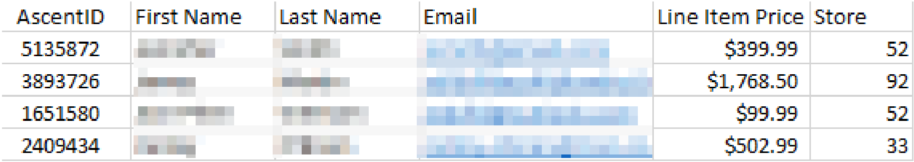
Data Security Best Practices

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. We ask our clients to abide by these best practices, too.

Best practices for data security:

Never send PII ("Personally Identifiable Information") or Credentials via email.

- Use a screen-grabbing tool such a Greenshot to obfuscate PII



AscentID	First Name	Last Name	Email	Line Item Price	Store
5135872	[redacted]	[redacted]	[redacted]	$399.99	52
3893726	[redacted]	[redacted]	[redacted]	$1,768.50	92
1651580	[redacted]	[redacted]	[redacted]	$99.99	52
2409434	[redacted]	[redacted]	[redacted]	$502.99	33

- If you have a file with PII in it, please upload it to File Manager. Never send the file in an email or ticket.
- Examples of PII include but are not limited to:
  - Names, particularly when paired with data below
  - Postal Address, Email Address, Phone Number
  - Birthday or other Demographic data
- For sending us API Tokens, API Keys, or other necessary credentials, please use a secure note, such as PrivNote. Read more here.

In case you're skimming this article... **Please never, ever send us files w/ sensitive information via email.**

ALWAYS upload files with customer data to a secure location (such as our in-platform File Manager).

Stay Safe from Phishing

- **Verify Before You Click:** If you receive an email that appears to be from us, double-check the sending domain to make sure it’s legitimate.
- **When in Doubt, Reach Out:** If something feels off, contact our team at support@ascent360.com — we’re happy to confirm.
- **We’ll Do the Same:** If we’re ever unsure about a request that comes from your side, we’ll reach out directly to verify it’s really from you.

Audit who has access to your account.

- **Regularly Review User Access:** Especially when roles change or team members leave.
- **Use Role-Based Permissions:** Give each team member access only to the data they need.

Educate Your Team

- **Train Regularly:** Make sure everyone understands how to handle data securely.
- **Stay Informed:** Security threats evolve — keep up with best practices and updates.

Password Reset & Login Updates

- **Secure Password Resets Only:** For your security, we no longer send new passwords via email or support tickets — even via services like PrivNote. To reset your password, please use the “Forgot Password” option on the login page.
- **SSO Now Available:** Want a smoother, more secure login experience? We now support Single Sign-On (SSO) so your team can authenticate using your own systems — no password setup required. Let us know if you’d like to enable this for your domain.

If you ever have a question or concern about data security, please contact us.