Mastercard programs:
Data Security

Dear Merchant!

This is our second newsletter regarding Mastercard rules and programs that apply to your business. Understanding these rules and programs and how they can affect Your activity is important as it allows to mitigate possible negative consequences to Your business. This newsletter provides general information on some of the Mastercard programs. If you would have any additional questions, do not hesitate to contact us.

Site Data Protection Program (SDPP)

SDPP was designed to protect against Account Data Compromise (ADC) events and facilitates the identification and correction of vulnerabilities in security processes, procedures, and website configurations.

PCI DSS COMPLIANCE

SDPP requires all merchants to be compliant with PCI DSS (Payment Card Industry Data Security Standard).

IMPORTANT:

1 All Cardinity merchants are required to install and comply with PCI DSS standards as well as to ensure, that any intermediary technical service providers of a merchant (i.e. third party processors or data storage entities) comply with the PCI DSS and minimum security requirements.

2 All Level 3 merchants (i.e. merchants having more than 20.000 e-commerce transactions annually) must annually validate their PCI DSS compliance and upon Cardinity's request submit to Cardinity a completed Self-Assessment Questionnaire (SAQ) or a Report on Compliance (ROC).

3 Non-compliance with SDPP requirements may result in fines being assessed by Mastercard, which might reach from €25.000 for up to €200.000.

NEWSLETTER

October, 2022

UAB "Click2Sell"

Saulėtekio ave. 15-1, Vilnius
LT-10224, Lithuania
www.cardinity.com
info@cardinity.com

Account Data Compromise Program (ADCP)

ACDP was designed to protect against account data compromise (ADC) events, that result, directly or indirectly, in the unauthorized access to or disclosure of account data or the unauthorized manipulation of account data controls, such as account usage and spending limits.

WHAT IS ACCOUNT DATA?

Any cardholder data and/or sensitive authentication data that includes, by way of example and not limitation:

- cardholder data — cardholder name, primary account number (PAN) and expiration date associated with an account (including any Token or Virtual Account) and any Payment Account Reference (PAR) value;
- sensitive authentication data — card validation code 2 (CVC 2) data.

YOUR RESPONSIBILITIES WITH REGARD TO ADC EVENT:

1 **Within 24 hours**, and on an ongoing basis thereafter, submit to Cardinity all known or suspected facts concerning the ADC event or potential ADC event.

2 **Immediately, and no later than within 24 hours**, identify, contain, and mitigate the ADC event or potential ADC event, secure account data and preserve all information, in all media, concerning the ADC event or potential ADC event .

3 **Within 24 hours** and continuing throughout the investigation and thereafter, provide to Cardinity all primary account numbers (PANs) associated with account data that were actually or potentially accessed or disclosed in connection with the ADC event or potential ADC event and any additional information requested by Cardinity.

4 **Proactively participate** and cooperate with Cardinity in the ADC event and/or potential ADC event investigation and provide any necessary information as may be required.

USEFUL LINKS:

- *Mastercard Security rules and Procedures*
https://www.mastercard.us/content/dam/public/mastercardcom/na/global-site/documents/SPME-Manual.pdf
- *Mastercard Trust Center*
https://www.mastercard.us/en-us/business/overview/safety-and-security/cyber-security.html
- *Mastercard for small and medium business*
https://www.mastercard.us/en-us/business/overview.html
- *Safety and security*
(https://www.mastercard.us/en-us/business/overview/safety-and-security.html)

NEWSLETTER

October, 2022

UAB "Click2Sell"

Saulėtekio ave. 15-1, Vilnius
LT-10224, Lithuania
www.cardinity.com
info@cardinity.com