

Credit Card Authorization Requirements Checklist

One Time Transactions	Recurring Transactions
<p>Telephone <i>Your Responsibility</i></p> <ul style="list-style-type: none"> <input type="checkbox"/> Get verbal permission <p><i>PaySimple Does For You</i></p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Email receipt 	<p>Telephone <i>Your Responsibility</i></p> <ul style="list-style-type: none"> <input type="checkbox"/> Get verbal permission <p><i>PaySimple Does For You</i></p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Email schedule confirmation <input checked="" type="checkbox"/> Email receipt for each transaction <input checked="" type="checkbox"/> Send email on schedule change
<p>Written <i>Your Responsibility</i></p> <ul style="list-style-type: none"> <input type="checkbox"/> Get signed authorization form <input type="checkbox"/> Give customer copy of signed form <p><i>PaySimple Does For You</i></p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Email receipt 	<p>Written <i>Your Responsibility</i></p> <ul style="list-style-type: none"> <input type="checkbox"/> Get signed authorization form <input type="checkbox"/> Give customer copy of signed form <p><i>PaySimple Does For You</i></p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Email schedule confirmation <input checked="" type="checkbox"/> Email receipt for each transaction <input checked="" type="checkbox"/> Send email on schedule change
<p>Online <i>Your Responsibility</i></p> <ul style="list-style-type: none"> <input type="checkbox"/> Enter Terms & Conditions on web form configuration screen <input type="checkbox"/> Enter Contact Information on web form configuration screen <p><i>PaySimple Does For You</i></p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Display printable online confirmation page <input checked="" type="checkbox"/> Email receipt 	<p>Online <i>Your Responsibility</i></p> <ul style="list-style-type: none"> <input type="checkbox"/> Enter Terms & Conditions on web form configuration screen <input type="checkbox"/> Enter Contact Information on web form configuration screen <p><i>PaySimple Does For You</i></p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Display printable online confirmation page <input checked="" type="checkbox"/> Email schedule confirmation <input checked="" type="checkbox"/> Email receipt for each transaction <input checked="" type="checkbox"/> Send email on schedule change.

*What PaySimple Does For You assumes that you have entered a valid email address for your customers, not altered any default email settings, and have enabled email notification for each transaction or schedule.

The Importance of Properly Authorizing Credit Card Transactions

Obtaining the proper authorization for your credit card transactions, in conjunction with implementing strong fraud prevention policies, are the most important steps you can take to protect yourself against disputes, return fees, and chargebacks.

Authorizations for credit card transactions are designed to protect both you and your customers. They provide a record of your customer's approval of a transaction, and they enable you to prove to your processor and to the card issuer that you had permission to process a transaction in the event that your customer later claims the transaction was not authorized.

Implementing security policies and card authorization procedures designed to detect fraudulent transactions before they are processed prevents the significant time involved in defending a chargeback and saves you the substantial fees assessed for chargebacks (not to mention the money you lose on the original transaction itself).

While taking these steps will not 100% protect you from chargebacks, (your customers can still ask that a charge be reversed because they claim that the product or service received was not as advertised), they can go a long way towards significantly reducing them by minimizing the risk that your transactions will be challenged as fraudulent or not authorized, and providing you the proof you need to defend a transaction should it be questioned.

The following sections provide guidance on how to obtain the proper authorization for one time and recurring credit card transactions, and tips on using the fraud prevention tools available to you as part of PaySimple.

Also provided are authorization form templates that can be customized for your business when it needs to obtain written authorizations. When using the templates, enter your business information in all the red entry fields—for example where you see **<Insert Business Name>**, you would remove that text, type your business name, and change the font color to black.

You'll find more details and handy templates in each section of the guide. Simply select the type of authorizations you'll be doing:

- [One-Time Mail & Telephone Authorization Guide](#)
- [One-Time Online Authorization Guide](#)
- [Recurring Telephone Authorization Guide](#)
- [Recurring Written Authorization Guide](#)
- [Recurring Online Authorization Guide](#)
- [Fraud Prevention Guide](#)

How to Authorize One-Time Mail & Telephone Credit Card Transactions

Credit card orders received via mail or over the telephone are known as card-not-present transactions, which means that you do not physically have the card in hand when authorizing the payment.

One-Time Telephone Transaction Authorizations

Typical Uses: One time telephone transactions are typically used when a customer is making a purchase over the phone, or paying a bill over the phone. For example:

- Ordering an item from a catalog
- Making a payment on an invoice received in the mail
- Leaving a deposit on a large purchase that will be completed in person at a later date.

How to Authorize:

1. Get verbal authorization over the phone from you customer
2. Send a receipt via email or regular mail

PaySimple provides three options for sending email receipts:

- **Quick Payment Form:** enter your customer's email address in the *Email Receipt To* field
- **Credit Card Payment (in Process Payments Center):** check the *Send Receipt* box in the *Email Notifications* section.
- **Email Receipt Function:** click any linked *Transaction ID* and use the *Email Receipt* button at the bottom of the *Transaction Details* page.

One-Time Mailed Transaction Authorizations

Typical Uses: One time mailed authorizations are often used as part of a contract or order form when a customer is making a single payment for product or services rendered. For example:

- Making a down payment when a contract is signed
- Mailing an order for goods from a catalog
- Making a charitable donation

How to Authorize:

1. Have your customer sign and date a form that includes
 - a. The amount of the payment
 - b. The date the payment is to be processed
 - c. The credit card account number and expiration date from which the payment is to be debited.
2. Keep this form on file, in digital or paper form, for at least one year.
3. Send a receipt via email or regular mail

PaySimple provides three options for sending email receipts:

- **Quick Payment Form:** enter your customer's email address in the *Email Receipt To* field
- **Credit Card Payment (in Process Payments Center):** check the *Send Receipt* box in the *Email Notifications* section.
- **Email Receipt Function:** click any linked *Transaction ID* and use the *Email Receipt* button at the bottom of the *Transaction Details* page.

Templates Provided: [One Time Credit Card Payment Authorization Form](#) --Use this form to authorize a ONE-TIME payment.

[Combination One Time/Recurring Credit Card Payment Authorization Form](#)

Use this form to authorize a ONE-TIME payment, or a recurring payment of the SAME amount each time with an OPEN end date.

How to Authorize One-Time Online Credit Card Transactions

Online credit card transactions are by definition those that are authorized by a consumer entering payment information into a web form, actively checking a box to agree to the terms and conditions for the transaction (pre-checked boxes are not allowed), and clicking a Submit button.

Typical Uses: Online orders for good or services, or online bill payments. For example:

- Purchasing an item from an online store
- Ordering an e-book
- Paying rent
- Making a charitable donation

How to Authorize:

1. Include the information specified below in your terms an conditions
2. Enable your customer to view and print a receipt immediately after submitting the web payment form.
3. Email a receipt for the transaction.

The following information must be included on your Online Payment Form (in the terms and conditions section, or elsewhere):

- Name of your Business
- Your business website address
- Official business mailing address
- Phone number answered during regular business hours
- A complete description of the goods/services being purchased
- Your Return, Refund, and Cancellation policy
- Your delivery policy and order fulfillment policy (if applicable)

What PaySimple Does For You: The web payment forms you create as part of your PaySimple system automate most of the authorization steps for you, including automatically generating a transaction confirmation page and emailing a receipt. To complete the process, you need to do the following:

1. When configuring your web form, add the following text to the **Terms and Conditions** field, in addition to your company's standard terms and conditions. Enter your business information in place of the red insert indicators.

I authorize {insert company name} to charge the credit card indicated in this web form, for noted amount on today's date. This payment is for {insert description of goods/services}. I understand that returns, refunds and cancellations are {insert your policy here}. I certify that I am an authorized user of this credit card and that I will not dispute the payment with my credit card company, so long as the amount corresponds to the terms indicated in this web form.

2. In the **Contact Information** section of the **Payment Form Configuration** screen, be sure to enter your main business address and a phone number and email address that is monitored during regular business hours.

Should your customer ever request a copy of the receipt, you can print a copy or email a copy from the **Transaction Details** page (accessed by clicking a linked **Transaction ID**)

How to Authorize Recurring Telephone Credit Card Transactions

You are permitted to authorize recurring schedules that debit a credit card account over the phone. Note that this is different from an ACH schedule, which CANNOT be authorized over the phone. The authorization requires that your customer understand the conditions under which the business is permitted to debit the account (such as amount, date, and frequency), as well as conditions for termination or change of the authorization.

Typical Uses: There are three typical uses for recurring credit card transactions transaction:

- Payments for the same amount on a regular schedule, such as weekly or monthly service fees.
- Payments for a different amount on a regular schedule, such as utility bills.
- Payment plans for discharging a large debt, such as installment payments on a large purchase.

Recurring Telephone Transaction Authorizations

How to Authorize:

1. Get verbal authorization over the phone from your customer to authorize the schedule
2. Send your customer a schedule confirmation via mail or email that includes:
 - The amount of the recurring transaction (or the amount range for a variable schedule)
 - The frequency of the debits (how often you will charge your customer)
 - The schedule start date, and end date (if defined.)
 - Instructions for terminating the schedule
 - Your business address and a phone number answered during regular business hours.
3. Mail or email a receipt for each payment made as part of the schedule
4. Mail or email notification to your customer at least 10 days in advance of any change to the schedule amount or frequency.

What PaySimple Does For You: By entering a schedule into PaySimple using default email settings, the system will automatically send all required emails to your customers (steps 2, 3, and 4 above.)

Additional Recommendation: Send a pre-notification email to your customer prior to the date the scheduled payment is processed. To do this in PaySimple, check the **Send Pre-Notification** box in the **Email Notifications** section of the **Recurring Payment** screen, and enter the number of days prior to the payment you would like it emailed.

How to Authorize Recurring Credit Card Transactions in Writing

You are permitted to authorize recurring schedules that debit a credit card account via a signed paper authorization form. The authorization requires that your customer understand the conditions under which the business is permitted to debit the account (such as amount, date, and frequency), as well as conditions for termination or change of the authorization.

Typical Uses: There are three typical uses for recurring credit card transactions transaction:

- Payments for the same amount on a regular schedule, such as weekly or monthly service fees
- Payments for a different amount on a regular schedule, such as utility bills
- Payment plans for discharging a large debt, such as installment payments on a large purchase

Recurring Transaction Written Authorizations

How to Authorize:

1. Have your customer sign and date a form (see templates below) that includes the credit card account to be charged, how to terminate the schedule, and the information specified below for the type of recurring payment schedule:
 - a. **Payments for the same amount on a regular schedule:** Amount, frequency, and start date
 - b. **Payments for a different (variable) amount on a regular schedule:** Frequency, start date, not to exceed amount
 - c. **Payment plans for discharging a large debt:** Total due, # of payments, amount of payment, frequency, start date
2. Give your customer a copy of the signed form
3. Keep this form on file, stored digitally or in paper form, for one year after the last payment on the schedule.
4. Send a receipt for each transaction via mail or email.
5. Mail or email notification to your customer at least 10 days in advance of any change to the schedule amount or frequency.

What PaySimple Does For You: By entering a schedule into PaySimple using default email settings, the system will automatically send all required emails to your customers (steps 4 and 5 above).

Additional Recommendation: Send a pre-notification email to your customer prior to the date the scheduled payment is processed. To do this in PaySimple, check the **Send Pre-Notification** box in the **Email Notifications** section of the **Recurring Payment** screen, and enter the number of days prior to the payment you would like it emailed.

Templates Provided:

[Credit Card Recurring Payment Authorization Form-Open--](#)

Use this form to authorize the SAME amount each time with an OPEN end date.

[Credit Card Recurring Payment Authorization Form-SET](#)

Use this form to authorize the SAME amount each time with a SET end date.

[Credit Card Recurring Payment Authorization Form—Variable](#)

Use this form to authorize a DIFFERENT amount each time, with an OPEN end date.

[Credit Card Payment Plan Authorization Form](#)

Use this form to authorize a SET number of payments of the SAME amount each time.

[Combination One Time/Recurring Credit Card Payment Authorization Form](#)

Use this form to authorize a ONE-TIME payment, or a recurring payment of the SAME amount each time with an OPEN end date.

How to Authorize Recurring Credit Card Transactions Online

Recurring online credit card transactions are by definition those that are authorized by a consumer entering payment information into a web form along with details about the schedule amount and frequency, actively checking a box to agree to the terms and conditions for the schedule (pre-checked boxes are not allowed), and clicking a submit button.

Typical Uses: PaySimple web payment forms support two types of recurring transactions

- **Bill Payments** for the same amount on a regular schedule such as payments for weekly or monthly services
- **Payment Plans** for discharging a large debt, such as layaway or installment payments on a large purchase.

How to Authorize:

1. Include the information specified below in your terms and conditions
 - a. Name of your Business
 - b. Your business website address
 - c. Official business mailing address and phone number answered during regular business hours
 - d. A complete description of the goods/services being purchased
 - e. Your Return, Refund, and Cancellation policy
 - f. Your delivery policy and order fulfillment policy (if applicable)
2. Enable your customer to view and print a receipt immediately after submitting the web payment form that contains
 - a. Full details of the schedule
 - b. A confirmation # for any transaction processed as part of the schedule when it was entered
3. Send your customer a schedule confirmation via mail or email that includes:
 - a. The amount and frequency of the recurring transaction
 - b. The schedule start date, and end date (if defined.)
 - c. Instructions for terminating the schedule
 - d. Your business address and a phone number answered during regular business hours.
4. Email a receipt for each transaction in the schedule.
5. Mail or email notification to your customer at least 10 days in advance of any change to the schedule amount or frequency.

What PaySimple Does For You: The web payment forms you create as part of your PaySimple system automate most of the authorization steps for you, including automatically generating a transaction confirmation page and emailing a receipt (steps 2,3,4, and 5 above). To complete the process, you need to do the following:

1. Select the Type of Recurring Schedule the Web Form will process (you can select only one type per form)
 - a. When configuring your web form select either “Bill Payment” or “Payment Plan” in the **Recurring Billing Schedule** field—the system will automatically populate your form with the required fields.

2. When configuring your web form, add the following text to the **Terms and Conditions** field, in addition to your company’s standard terms and conditions. Enter your business information in place of the red insert indicators.

I authorize {company name} to debit the credit card account indicated in this web form, for the noted amount on the schedule indicated. This payment is for {insert description of goods/services}. I understand that returns, refunds and cancellations are {insert your policy here}. I understand that this authorization will remain in effect until the schedule end date, or until I cancel it in writing which ever comes first, and I agree to notify the business in writing of any changes in my account information or termination of this authorization at least 15 days prior to the next billing date. If the above noted payment date falls on a weekend or holiday, I understand that the payment may be executed on the next business day. I certify that I am an authorized user of this credit card and that I will not dispute the payment with my credit card company, so long as the amount corresponds to the terms indicated in this web form.

3. In the **Contact Information** section of the web form configuration page, be sure to enter your main business address and a phone number and email address that is monitored during regular business hours.

Additional Recommendation: It is also recommended, but NOT required, that you send a pre-notification email to your customer prior to the date the scheduled payment is processed. Your customers can’t enable this feature when entering their schedules via web payment forms. You need to complete these steps AFTER the new schedule has been entered.

1. Locate the New Schedule in the **Active Recurring Schedules Report** in the **Upcoming Activity** section of the **Home Dashboard**.
2. Click the linked Schedule ID to open the schedule
3. Expand the **Email Notifications** section of the **Recurring Payment** screen
4. Check the **Send Pre-Notification** box and enter the number of days prior to the payment you would like it emailed.
5. Save the schedule.

Fraud Prevention Guide for Mail, Telephone & Online Credit Card Transactions

Mail, telephone and online credit card transactions are inherently more risky than in-person transactions, as you never physically have possession of or see the credit card. Thus you must rely on other methods to determine if the person making the payment is an authorized user of the card.

A combination of technology and common sense can go a long way toward preventing fraudulent transactions. The simple precautionary steps you take can make a significant difference in protecting your business and your customers. The following are some suggestions on what to do.

Using AVS Match

AVS (Address Verification System) requires you to get a billing address from your customer and matches that address to the one the credit card issuer has on file for that card during the transaction authorization process. Performing this check is so important that **you will be charged more to process a transaction if you do not perform the AVS check**—which is why PaySimple automatically enables AVS on your account.

The default setting for AVS Match is to process the transaction regardless of the result because there are a number of reasons why it might fail for a valid transaction, such as the AVS system being momentarily down, or the card not being found in the AVS system. (Note that to avoid an extra charge you are required to perform the AVS check—not get a positive response.)

A good way to identify and prevent the processing of potentially fraudulent transactions is to program your system to fail any transactions that AVS identifies as no match—meaning that both the address and zip code do not match what is on file. To do this:

1. Log into PaySimple and click the **System Management** button
2. Click the **Fraud Settings** link in sub-navigation
3. In the **Credit Card Settings** section, locate the **AVS** line and click the **Configure** link
4. In the long list of options, locate **N** under the **AVS Code Column** and uncheck its box
5. Click the **Save** button at the bottom of the page

Using CVV2 Match

The CVV2 code (also known as a CVC code) is an identification number located on the credit card that is not part of the card number itself. For Visa and MasterCard it is the three digit number printed on the back of the card located near the signature line. For American Express it is a 4 digit number located on the front of the card on the right side, just above the credit card number. For Discover it is a 3 digit number located on the front of the card on the right side, just above the credit card number.

The idea behind the CVV2 number is to provide merchants with some proof that the person authorizing the transaction actually has the card in hand. Performing this type of check is protection against fraudulent transactions being initiated by someone who has stolen credit card numbers—because the CVV2 is never stored in any payment processing system. Thus even if a database of card numbers is stolen, the thief would never be able to steal the CVV2 codes that go with the cards.

Performing a CVV2 match is not required, and you will not be charged more if you do not do it (except for Discover transactions, which do charge more if the check is not performed). However, enabling the check and programming it to reject a “no match” response can significantly reduce your risk of chargebacks. In fact, proof of a CVV2 match on an authorization can help you defend yourself in the event of a chargeback. Follow the steps below to enable CVV2 in PaySimple.

1. Log into PaySimple and click the **System Management** button
2. Click the **Fraud Settings** link in sub-navigation
3. In the **Credit Card Settings** section, locate the **CVV2** line and select the **Enable** radio button
4. Click the **Configure** link that appears
5. Locate **N** under the **CVV2 Code Column** and uncheck its box in the **Allow Column**
6. Click the **Save** button at the bottom of the page

Note: You can by-pass a CVV2 check for an individual transaction by selecting a radio button stating that the code is not available.

Identifying Fraud

In addition to validation during the authorization process, there is much you can do to train your employees to identify fraudulent transactions before even attempting to process them. Even with all the technological tools at your disposal, it is possible for an expert thief to beat them. So start with the premise that if something sounds fishy or too good to be true, it probably is—and you should think twice about accepting the order.

The following guides provided by VISA, can help you put effective policies and procedures in place, and train your employees:

- [Heads Up to the Warning Signs of Fraud](#)
- [If the Card is NOT There—You Need to be More Aware](#)
- [Take the Order—but Don't Get Taken In](#)

Protecting Your Customers' Information

In addition to protecting your company from processing fraudulent transactions, you are also responsible for protecting your own customers' information from being compromised.

As part of your PCI DSS (Payment Card Industry Data Security Standard) Compliance certification, you should have a security policy in place around how you store and protect customer information—including credit card numbers. You can learn more about PCI in the [PCI Center on PaySimple's website](#).

Utilizing PaySimple for all of your electronic storage of cardholder data is a smart first step towards compliance. Once a credit card number is encrypted and securely stored in PaySimple's PCI Certified system, you can perform additional transactions without the need for external access to the full number again.

But, if you store card holder data in paper form—such a signed authorization forms for recurring schedules—you need to make certain that those forms are protected. The following are some guidelines to use:

- Store any paper documents containing credit card numbers in a locked file drawer or safe
- Limit access to documents containing credit card number on a need-to-know basis
- Discard documents containing credit card numbers when there is no longer a business need to keep them (For recurring schedule authorizations this is one year after the last payment made on the schedule.)
- After successfully entering and processing a transaction in PaySimple (wait until you have confirmation that the transaction settled), redact (cross-out with a dark pen) the CVV2 number and all but the last 4 digits of the credit card number on any paper authorization forms.

If you store authorization forms in digital format, you need to remove the CVV2 number and all but the last 4 digits of the credit card number (after you have successfully processed a transaction of course.) You can achieve this by redacting (cross-out with a dark pen) this information before scanning a written document for storage. Or, if the authorization form is already in digital format, use a tool such as Microsoft Paint or Adobe Acrobat Standard to delete it prior to storage.