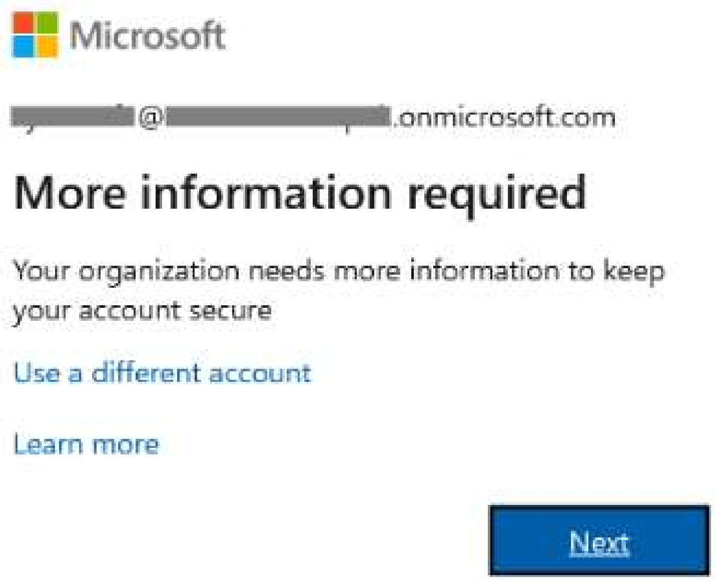
Multi-Factor Authentication (**MFA**) has been enabled on your Goodwin University account.

This will greatly improve the security of your organization as a whole, and help keep your data safe.

Upon logging into your account, you will be prompted to provide Microsoft with more information. (see below)



Microsoft

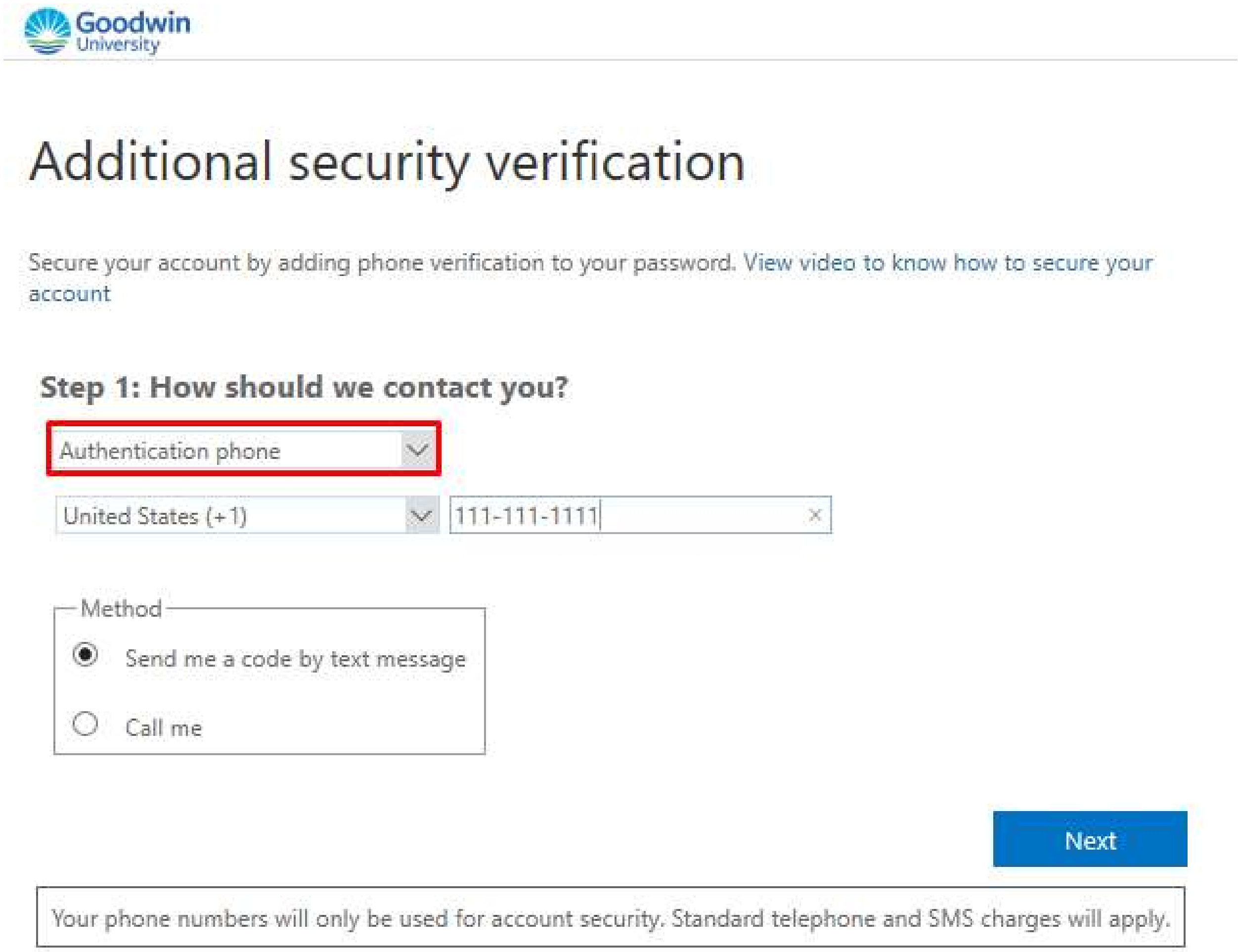
[redacted]@[redacted].onmicrosoft.com

More information required

Your organization needs more information to keep your account secure

You are required to opt into one of the following methods of identity verification.

1) Being sent a SMS text message containing a 6-digit code sent to a **cellphone number** of your choice (most common choice)
2) Receiving a phone call to a phone number of your choice (the most time consuming / inconvenient)
3) Downloading the **Microsoft Authenticator app** to your cellphone (iOS or Android) and receiving a pop-up notification asking to Approve or Deny your login. (quickest method)



Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account

Step 1: How should we contact you?

Authentication phone

United States (+1) 111-111-1111

Method

● Send me a code by text message

○ Call me

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

Choose a verification method from the drop-down list (Authentication Phone is selected in the drop-down above)

Click Next -> A verification code will be sent to your cellphone to finalize the MFA setup.

Microsoft will send you a SMS text message each time you sign in from a **NEW** device/network*. *(You may be sent a code if you sign in from a new network such as a coffee shop, even though you're using the same laptop you always login with.)

Each device that you sign in on will retain its authentication status for 14 days.

If you sign into your Goodwin Email or Office365 portal at least once in 14 days, you will not be sent a verification code.