Reducing the Risk of Fraud and Scams in the Zelle Network

With digital baking on the rise, fraudsters are busy increasing their attacks on customers. While we work hard to protect your account, we have included tips and best practices to help you remain vigilant when using Zelle. Keep in mind, we will never call you to request that you send money, ask for account information, or approve a transaction.

Tips & best practices against Fraud

- Your financial institution will never call you to request information you received via text (sms)
- Don't provide your account number or personal information by email or text
- Don't trust caller ID; Caller ID may be modified to show your financial institution's name
- Don't feel pressured to provide information immediately in response to requests via text, email, or phone. Using their published phone number, reach out to confirm that the request is legitimate
- Don't give information over the phone if you receive a call stating that a transaction is canceled, even if the caller claims to be from your financial institution. Once again, contact your financial institution using a published phone number to inquire about the transaction.
- Don't click on links in unsolicited emails or texts
- Don't give an unsolicited caller remote access to your computer

Scam and Fraud related to COVID-19

- Be aware of charity scams that claim to help COVID-19 victims and their families, along with investment schemes involving research for the development of a vaccination.
- Some scammers claim to be from medical organizations that have a COVID-19 vaccination and require over-the-phone payments to reserve a dose.