Mastercard In Control for Commercial Payments

Email Encryption

October 2018

EMECR

Contents

Summary of Changes, 14 October 2018

This document reflects updates effective since the previously-published version.

Description of Change	Where to Look
Updated the section for the new proofpoint encryption.	Reading Encrypted Emails as a New Email Recipient

Chapter 1 Email System Configuration

For example, an email from In Control with a from address of inControl@issuer.com is sent to an employee of the issuer. This is common during the integration and deployment of In Control.

The issuer's email system processes the incoming message and may reject it because it comes from issuer.com. In general, email that comes from that email system is not received as an incoming message.

To resolve this issue:

- Whitelist the from address (for example, inControl@issuer.com).
- Whitelist all mail from the IP addresses associated with deliverygateways.mastercard.com, used to send In Control email.
- Implement Sender Policy Framework (SPF) records for the alerts.issuer.com domain to authorize the IP addresses to send mail.
- Consider an In Control configuration where email is not sent from the same domain or a subdomain of the domain used for corporate email. For example, change inControl@issuer.com to inControl@issuer-alerts.com.

Chapter 2 Overview

Protecting sensitive data is a top priority at Mastercard.

Mastercard uses secure industry-standard protocols such as Transport Layer Security (TLS) and applications to secure the electronic transmission of sensitive data through the Internet.

The TLS protocol uses symmetric keys with standard encryption to encrypt and decrypt confidential communications between a sender and the recipient.

NOTE: Always use the latest version of TLS available.

Chapter 3 Encryption Technology

Mastercard implementation leverages this technology to protect data sent by email from Mastercard locations to customers and third parties.

Proofpoint does not replace any existing methods used by Mastercard to securely transmit sensitive data to customers.

Chapter 4 Customer Impact

Most customers see no impact from this additional measure of protection:

- Customers with a secure email TLS connection: No impact to their email and no impact on the delivery speed of emailing sensitive data to customers.
- Customers without a secure email TLS connection: Must access their secure emails through proofpoint to ensure the secure delivery of confidential information.

Chapter 5 Reading Encrypted Emails as a New Email Recipient

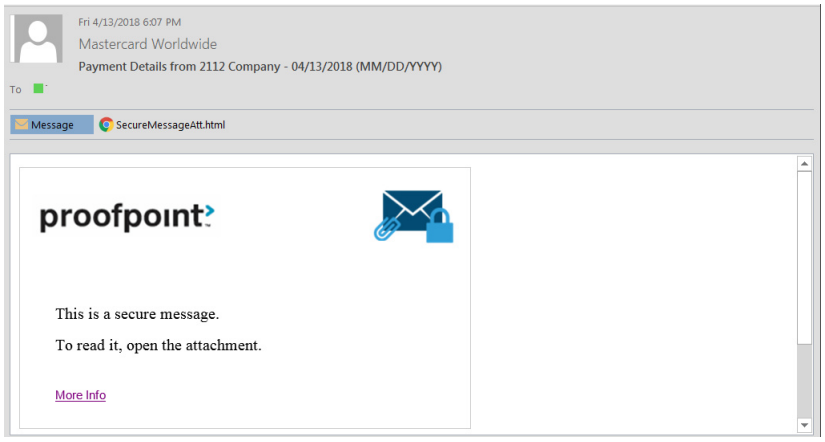
About this task

You will receive an encrypted email from Mastercard with a proofpoint message.

For details on setting up and sending emails using proofpoint, see the *Mastercard In Control for Commercial Payments - Issuer Application Specification Guide* on Mastercard Connect.

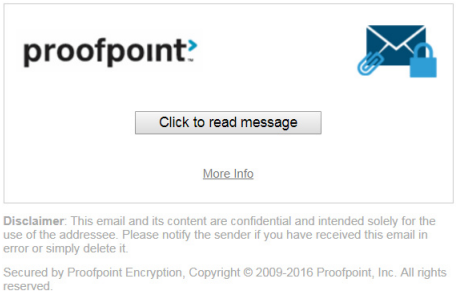
Procedure

1. Click the attachment included in the email.



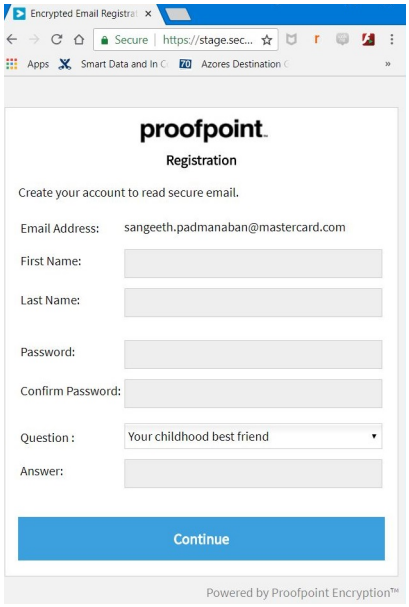
   The **Opening Mail Attachment** dialog box appears.
2. Click **Open**.

   The attachment opens on a Web browser through a secure link.



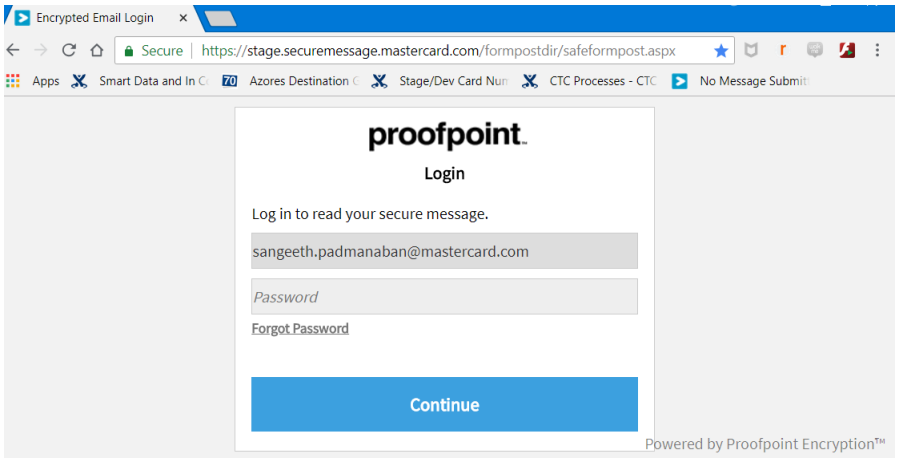
3. Click **Click to read message**.

   The **Registration** page opens.



4. Enter the **First Name**.
5. Enter the **Last Name**.
6. Enter the **Password**.
7. Enter the **Confirm Password**.
8. Select the **Question** and **Answer**.
9. Click **Continue** to view the email.

The page below shows after registration on next log-in.



Results

You can read the encrypted email message using proofpoint.

Chapter 6 Reading Encrypted Emails as a Registered Recipient

Enter your proofpoint ID and password. Click **Continue**.

Chapter 7 Supported Operating Systems and Browsers

Operating System	Supported Browser
Windows 7	IE 7, IE 8, IE 9, IE 10, IE 11, Firefox 28, Chrome 37 For security reasons, proofpoint recommends using the latest version of your chosen browser. For example, IE 6 is no longer supported and IE 7 is not recommended.
Red Hat Enterprise Linux ES / CentOS	Firefox 28, Chrome 37
Mac OS 10.8.X and 10.9.X	Secure Reader is supported on the native browsers for these mobile device operating systems.

The supported browsers use a rapid release schedule and rapid version number increments. The version numbers listed above were tested at the time of the last proofpoint release.

As these browsers release new versions, proofpoint makes best efforts to support them.

Chapter 8 Sender Policy Framework Records

SPF records are Domain Name System (DNS) records that specify the Internet hosts that are allowed to send mail for a given domain.

In Control can send email from any of the IP addresses associated with deliverygateways.mastercard.com.

These IP addresses should be specified in the SPF record for the domain seen in the "from" address of In Control-generated emails.

Additionally, customers should add the following SPF TXT (text) record to the DNS records for the sending domain:

v=spf1 include: deliverygateways.mastercard.com ~all

Example, using a supported IP address: An issuer specifies a "from" address of inControl@issuer.com. The DNS records for issuer.com in a sample SPF record would be:

v=spf1 include: deliverygateways.mastercard.com ~all

For domain alerts.issuer.com that already has an SPF record, include: deliverygateways.mastercard.com must be added to the allowed IP addresses for the domain.

For more information on SPF records, refer to publication RFC 4408 of the Internet Engineering Task Force (IETF).

Chapter 9 Operational Support

Registered recipients who incorrectly enter their password five consecutive times are logged out by the Safemail system.

Contact Global Customer Service for assistance. Users who forget their password should also contact Global Customer Service.

Phone:

- 1 – 800 – 288 – 3381, option 4 (U.S.)
- +1 – 636 – 722 – 6636, option 4 (Outside the U.S.)

Email:

- SmartDatahelp@Mastercard.com
- InControl@Mastercard.com

Global Customer Service delete the user's profile. The user then opens the secure email and follow the prompts to re-register.

The password expires after 90 calendar days. Choose a new password that has not been used in the previous two password resets.

Chapter 10 FAQs

1. Emails are being sent to the customer but they are not receiving them.

   Ask the user to check their email spam folder to ensure the email message is not classified as email spam. Ask the customer's email administrator to locate the email message if you cannot find it in the spam folder.
2. User receives the email message but cannot access the page to download it.

   The user's email or information security department could be blocking the link through their internal IT controls.

Mastercard can only confirm that the message was received by the recipients email system, not the recipient.

We cannot identify what happened after that system received the message. To confirm that the recipient system received the message, contact Global Customer Service.

Notices

Proprietary Rights

The information contained in this document is proprietary and confidential to Mastercard International Incorporated, one or more of its affiliated entities (collectively "Mastercard"), or both.

This material may not be duplicated, published, or disclosed, in whole or in part, without the prior written permission of Mastercard.

Trademarks

Trademark notices and symbols used in this document reflect the registration status of Mastercard trademarks in the United States. Please consult with the Global Customer Service team or the Mastercard Law Department for the registration status of particular product, program, or service names outside the United States.

All third-party product and service names are trademarks or registered trademarks of their respective owners.

Disclaimer

Mastercard makes no representations or warranties of any kind, express or implied, with respect to the contents of this document. Without limitation, Mastercard specifically disclaims all representations and warranties with respect to this document and any intellectual property rights subsisting therein or any part thereof, including but not limited to any and all implied warranties of title, non-infringement, or suitability for any purpose (whether or not Mastercard has been advised, has reason to know, or is otherwise in fact aware of any information) or achievement of any particular result. Without limitation, Mastercard specifically disclaims all representations and warranties that any practice or implementation of this document will not infringe any third party patents, copyrights, trade secrets or other rights.

Translation

A translation of any Mastercard manual, bulletin, release, or other Mastercard document into a language other than English is intended solely as a convenience to Mastercard customers. Mastercard provides any translated document to its customers "AS IS" and makes no representations or warranties of any kind with respect to the translated document, including, but not limited to, its accuracy or reliability. In no event shall Mastercard be liable for any damages resulting from reliance on any translated document. The English version of any Mastercard document will take precedence over any translated version in any legal proceeding.