CommercePayments™

Strategies for Fraud Mitigation

General Internet Security

- **Browsers:** Always sign-out when finished using any online application and close the browser. Use the most current version of a recommended browser that is both compatible with the applicable Commerce Bank product and supports Secure Sockets Layer (SSL) protocol and 256-bit encryption. Apply any updates to your computer's operating system and your browser as often as they are made available. Contact Commercial Customer Support at 800.207.0886 for details regarding browser compatibility with Commerce Connections®, and 800.892.7104 for ControlPay® Advanced.

- **Patch Management Policy:** Ensure your company has an established Patch Management Policy and that it covers third-party client software such as Adobe, Flash and Java. Ensure that all third-party software is updated with the latest security patches. Install new security patches as soon as your operating system and Internet browser manufacturers make them available.

- **Phishing-Business Email Compromise (BEC):** An increasingly common, sophisticated scam, targeting businesses that regularly perform electronic payments. The scam is carried out by compromising business email accounts through calculated social engineering or computer intrusion techniques to conduct unauthorized transfers of funds. In 2018, the FBI reported over $12.5 billion in loss to such scams. Organizations should evaluate their processes for electronic payments. Some recommendations to avoid becoming a victim include:

  1. Call to verify payment requests received through email. Do not call any number contained within the email and do not reply to the email. Call the requestor directly at a number you have on file.

  2. Train employees to identify these scams.

  3. Verify changes in vendor payment location and confirm requests for transfer of funds.

  4. Be careful when posting financial and personnel information to social media and company websites. This information can be used to craft the phishing email to make it more believable.

  5. Regarding wire transfer payments, be suspicious of requests for secrecy or pressure to act quickly.

  6. Scam emails are frequently sent from email domains that are a slight variation on the company name they are attempting to impersonate, and at a quick glance may look authentic. If possible, register all Internet domains that are slightly different than the actual company domain.

  7. Conduct social engineering testing, including phone and email, to test the effectiveness of your security awareness training program.

- **Email Security:** Automate scanning of attachments and URLs within email in a Sandbox before delivering to corporate email system for Zero Day malware detection. Also Implement Spam Filtering on inbound email to block unsolicited email that may contain malicious URLs. Implement email authentication technologies, such as Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting and Conformance (DMARC).

  Always beware of email asking for personal or login information. Train employees to recognize phishing emails and how to identify potential threats in email and instant messages, in addition to recognizing malicious sites through web browsing. Although fraudulent email can be difficult to recognize, beware of emails that:

  1. Request that you click a link which could take you to a spoof website – one that looks like a real company website and may even include the real company's official graphics and design.

  2. Ask you to give, confirm, or update sensitive personal information, such as Social Security numbers, usernames, passwords, PINs, or account numbers. Commerce will not ask you to enter (or record) personal or account information via email.

  3. Use pop-up windows for entering or confirming personal data.

  4. Have a sense of urgency asking you to provide the information immediately, citing a specific event that might happen if you fail to respond. For example, the email may state that your account may be closed or suspended temporarily.

  5. Contain spelling errors and/or bad grammar. Intentional spelling errors may allow the email to bypass spam filters used by Internet Service Providers (ISPs).

If you receive one of these email messages, do not open any attachments or click on any links in the email.

These emails are not authentic, and the links may contain Trojans which could jeopardize your online banking. If a user clicks on a link, please contact Commercial Customer Support immediately at 800.207.0886 for Commerce Connections®, or 800.892.7104 for ControlPay® Advanced.

- **Secure Location:** Position those computers used to transact business in a secure location. Try to keep computers away from public areas and beware of opportunities for "shoulder surfing" where unauthorized persons might view transactional activity on a computer screen.

- **Dedicated PC:** Commerce strongly recommends that your company have dedicated computers for online financial transactions, with all email and other web browsing capabilities blocked from those dedicated computers.

- **Time-Out:** Utilize the "time-out" feature available for your computer. Set the screen to revert to a screensaver after a specified number of minutes of inactivity and require a password to log back in. Never leave computers unattended while using any type of online banking services.

- **Password Protection:** Remind users to maintain strict confidentiality of login/authentication credentials, e.g., IDs, passwords, PINs, and (if applicable) fobs. These credentials should only be used as required during the normal login/authentication process. A Commerce representative will never request (nor has any reason to know) your login/authentication credentials for any reason, whether through email, via phone, text, or other method. Never respond to a request to disclose these credentials (other than using them to complete the normal login/authentication process), but please contact Commerce immediately if you receive such a request. Don't share or post IDs, passwords, or PINs or use "guessable" IDs, passwords, or PINs. Disable automatic password-save features in the browsers and software you use to access the Internet. Commerce also recommends that you set a reminder to change your passwords periodically, and that you use a unique password for each website.

- **Encrypted Applications:** When using applications that require login credentials and/or process sensitive data, such as Commerce Connections® and ControlPay® Advanced, always ensure "https://" is in the address bar just prior to the website address. Commerce Bank employs encryption technology such as Extended Validation (EV)-SSL certificates to encrypt the transmission between your browser and Commerce as well as help you verify you're at our site (look for the green or blue address bar).

Commerce Bank Web Based Applications Security

- **Separation of Duties in Commerce Connections®:** Commerce strongly recommends that you designate different individuals as your Security Administrator and System Administrator. This separation of duties can help mitigate the chance for internal losses due to fraud. Commerce also requires two System Administrators for most System Administration functions: one Administrator to input the change and a second Administrator to approve the change. If you do not already separate these functions, please refer to your Commerce Connections® User Manual or contact us for additional information.

- **Restrict User Access:** Assign users access to only the applications/modules and accounts each user requires for his or her specific job function. Immediately delete or modify all authorities upon employee termination or a change in duties. If the departed employee is enrolled in Enhanced Security within Commerce Connections®, contact Commerce immediately upon their departure/reassignment so Commerce can disable the Enhanced Security user. Review user access on a regular basis to ensure unauthorized users have not been added to the system, and that authorized users have not been granted unnecessary permissions.

- **Utilize the Controls in Commerce Connections®:** Various modules within Commerce Connections® provide companies with an opportunity to limit exposure and require secondary review and approval of funds transfer activity. These controls are integral to the security of your financial transactions and we cannot emphasize enough the need to incorporate them into your operational procedures. Controls available to reduce your risk of fraud include:

  1. Transaction, user, account and daily limits for various types of transactions. These may be established and systematically enforced to limit your exposure and allow for the proper separation of duties among your employees.
  2. Review of wire transfers and ACH activity by a second authorized user. Again, the separation of duties in a funds transfer environment can mitigate the opportunities for fraudulent activity and reduce the opportunity for errors.
  3. Administrative Dual Approval. Most System Administration requires two System Administrators: one Administrator to input the change and a second Administrator to approve the change.

- **Read and React to messages in Commerce hosted applications:** Commerce will periodically post messages inside of Commerce Connections® and ControlPay® Advanced with important information relating to security and threats. We strongly advise that you carefully and promptly review these messages and respond accordingly.

Mobile Devices Security

- **Conducting Business financial transactions:** Use devices that follow your organizations security policies, enforced through an enterprise mobile device management solution. Do not circumvent security features or otherwise "jailbreak" your mobile device. Wipe or securely delete data from your mobile device before you dispose of it.
- **Access: Never** access bank accounts from cafés, public Wi-Fi hotspots, or hotspots not controlled by you. Only download applications from trusted App Stores.
- **Encryption:** Ensure encryption is turned on for your mobile device.
- **Protection:** Mobile devices should be password protected and auto lockout should be enabled. Ensure your device has current anti-virus software and all operating system and application updates and patches. Firewalls should be enabled if possible. Keep your mobile devices with you always or store them in a secured location when not in use.
- **Wireless access:** Bluetooth, Wi-Fi, etc., on the mobile device should be disabled when not in use to prevent unauthorized wireless access to the device.

Operational Security

- **Verify Transactions:** Always carefully and thoroughly verify transactions for authenticity and promptly reconcile accounts. If you receive a request from a vendor to change routing information for an electronic payment, you should authenticate the request to ensure it is legitimate by performing a call-back to a number you already have on file, as caller IDs and email addresses can be spoofed. Commerce offers same-day reporting for most types of transactions and encourages companies to verify activity as quickly as possible during the banking day. If you believe any transactions are in error or were unauthorized, please contact Commerce immediately.
- **Separation of Duties:** Commerce recommends a separation of duties between the individual verifying activity/reconciling accounts and the staff person(s) with authority to originate transactions. The verifier/reconciler should not be given system authority to originate transactions.
- **Dual Controls:** Commerce recommends that dual control approvals are completed from separate computers. Known malware is designed to capture multiple users' credentials on the same computer. Commerce also requires initiation of electronic payments under dual control: one person authorizes creation of the electronic payment and a second person authorizes the release of the payment.

These Strategies assume that your organization has a commercially-reasonable base security infrastructure in place. Furthermore, these Strategies should not be your organization's sole means of protection against fraud losses, but rather they should be included as part of a more comprehensive program implemented by your organization to identify, mitigate, and insure against potential risk from fraud losses. Even if complied with in its entirety, these Strategies do not guaranty against becoming a victim of fraud. This is only an attempt to provide some commonly-accepted practices that may help reduce the likelihood that you become the victim of fraud. Commerce Bank, which is not holding itself out as a security consultant or expert, makes no guaranty, warranty, or representation of any kind as to the results that you may achieve by following the Strategies and disclaims any liability related thereto. The term Strategies does not mean or imply that these practices are a definitive or uniformly-accepted compilation of optimal security practices.

For questions related to Commerce Connections® security, please contact your Treasury Services officer or Commercial Customer Support at **800.207.0886.**

For questions related to ControlPay® Advanced, please contact your account manager or Commercial Card Client Care Center at **800.892.7104.**

Commerce Bank™
Member FDIC

Challenge Accepted.®