# Debit Card Fraud Tips and Lost Card Contact Information

THE GIFFORD STATE BANK

**Debit Card Information Travel Tips**

If you plan to use your debit card while traveling outside the US, please notify us of the following to help minimize disruption in your service:

*Travel Dates
*Destination
*Current Cell Phone Number
*Increased Point of Sale or Cash Limit Needs

**Important Phone Numbers**

*The Gifford State Bank **217-568-7311**

*Shazam **800-383-8000**
(To report a card lost or stolen after banking hours)

*Shazam Falcon Fraud Protection **866-508-2693**
(To help with card fraud after banking hours)

**When shopping at retail stores**

**We recommend running your Gifford State Bank debit card as a debit using your 4 digit PIN**, rather than credit which only requires a signature.

**When Shopping online**

**Online retailers often require an email address to register at their website**. If a website is compromised, criminals can leverage your email account to hack your other e-commerce accounts.

**Use a single card for all online purchases to minimize your risk to one account.**

Monitor your payment account regularly for unauthorized purchases or other charges.

**Beware of phishing ads or pop-ups for "amazing" deals.**

Hackers often set these to install malware on your computer when you click. The thieves could also be trolling for information, payment account credentials or other personally identifiable information (PII) used to steal your identity.

**Don't shop online using public computers or networks.**

Libraries, food courts and coffee shops are dangerous places to do online business. Bad guys may have installed key loggers, sniffers or other malware designed to steal your information.

**Keep your computer and browser up to date with the latest patches and software.**

**Shop at reputable sites and be sure the sites you visit are legitimate.**

Cyber criminals can create website URLs that look very similar to the real websites to fool shoppers. For example: A scam site could be called hxxp://www.amaxon.com and be set up to look exactly like Amazon.com. The scam site can then steal any information you enter at the site, such as your Amazon.com login credentials or your payment card number. Pay close attention to the browser's access bar before entering any sensitive information, and move your mouse pointer over any link that directs you to a shopping site to make sure the link takes you to a legitimate website.