ANTI-FRAUD AND CYBERSECURITY BEST PRACTICES CHECKLIST

Help Strengthen Your Defense Against Fraud and Cyber Threats

As digital transactions become standard, the risk of fraud and cybercrime continues to grow. Businesses must proactively implement safeguards to help protect against both internal and external threats.

Account Structure

- ☐ Create separate accounts for payroll and operations.
- ☐ Establish dual account audit/reconciliation processes.

Transaction Protection

- ☐ Review and reconcile all accounts daily and monthly.
- ☐ Formalize policy and procedures for the destruction of private documents.
- ☐ Establish employee transition and termination procedures that include login credentials and passwords.
- ☐ Maintain ACH and wire transfer limits for both the organization and each user.
- ☐ Verify any changes in payment instructions through a known associate, using a phone number you have on record.
- ☐ Implement dual control for initiating and approving transactions.
- ☐ Never use the same computer to initiate and approve transactions.

Device Best Practices

- ☐ Keep operating system and other software up to date. Don't forget programs like Java®, Adobe®, and web browsers (Firefox®, Chrome®, Safari®).
- ☐ Establish guidelines to help secure password utilization. (strong password design, privacy, and periodically updated)
- ☐ Understand the risks of using "cloud" based applications.
- ☐ Uninstall programs that are not used or unnecessary.
- ☐ Require auto-locking computers after a period of inactivity.
- ☐ Implement a firewall.
- ☐ Back up servers (real time if possible)
- ☐ Install Anti-Virus, Anti-Malware and Anti-Spyware software. Keep these systems up to date, and scan for issues regularly.
- ☐ Install an Anti-Malware browser plug-in.
- ☐ Enable SIM Protection: This added layer of security helps prevent SIM swap fraud, which can lead to account takeovers and financial loss.

Internet Browsing Best Practices

- ☐ Do not install software from unknown sources.
- ☐ Do not click on web advertisements or 'pop-ups'.
- ☐ Do not open attachments on unsolicited e-mails. Contact the sender to verify before opening the attachment.
- ☐ Log off online accounts that are not currently being utilized.
- ☐ Implement policies restricting internet access based on need and content.
- ☐ If possible, use a dedicated computer for processing bank transactions. Use a separate computer to check e-mails and browse the Internet.

Internal Operations

- ☐ Use dual authorization for all bank transactions, including wire transfers, online ACH originations, ACH direct transmissions, and remote deposit.
- ☐ Set policies regarding passwords that include: alphanumeric passwords, different passwords for different applications, change often.
- ☐ Require system administrators to have different accounts/passwords from their regular user accounts.
- ☐ Conduct surprise audits.
- ☐ Separate employees to initiate/approve transactions and audit the monthly bank statement.
- ☐ Conduct employee training that helps employees understand the issues.
- ☐ Have a disaster contingency/incident response plan in place.

Banking Services*

- ☐ Require dual authorization when utilizing bank services.
- ☐ Use Check Positive Pay to help protect against check fraud.
- ☐ Help stop fraudulent ACH transactions by using our ACH Positive Pay service. With this service, you can control electronic withdrawals from your account.
- ☐ Predetermine amounts authorized ACH originators can debit accounts by using ACH debit filters.
- ☐ Use alerts to be notified of account changes and activity.

If you believe you responded to or received a fraudulent email, contact Online Banking Support at 800-840-4999 (Mon - Sat, 6:00 a.m. - 9:00 p.m. MT.). Also, forward any emails that you believe are fraudulent to abuse@amegybank.com.

If you suspect that someone has gained access to important personal information, such as your bank account number or your Social Security Number and may use that information for illegal purposes or to withdraw money from your account, call 800-840-4999 (Mon - Sat, 6:00 a.m. - 9:00 p.m. MT.).

*Some Treasury Management products are subject to credit approval and agreement. Contract and fees may apply. Contact Amegy Bank Treasury Management or go to **www.amegybank.com/business/treasury** for more information on Banking Services offered by Amegy Bank.

NOTIFY YOUR BANK IMMEDIATELY IF YOU SUSPECT FRAUDULENT ACTIVITY.

CONTACT INFORMATION:

www.amegybank.com/business/treasury

Amegy Bank®
Here, You Grow®