

## Sending Credit Card Information over Email FAQ

*Why is it a bad idea to accept credit card information over email?*

PCI DSS requirement 4.2 states that credit card information must not be captured, transmitted, or stored via email. More important to understand, however, is that email is transmitted and stored unprotected in clear text and leaves a trail of copies (in inboxes, sent folders, drafts folders, email trash, web browser caches, computer recycle bins, etc.).

*What constitutes credit card information?*

Credit card information consists of one or more of the following: full credit card number, expiration date, and the code (CVC) on the back of a credit card.

*My customers send me credit card information over email. What should I do?*

As an institution of higher education, we should educate our customers about the dangers of using email to conduct financial transactions. As merchants, we should discourage the sending of credit card information to the point of not processing credit card transactions when the information has been provided over email.

Furthermore, never respond to your customers by including their original email (without deleting or truncating credit card numbers and deleting CVC codes) as you are exacerbating the problem by doing so.

*I mailed a form/application or posted a form/application on my website accepting credit cards as payment, but my customers email the form. What should I do?*

First, consider removing your email address from any form/application or website that mentions credit cards. Second, add the following (or similar) text in a very visible fashion to your form/application or website, discouraging the sending of credit card information over email:

For your protection, Western Illinois University does not accept and will not process credit card information provided via email or text messages. Please contact us at (309) 298-xxxx or drop by our office, and we will gladly assist you.

*I've received credit card information over email in the past. How do I delete these emails and the trails that they leave?*

Delete email containing credit card information from your inbox, sent folder, drafts folder, and any other folders that you may have created. Once that is done, empty your email trash, empty your web browser cache (temporary browser files), and empty your computer's recycle bin or trash.

*I conduct a large volume of business with some of my customers. Is there a way to protect our email conversations so that we can transfer credit card information safely over email?*

PCI DSS requirement 4.2 does allow for the use of email to transmit credit card information if such email can be protected (encrypted). Email, however, does not typically lend itself to encryption since our email conversations occur with large numbers of parties. It is possible to arrange for the protection (encryption) of email for merchants that conduct business with the same customer(s) repeatedly. Be warned that, while this capability may be available, it does not scale to a large number of vendors communicating with a large number of customers. Contact the office of the Chief Technology Security Officer (CSTO) at (309) 298-4500 to discuss your options.