PROTECT YOUR SMALL BUSINESS FROM FRAUD

Preventing Fraud

Worksheet to Provide a 360 Degree View for Small Businesses

REGIONS NEXT STEP FOR BUSINESS

ARE YOUR FUNDS BEING TRANSFERRED SECURELY?

ARE YOU LOSING REVENUE TO FRAUD?

ARE YOU KEEPING COMPANY INFORMATION PRIVATE?

ARE YOU RECEIVING PHISHING EMAILS AND MALWARE ATTEMPTS?

ARE YOU AWARE OF THE LATEST FRAUD TRENDS?

ARE YOUR VENDORS LEGITIMATE?

ARE YOUR INTERNAL CONTROLS STRONG ENOUGH?

PROTECT YOUR SMALL BUSINESS FROM FRAUD

Preventing Fraud

Checklist of Best Practices for Small Businesses

REGIONS NEXT STEP FOR BUSINESS

PAYMENTS

1 Reconcile to spot abnormal activity

- Reconcile your accounts in a timely manner.
- Segregate your accounts by purpose, type, and/or payment method.

2 Place stop payments on any checks that have been lost or stolen

3 Convert paper payments to electronic payments

For Employees

- Use Automated Clearing House (ACH).
- If an employee does not have a bank account, offer to deposit their pay directly to a payroll card that allows them to use it like a bank debit card.

For Vendors

- Pay via ACH or purchasing card.
- Use wire transfers for high-value or time sensitive payments as well.

4 Securely store check stock, deposit slips and bank statements, then destroy securely

5 Use Positive Pay

This powerful tool allows you to send information to your bank about the checks you've written so that when checks come in to pay, they are matched to what you've told them. Positive Pay is also available for ACH. If you've authorized a supplier or other partner to draft money from your account you can pre-approve these transactions.

INTERNET BANKING

1 Use dual control for transaction initiation

- Use Wire and ACH.
- Use email alerts for approvals.

2 Reconcile your accounts daily to look for fraudulent activity.

3 Use a secure environment

- Use a dedicated PC.
- Limit web surfing.
- Use firewall, anti-virus, anti-malware, anti-spyware.

4 Use strong passwords and protect them

- Create passwords that are **not easy to guess.**
- **Change your password** at least every 60 days.

****

- **Keep your passwords secure**. Do not store a list of passwords or keep them near your computer. Do not share passwords or login with anyone.
- **Be careful of social engineering.** Know that the bank will never call you to ask you for your ID or password.

5 Beware of your email

- **Do not click on links** that look suspicious.
- **Be aware of advertising scams for virus scanners** showing what looks like a real virus scan of your computer.
- **Never click a popup that states software needs to be installed/purchased** to solve a problem.
- **Be aware of banner ads.** They are being used by hackers to hide malware that can be installed on a PC without the user ever clicking on them.

RESOURCES

Regions: regions.com/stopfraud

Internet Crime Complaint Center: www.ic3.gov

NS1039FW-IMP (3/18)