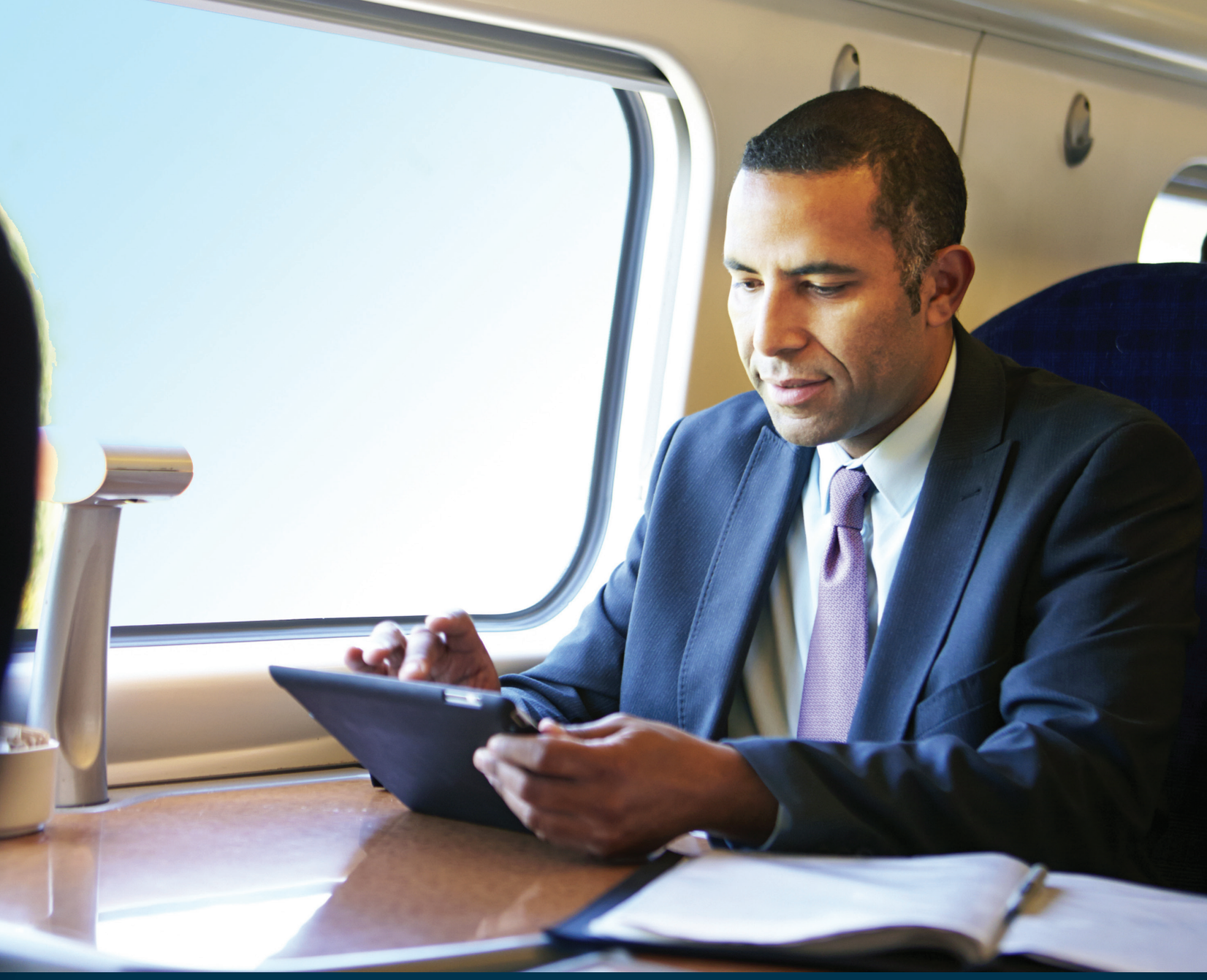

MAKING BUSINESS FINANCIAL SECURITY A PRIORITY

CAPITAL BANK

THE CHALLENGE OF FINANCIAL FRAUD

A typical business
LOSES 5%
*of its revenues every year to fraud.**

That's a median annual loss of
$150,000

SOLUTIONS THAT HELP SAFEGUARD YOUR INFORMATION

At Capital Bank, we understand the constant challenge your business faces in safeguarding sensitive business and account information from fraud attempts. Not only could you lose revenue, but also time working to identify and eliminate check fraud as well as maintain control over ACH and wire transactions. That's why we are committed to offering our customers a higher level of security through innovative products that put you in control. The following is a brief overview of how we can assist you.

OUR SOLUTIONS

WHAT YOU NEED

COMPLETE CREDIT/DEBIT BLOCKS

To help control both check fraud and forgery and electronic fraud, you can completely block all incoming debits and/or credits and enable full control over your account while receiving external transactions. This service streamlines payables and eliminates costly check and paper processing expenses for recurring disbursements. Complete blocks make reconciliation and cash flow forecasting processes easier.

CONTROLLING CHECK FRAUD & FORGERY

LOCKBOX SERVICES

Segregation of duties is a particularly important treasury control issue. Lockbox Services provide you the means to segregate the responsibilities of billing and receiving to prevent "unauthorized" internal losses. Lockbox Image Services offer you paperless workflow solutions that can provide secure, controlled access to a payer's check or remittance documentation containing customer-sensitive data, such as credit card (PCI) or patient health information (PHI).

CHECK POSITIVE PAY

Check Positive Pay is an account reconciliation service offered through Business Banking Online that helps combat check fraud and forgery by matching checks presented for payment against an approved list of checks issued by your business. Those without an exact match will be flagged as suspect and reported to you for a pay/no-pay decision. You may also validate the name of the payee on the check to the name provided in the check issue file as an additional safeguard.

CONTROLLING ELECTRONIC FRAUD

ACH POSITIVE PAY

ACH debits to your account are first compared to existing authorizations you previously set up. Items matching the criteria you establish will be released for payment. Any exception, or ACH debit without a prior authorization on file, will be available for your online review and decision.

PURCHASING CARD

Purchasing card programs can help reduce fraud exposure through electronic payments, automated spending controls, and more efficient reconciliation.

INTERNATIONAL WIRE BLOCK

This is an additional control that can be placed on an account that prevents the release of wired funds to any beneficiary located outside the U.S.

* Association of Certified Fraud Examiners, 2016 Global Fraud Study "Report to the Nations on Occupational Fraud and Abuse," 2016.

WAYS WE SAFEGUARD YOUR INFORMATION

In addition to the services we offer to help protect you from fraud, we are also strongly focused on processes and technology that help us maintain the integrity of your information.

Capital Bank uses and recommends our customers use strong authentication processes to help protect your sensitive information online including:

- **Dual Approval Method** – Businesses use this risk control to help prevent the unauthorized release of payment transactions by requiring two separate individuals to approve changes to user entitlements, beneficiaries, and payment instructions.
- **Verification Method** – This method requires verification of the transaction to be taken offline from the web browser, such as through telephone or SMS text message.
- **Set Limits** – Customers can establish limits for online banking transactions they deem appropriate.
- **Security Tokens** – Tokens provide an additional layer of security, requiring the login process to include a user name, password and token when initiating ACH and/or wire transactions.
- **SHA-256 TLS Encryption with Extended Validation (EV) Certificates** – Data exchanged between the customer and the bank is encrypted using some of the highest levels of encryption available from trusted certificate authorities. Certificate authorities take extra steps to validate the recipients of digital certificates. Validation is indicated by a green font on your address bar, providing customers an extra measure of confidence in the website's identity and protection against fraud.

Our external-facing applications are protected from malicious attacks against our servers by firewalls and intrusion detection systems. These solutions not only help protect our applications from hackers but also detect intrusion attempts and alert us.

YOUR BUSINESS BENEFITS

- Improved control and security with the ability to make pay/no-pay decisions on potentially fraudulent items.
- Convenient access to our tools through our secure Business Banking Online application.
- Lower costs through reduced fraud exposure and potential losses associated with electronic payment fraud.
- Reduced work-hours as a result of reviewing items before they travel through the banking system.

WHAT YOU CAN DO TO PROTECT YOURSELF

Here are some important steps you can take to strengthen your own account security.

- Conduct reconciliation of all banking transactions on a daily basis.
- Initiate ACH and wire transfer payments under dual control, with a transaction originator and a separate transaction authorizer.
- Familiarize yourself with Capital Bank's account agreement and with your liability for fraud under the agreement.
- Stay in touch with other businesses to share information regarding suspected fraud activity.
- Immediately notify and escalate any suspicious transactions to Capital Bank, particularly paid checks, ACH or wire transfers. There is a limited recovery window for these transactions and immediate notification and escalation may prevent or minimize loss.

Employ best practices to secure computer systems including the following:

GENERAL SECURITY PRACTICES

- Be wary of phishing email scams that attempt to gather sensitive information or deploy malware.
- Do not click on links or attachments in unknown or suspicious emails. This is how most malware is introduced.
- Use dedicated PCs for sensitive online transactions.
- Establish a password-protected screensaver set to activate after some period of inactivity.
- Use bookmarks or saved links to access Online Banking.
- Log off and close browser windows of websites when you are finished.
- Shred sensitive data and use secure shred bins.
- Consider hiring security professionals to test your security procedures and offer training programs.
- Be cautious of emails that appear to be a vendor or customer requesting a change in payment information. **Any changes** from **any email** should always be authenticated by performing a callback verification to the vendor/customer's telephone number on file.

LOGGING IN

- Create a strong password with at least 10 characters that includes a combination of mixed case letters, numbers and special characters.
- Try not to use words found in the dictionary. Instead use the 1st characters from a poem, phrase or song you remember substituting and adding numbers, letters and symbols.
  Example: My Son Loves to Play Soccer and Football > M$L2PSaF
- Prohibit the use of "shared" usernames and passwords for online banking systems.
- Use a different password for each website that is accessed.
- Change the password a few times each year.
- Never share username and password information for online services with third-party providers.

FIREWALL/SECURITY SOFTWARE

- Install and maintain a dedicated, actively managed network firewall and/or and intrusion/prevention system.
- Consider engaging a Managed Security Service Provider to safeguard your network.
- Install commercial anti-virus and desktop network firewall and/or an intrusion prevention system software on all computer systems.
- Make certain computers are patched regularly, particularly operating systems and key applications with security patches.
- Block or limit the use of social media sites (Twitter, Facebook, etc.) on PCs used to conduct financial transactions.
- Confirm backups have completed successfully and that the data is available on the backup media.

KEEP WHAT YOU'VE WORKED HARD TO EARN

For more information on strengthening the security of your bottom line, contact your Relationship Manager or Treasury Management Services Officer.