First Interstate Bank

Fraud Awareness and Prevention Checklist

Although we would like to think that fraud always happens to the "other guy", the fact is that fraud can happen to anyone and may even be perpetrated by someone you know and trust. No business is 100% safe from fraud; however you can take steps to minimize the chances of it happening to your business. Please take a few minutes to review the tips provided and then take measures to implement as many as possible. Remember, you don't have to implement every tip, but the more you can put in place, the safer your business will be.

Transaction Controls

- Review and reconcile accounts daily and monthly.
- When possible, convert paper payments, i.e. checks to electronic formats.
- Secure your check stock and manage under dual control if possible. Never sign blank checks in advance of payments.
- Secure your workplace by deterring non-employees from accessing files, including trash bins.
- Set up a separate computer with no access to email or web surfing for online banking. This small investment will possibly save you thousands of dollars in the long run.
- Sign up for free electronic I-Statements to prevent your banking information from being stolen in the mail.

Anti-Malware

- Exercise extreme caution when confronted with any request to divulge account information or banking passwords. First Interstate Bank will never ask you for password information.
- Immediately report any account transactions that you question.
- Never leave a computer unattended while logged into online banking.
- Never access bank or sensitive sites at Internet cafes, public libraries, etc.

Antivirus and Spyware Software

- Do not open attachments in an email if the subject line or email itself looks suspicious or is unexpected.
- Do not download from unfamiliar file-sharing sites
- Update your antivirus software regularly and set it to run daily and automatically.
- Install a firewall as a first line of defense against hackers.

Internal Controls

- Use dual control for all monetary transactions, including ACH originations, wire transfers and bill pay.
- Set policies for regarding password security:
  - same passwords are not used for different applications
  - passwords are not easy to guess: i.e. pet names, birthdates, children's names
  - passwords contain a combination of letters, numbers and special characters
  - passwords are changed at least every 60 – 90 days

Every layer of security that you put in place today will help protect your business. Don't wait until it's too late. Start taking control of your security to insure that your business is safe from fraud.