FRAUD ALERT!

Important information about the recent increase in cybercrime and fraud attempts.

Avoid falling victim to cybercriminals.

Scammers and cybercriminals look for opportunities to take advantage of the vulnerable, especially during times of emergencies or natural disasters. We are seeing a large increase in the number of scams happening due to the Coronavirus Pandemic with scammers attempting to gain access to personal information like account and routing numbers, user names, passwords and social security numbers using phone calls, phishing emails and fraudulent websites. In some cases cybercriminals are asking that you click on links or download documents which could potentially install malicious software on your computer to steal sensitive information.

Remember these guidelines to stay safe.

- Be aware of what appear to be emails and links from the Centers for Disease Control and Prevention (CDC) and the World Health Organization (WHO) that will redirect you to fraudulent websites asking for your user name and password.
- The Federal Deposit Insurance Corporation (FDIC) is also warning consumers that scammers are fraudulently posing as representatives. The FDIC will never contact you requesting personal information.
- Check the sender's email address and make sure that the source is legitimate.
- Don't click on links from any unfamiliar sources.
- Ignore offers for vaccinations or treatments for Coronavirus.
- Ignore links and deceptive claims about new Coronavirus outbreaks in your area.
- If you receive a phone call requesting any personal information, hang up immediately.
- Do not respond to any communication regarding government stimulus checks or any other government relief program.
- The government will never ask you to pay a fee upfront for any stimulus or relief check, there are no fees or charges of any kind to receive these funds.
- The government will never contact you for personal information like your Social Security Number, bank account number or credit card information.
- Be hyper-vigilant regarding any donations and requests for cash, gift cards or requests to wire money. If you choose to donate to a charity or a cause, do some research to make sure you're absolutely certain they are a legitimate entity.

We're here to help.

If you feel you've been the victim of fraudulent activity, Call us. We'll work with you on reporting the incident to make sure your financial life is healthy and safe. Because this situation is evolving moment-by-moment we encourage you to regularly check our website for updates. We're here to protect your financial life, so you can protect what you value most.

Be assured.

Please be assured that your money is safe with us. It's important to remember that your money is insured by the Federal Deposit Insurance Corporation (FDIC) up to $250,000 for each depositor, per insured bank, for each account ownership category.

We offer online and mobile banking through our Glacier Family of Banks Mobile App for customers with checking, savings and loan accounts.

None of us have faced circumstances like today's, but we're here to work through it together, the way neighbors do. Banking is a community asset, and we're offering the community the strengths of our business.

- View your account balances, statements and transactions.
- Pay bills.
- Transfer funds.
- Make loan payments.
- Set up email and text alerts.
- Deposit checks with the Glacier Family of Banks Mobile App.

For more information on services that we provide to assist you in online banking, fraud alerts, mobile banking, and more, please contact your local branch.

Member FDIC