First Carolina Bank | BM Technologies, Inc.



Keep your account and your refund safe—don't share your information!

At BM Technologies, Inc., your school's partner for refund disbursements, account security is a high priority of ours. Please note, we will never contact you and ask for information such as your account password, PIN, or debit card number via email, text, or phone. We will only ask for your one-time passcode (OTP) if you call us directly. If someone asks for this information, immediately hang up or disregard and report it to us at 855-398-7260.

The BM Technologies, Inc. Team

Please keep an eye out for these red flags when you are receiving communications regarding your financial accounts:

- **Unsolicited calls, texts, or emails**—We will not make unprompted calls or send unprompted emails regarding your refund. The only texts you can expect from us are refund status updates (if you subscribed to them) and OTPs.
- **Urgent or threatening language**—Scammers often pressure you to act immediately.
- **Requests for personal information**—We will never ask for your PIN, passwords, or full account number via phone, email, or text.
- **Suspicious links, attachments, or QR codes**—Be cautious of unexpected links or downloads. Hover over links to check their destination before clicking. For QR codes, visit a known domain instead of scanning.
- **Unfamiliar sender addresses**—Look for slight misspellings or random numbers in email addresses (like "support@bankk.com").
- Unexpected payment requests—We will not ask you to send money, especially via wire transfers or gift cards.
- Login or verification requests—Avoid clicking links to "verify your account"—go directly to refundselection.com instead.
- Caller ID spoofing—Don’t trust phone numbers alone; scammers can fake them to look legitimate.