COMPEER FINANCIAL®

PROTECTING YOURSELF FROM FRAUD:
BEST PRACTICES

Fraud comes in many forms, from phishing scams to identity theft. Arm yourself with knowledge and learn how to spot and avoid common threats and scams before they happen.

Preventing Invoice/Wire Fraud

✓ **Verify Payment Requests**
Always double-check the legitimacy of payment requests, especially if they involve changes to vendor information or payment methods.

✓ **Confirm Contacts**
Independently verify the identity of the sender before making any payments, particularly if the request is unexpected or seems suspicious.

✓ **Train Your Team**
Educate your team about the risks of invoice and wire fraud and establish clear protocols for verifying payment requests.

Preventing ACH Debit Fraud

✓ **Secure Account Information**
Safeguard your account and routing numbers to prevent unauthorized electronic withdrawals.

✓ **Monitor Transactions**
Regularly review your account statements and activity for any unauthorized debits or suspicious transactions.

✓ **Limit Access**
Restrict access to sensitive financial account information and provide account details only to trusted individuals or entities.

Preventing Check Fraud

✓ **Use Secure Checks**
Invest in high-security checks with features such as chemical voids or security inks to deter counterfeiters.

✓ **Secure Check Stock**
Store blank checks in a secure location and limit access to authorized personnel only.

✓ **Monitor Check Clearing**
Track issued checks and reconcile them with cleared transactions to detect any discrepancies or fraudulent activity.

PROTECTING YOURSELF FROM FRAUD: BEST PRACTICES

Page 2

Preventing Impersonation Scams

✓ **Verify Requests**
Independently verify any requests for sensitive information or financial transactions, especially if they come from high-ranking executives or unfamiliar sources.

✓ **Double-Check Identities**
Scrutinize email addresses and domain names for subtle differences or irregularities that may indicate spoofing or impersonation.

✓ **Confirm via Multiple Channels**
Before taking action on any request, confirm its legitimacy through multiple communication channels, such as phone calls or in-person meetings.

Best Practices for Online Security

✓ **Use Strong Passwords:** Create complex passwords and change them regularly.

✓ **Enable Two-factor Authentication:** Enhance security by enabling two-factor authentication wherever possible.

✓ **Be Cautious of Public Wi-Fi:** Avoid sharing sensitive information over public Wi-Fi networks.

✓ **Shred Documents:** Regularly shred documents containing personal information.

✓ **Monitor Your Credit Report:** Check your credit report for any suspicious activity.

Compeer Financial’s Approach to Preventing Fraud

As a financial services provider, Compeer Financial employs robust security measures to safeguard the information of our clients, including:

Identity Verification
We verify your identity before processing any requests involving account changes or transactions.

Secure Online Portal
Our online portal utilizes secure codes and locks down after multiple incorrect attempts, ensuring your account remains protected.

Secure Messaging
We use encrypted messaging to communicate sensitive information, mitigating the risk of interception by hackers.

Team Member Training
Our team undergoes regular training to stay updated on the latest security protocols.

Stay vigilant and proactive in protecting your financial information. By following these best practices, you can reduce the risk of falling victim to fraud.