

Data Security & Fraud Reduction

Maximize Your Data Security By Using PayTrace

Use PayTrace To Maximize Your Data Security:

Allow PayTrace to take the burden of storing sensitive customer data off of your shoulders by storing your data in our high security facilities. In addition, all customer payment account numbers are immediately encrypted upon entry in to the system and not viewable again in their complete unmasked form. PayTrace is Certified with the Payment Card Industry Data Security Standards (PCI DSS), giving you confidence that we're a robust solution to your growing information security needs.

- PayTrace's data centers employ numerous security features, including:
 - Fully redundant and geographically remote data centers to ensure your data is safe from catastrophe and available when you need it.
 - 24/7 on-site staff monitoring physical and electronic network access.
 - 24 hour video surveillance with a 60 day minimum retention policy.
 - Three factor authentication required for access.
 - Visitors are escorted by authorized personnel at all times.
 - Built to be resistant to explosions, and other penetration threats.
- PayTrace has been PCI DDS Certified since 2005, and completes an on-site physical audit annually in order to maintain it's PCI Certification. To learn more about PCI Certification, please visit: <https://www.pcisecuritystandards.org/>

Manage Your Staff's Access To Customer Data With PayTrace:

Create as many log-in profiles as you need and grant each user permissions on a need-to-know basis. Additionally, make sure only the proper people are accessing your data with multi-factor authentication log-ins. You may further lock down access by creating Internet Protocol (IP) Address rules to limit access to one or more computers. You may also track transactions within the software by user, allowing effortless follow-up when needed.

Use PayTrace To Eliminate The Need To Touch Payment Data:

Utilize one of PayTrace's Shopping Carts or the API Secure Checkout to allow your customers to enter their own payment information. Customer entered payment information may be used to process a real-time transaction and/or stored to process future repeat transactions. This functionality allows your staff to process payments without ever seeing or touching the customer's sensitive data. In addition, fraud prevention tools such as Address Verification System (AVS) and Card Security Code (CSC/CVV) are available to help prevent fraudulent payments.

The secure advantage.

<https://PayTrace.com>