Date: [Insert Date]

Subject: IMPORTANT: Urgent Security Alert Regarding Your Account

Dear [Customer Name],

We are writing to alert you of a recent increase in fraudulent activities involving phishing and spoofing that target our customers. Your security is our top priority, and we want to ensure you have the information needed to protect your personal and financial information.

What is Phishing and Spoofing?

- **Phishing:** Scammers send fraudulent emails or text messages (SMS) designed to trick you into revealing sensitive data like passwords, PINs, or account numbers.
- **Spoofing:** Scammers disguise their phone number or email address to make it appear as though the communication is coming directly from [Bank Name].

How to Protect Yourself:

- **Verify the Source:** We will never ask for your password, PIN, or one-time passcode (OTP) over the phone or via email.
- **Do Not Click Links:** Avoid clicking links in unsolicited emails or texts. Instead, type our official website address directly into your browser.
- **Check for Urgency:** Be wary of messages that create a false sense of urgency or threaten to freeze your account immediately.

What to do if you suspect a scam:

If you receive a suspicious call, email, or text claiming to be from [Bank Name], please do not respond. Contact us immediately using the official number on the back of your debit/credit card or by visiting our official website at [Insert Website URL].

If you believe you have already shared your information with a suspicious source, please call our Fraud Department at [Insert Phone Number] right away.

Thank you for being a valued customer and for staying vigilant against fraud.

Sincerely,

[Bank Name]
Customer Security Department