUR TRANSACTIONS TO SPOT THE FIRST SIGNS OF TROUBLE.

- □ Review all outgoing items (wires, ACH, checks) daily
- □ Use Positive Pay (check and ACH) to identify suspicious transactions
- □ Reconcile all bank accounts every month
- □ Divide duties to ensure the employees issuing payments aren't the same as the employees reconciling bank statements
- □ **Yes, my transaction monitoring protections are in place**

Focus on Cyber-Resiliency

By adopting strong internal controls and procedures, you can help protect your organization and its people. These checklists can help identify the issues you need to focus on when defining your controls. Remember, success is when your controls make it so difficult for the crooks they decide to target someone else.

Five Red Flags of Wire Fraud

The sender places a "rush" request:
Scammers will insist the transfer take place immediately. Resist the hustle.

The sender insists on communicating via email only:
If you can't verify the request, wait.

The requestor—the CEO or executive—is out of the office:
Always verify this request with another executive before sending any funds.

The nature of the request or the amount is unusual or inconsistent with prior experience:
If it is out of the ordinary, definitely be suspicious.

The email address or other details in the request are wrong:
If it looks strange, don't fulfill the request without getting authorization.

Contact Treasury Services Client Support at 866-594-2304 with any questions or for information on preparing your fraud defense.

Access the Hancock Whitney Bank website by typing or bookmarking the web address **hancockwhitney.com.** Never click on links in emails to access our website.

FRAUD DEFENSE
COVER ALL YOUR BASES

- Defend Your Business
- Secure Your Process
- Educate Your Staff
- Protect Your Banking Assets

Hancock Whitney Bank, Member FDIC. Terms and conditions apply.

10/20