



## Response to Unsolicited Social Security Numbers

In cases where an email is received which contains SSN or other high risk confidential information (such as an individual bank account or credit card number), users should first determine whether the SSN is needed or not.

1. If the SSN has been provided and is *not necessary*, respond (not including the original message) with the following response:

"I am not permitted to receive SSN or credit card numbers in unencrypted email. I have deleted your message. Please re-send with no SSN or credit card number."

2. If the SSN has been provided and *is necessary*, respond (not including the original message) with the following response:

"I am not permitted to receive SSN or credit card numbers in unencrypted email. Following standard Harvard practice, I have destroyed your original message containing this information.

You may re-send using the right process, which is to transmit this information by XXXX."

As appropriate, decide which of the following will be XXXX, the most suitable process. The message back to the sender should just provide one way to do the transfer.

- Fax to a secure attended location
- Send by US postal mail
- Provide in phone call
- Use a secure file transfer method (e.g. Accellion)
- Provide via encrypted file; call me at xxx.xxx.xxxx to provide the password

Following standard Harvard practice, I have destroyed your original message containing this information."

3. Note: International transactions that require high risk confidential information must only take place through use of secure file transfer (e.g. Accellion), faxing to a secure attended location, or via encrypted file, e.g. Winzip.