***SYNERGY CO-PARENTING SOLUTIONS, LLC***

PO BOX 80241

PORTLAND, OR 97280

[rfox@synergycoparentingsolutions.org](mailto:rfox@synergycoparentingsolutions.org)

[malter@synergycoparentingsolutions.org](mailto:malter@synergycoparentingsolutions.org)

CREDIT CARD RECURRING PAYMENT AUTHORIZATION

I authorize Synergy Co-Parenting Solutions, LLC (Synergy) to charge my credit/debit card for services provided to me per the agreement on file. I authorize charges to be made concurrent with the services provided at the hourly rate per the signed agreement. The card will be charged after each service is provided. This authorization will expire upon written notice of the cardholder to Synergy, or upon termination of services with Synergy, provided there are no funds owing.

Card Number\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ EXP \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

CVV\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name on Card\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Address \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ZIP\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

RECEIPT REQUESTED? Y/N EMAILED OK? Y/N

SIGNED\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

PRINTED NAME \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

DATE \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

I agree to $\_\_\_\_\_\_\_\_\_\_ to be charged on this card on a \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ basis until my balance of \_\_\_\_\_\_\_\_\_\_\_\_\_ is paid in full.

OR

I agree to allow my monthly balance to be paid in full on this card for services provided to me by Synergy Co-Parenting Solutions, LLC.

If you permit recurring transactions, you must (i) obtain your customer’s consent to periodically charge the customer on a recurring basis for the services purchased; (ii) retain this permission for the duration of the recurring services and provide it upon request to us, Processor or the issuing bank of your customer’s Card; and (iii) retain written documentation specifying the frequency of the recurring charge, the duration of time during which such charges may be made and the amount or range of amounts that may be charged. You must not submit any recurring transaction after receiving: (a) a cancellation notice from your customer (so long as such notice was timely provided at least three (3) days prior to the transaction date); or (b) notice from us, Processor or any Card Brand that the Card is not to be honored. In your transaction data, you should include an electronic indicator that the transaction is a recurring transaction. You will promptly notify us in the event you learn that cardholder information has changed with respect to a customer that is currently subject to recurring charges.

You may not suggest or require that your customers waive their right to dispute a card payment transaction.

2.14 Receipts. You must make a written receipt available to your customers for any transaction greater than fifteen dollars ($15.00). You may give your customers the option to receive or decline a written receipt. As a convenience, but not in lieu of a written receipt, you may also offer electronic receipts for delivery through email to your customers.

PCI DSS requires that you implement and maintain certain data security policies and procedures. As of the date of this Agreement, PCI DSS mandates that you comply with the following requirements:

1. Install and maintain a network firewall to protect Cardholder Data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.
3. Protect stored Cardholder Data.
4. Encrypt transmission of Cardholder Data across open, public networks.
5. Protect all systems against malware and regularly update antivirus software or programs.
6. Develop and maintain secure systems and applications.
7. Restrict access to Cardholder Data by business need to know.
8. Identify and authenticate access to system components.
9. Restrict physical access to Cardholder Data.
10. Track and monitor all access to network resources and Cardholder Data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security for all personnel.

As part of the above, you must not, and will ensure that your Merchant Suppliers do not, store any portion of the magnetic-stripe data subsequent to the authorization of a sales transaction, nor any other data prohibited by the Card Brand Rules or the Bank Rules. You or your Merchant Suppliers must not store CVV2 data at any time.