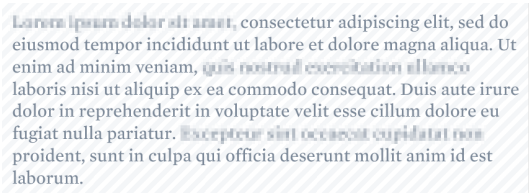
Passing Data Securely to Ascent360

Customer data security is our #1 priority.

We hold ourselves to strict standards and expect our clients to uphold their end of data security best practices. This includes taking extra precautions when passing data back and forth.

Below is a list of best practices to remember when passing us data:

1. **Never send PII (Personally Identifiable Information) over email.**
    - Use a screen-grabbing tool such a Greenshot to obfuscate PII
    - 
    - If you have a file with PII in it, upload it to **Integrate > File Management** (or to your pre-configured SFTP folder). Please see Dropping and Retrieving Files with File Management.
    - Examples of PII include but are not limited to:
        - First Name
        - Last Name
        - Postal Address
        - Other Geographic Information
        - Email Address
        - Phone Numbers
        - Birthdays
        - Demographic Information
2. **Never send passwords or API Key credentials over email.**
    - Use a secure note, such as Privnote, to send us passwords, API keys, or other important credentials. Please see Open or Send a Privnote.