Servis 1st Bank Best Practices

Credit Card Security Tips

Bad actors are after all the credit card data in your organization's system. It only takes one mistake to put all that data at risk. Below are some practices to help you keep your card data safe:

Paper Documents

- Lock up documents containing credit card information
- Properly destroy card data, following your organization's guidelines
- Use a delivery service or carrier that provides tracking information
- Never store card data for longer than six months unless you are legally required to do so

Working Remotely

- Keep your software up to date
- Never visit unknown websites
- Only use your work system for work
- Lock and secure your device when not in use
- Always use an organization approved Virtual Private Network (VPN), which creates a safe internet connection that shields your online activity from the bad guys

Mobile Devices

- Use a passcode or biometric lock
- Never text full cardholder information
- Never take or send a picture of credit card information
- Use a dedicated phone or tablet for taking card information
- Use a validated card reader that encrypts card data

Electronic Documents

- Never save full card numbers, only the last four digits; software can search for 16-digit number sequences
- Never store the three- or four-digit security codes
- Avoid storing on removable media, like thumb drives, whenever possible
- Never send full card numbers over a public network without using encryption (the process of scrambling the information to make it unreadable)

Stay Alert!

- Notify security if you notice any oddities or evidence of device tampering
- Report any strange system messages or weird behaviors on your device to IT
- Stay aware of your surroundings; you never know who might be listening to your conversations or watching what you do
- Never share card data with unauthorized individuals
- Never reuse passwords or create passwords containing personal information
- Always verify links or attachments are legitimate before interacting with them
- Check your account and card activity daily for any discrepancies
- Always verify verbally with the sender if you receive a request for information or changes

What to Do If You Suspect Fraud

If you suspect fraud, immediately notify your ServisFirst Bank account officer.
The sooner you contact the bank, the higher the chances of getting your funds returned.

Servis 1st Bank®

For more information on how to protect your organization, please visit www.servisfirstbank.com/fraud-prevention-education/.

Please contact Cash Management with any questions at 866.922.5794 or contact your local banker.