FRAUD PROTECTION CHECKLIST

STAY PROTECTED

ALERUS

In today's digital age, businesses face ever-evolving threats from cybercriminals seeking to exploit vulnerabilities for financial gain. To protect themselves and their clients, businesses must implement robust fraud protection measures. This list demonstrates some of the many guidelines to help you protect your business and clients from cyber threats and maintain a secure environment for your operations.

Technology

- □ Ensure software, hardware, operating systems, and browsers are up to date with security fixes.
- □ Use reputable antivirus, anti-malware, and anti-spyware software and keep them updated.
- □ Utilize and keep firewalls and intrusion detection and response systems updated.
- □ Password-protect wireless networks and keep guest or client Wi-Fi separate.
- □ Secure networks and devices with passwords and encryption.
- □ Implement strong passwords and enable multi-factor authentication (MFA).
- □ Restrict software installations to administrative users only.
- □ Regularly backup data and test backups for reliability.
- □ Be cautious of downloading suspicious apps or files.

Physical Security

- □ Secure buildings with locks and alarms.
- □ Secure remote deposit capture (RDC) systems and check storage.
- □ Follow secure document management procedures.

Logical Security

- □ Encrypt data.
- □ Use multi-factor authentication.
- □ Limit application access to essential functions.
- □ Implement transaction controls and dual approval processes.
- □ Follow stringent password security parameters.

Employee Training

- □ Train employees on handling sensitive information and identifying scams.
- □ Educate employees on identifying common scams and handling sensitive information.
- □ Restrict access to sensitive areas and enforce clean desk policies.
- □ Properly destroy sensitive documents and establish document retention policies.
- □ Avoid reusing passwords across sites; consider using a password manager.
- □ Think before clicking or sharing sensitive information online.
- □ Be cautious with social media privacy settings and app permissions.
- □ Ensure your home Wi-Fi is password protected.
- □ If possible, refrain from using personal devices for business purposes.
- □ Lock or sign off computer when not in use.

Cybersecurity on the Go

- □ Avoid public Wi-Fi; use a VPN if needed.
- □ Don't use public charging cords or USB ports.
- □ Create and save bookmarks for important websites.

This list is not inclusive of all fraud protection practices and is intended to help recognize, prevent, and report potential fraud.