

## **REGULATIONS REGARDING SALES WITH PAYMENT BY CREDIT CARD CARD NOT PRESENT<sup>1</sup>**

*These regulations, the “Card Not Present Regulations”, apply to sales in which payment is made by Credit Card in conjunction with Sales Methods in which the Credit Card is not present upon the occasion of payment. “Sales Methods” covered by the Card Not Present Regulations include, for example, sales over the Internet, sales by mail order and/or telephone order, mobile telephone payments and Recurring Payments. “Recurring Payments” means subscription payments in which the Cardholder has consented to the Merchant regularly debiting the Credit Card on recurring future occasions (e.g. subscriptions).*

*The Card Not Present Regulations constitute a supplement to the general terms and conditions for the Agreement for Acquiring Credit Card Transactions (the “Main Document”) entered into between the Merchant and Euroline. In the event of any conflict between the Main Document and the Card Not Present Regulations, the Card Not Present Regulations shall take precedence. Words commencing with a capital letter indicate a word which has been given a specific content/definition in the Main Document; in these Card Not Present Regulations, such words shall have the same meaning as in the Main Document.*

### **1. Generally regarding sales with payment by Credit Card in conjunction with sales over the Internet, mail and telephone order**

In conjunction with sales over the Internet, mail and telephone order, the Credit Card is not physically present and the Merchant is thus unable to identify the Cardholder in the same manner as when the Credit Card is present. Accordingly, subject to the limitations which may be set forth in section 6 below, the Merchant shall at all times bear the risk associated with all purchase transactions in conjunction with sales over the Internet, mail and telephone order. This entails that Euroline shall be entitled to charge back the Merchant for such amounts that are the subject of a complaint by a Cardholder. The aforesaid shall apply irrespective of whether or not the Cardholder’s objection is justified.

### **2. Special obligations in conjunction with sales over the Internet, mail and telephone order**

The Merchant undertakes as follows:

- on the order form or Internet page, to clearly inform the Cardholder, prior to the payment instructions, regarding the country in which the Transaction takes place and the country in which the Merchant pays VAT;
- on its website, not to have links to websites containing unlawful and/or unethical activities or to activities which may objectively be deemed to damage Euroline’s reputation;
- to notify Euroline immediately in the event 1) the website on which the Merchant’s sales take place is to change www-address, and 2) new www-addresses which the Merchant uses for its sales.

### **3. Verification**

In conjunction with debiting of the Cardholder, the Merchant shall carry out the verifications set forth below.

#### *3.1 Authorisation*

Authorisation must at all times take place in conjunction with payment, irrespective of the purchase amount. Authorisation shall be coded with the correct Sales Method. The codes to be used in this context are set forth in the Instructions.

When verifying the status of the Card Holder’s Credit Card (verification of card status) a zero value authorisation shall be used pursuant to Euroline’s process descriptions applicable from time to time.

---

<sup>1</sup> Decision of ELCRC 2010-05-04

### *3.2 Address verification*

Address verification shall be carried out in accordance with the Instructions to the extent stated in an appendix to the Main Document. Address verification entails verification that the requested delivery address corresponds to the address that the Cardholder has given to the card issuer. Where authorisation of purchase transactions takes place electronically, "Address verification only" shall be clearly stated on the order documentation with respect to address verification. Address verification is only applicable to mail order and/or telephone orders.

### *3.3 Security code*

Verification of security codes shall always be carried out, unless otherwise agreed between the Parties. Verification of security codes entails verification that the security code which is normally found to the right of the signature panel on the back of the Credit Card, sometimes referred to as CVV2 or CVC2, corresponds to the security code registered with the card issuer. The Merchant may not, under any circumstances, store the three-digit security code.

## **4. Order form/order documentation**

### *4.1 Content*

The Merchant's order form/order documentation must be made out to the Merchant and contain:

- the Merchant's name, city and organisation number;
- the Cardholder's name;
- the Cardholder's address (delivery address);
- the Credit Card number and valid thru date;
- the order date;
- the order amount;
- information regarding value added tax.

With respect to bank cards issued by Swedbank, and the Merchant is Swedish, the order form/order documentation must also contain information regarding the method of payment, i.e. information whether payment is to be debited from a bank account or to be on credit.

### *4.2 Storage*

The Merchant shall store order forms/order documentation for a period of 18 months. Upon request by Euroline, the Merchant shall provide order forms/order documentation regarding individual Transactions within five (5) banking days.

### *4.3 The Cardholder's receipt*

The Cardholder shall always receive from the Merchant a receipt for ordered goods or services. Where appropriate, e.g. in conjunction with Internet sales, the Merchant shall provide the Cardholder with an electronic receipt containing the information stated in section 5.2 below.

## **5. Reporting**

### *5.1 Submission of purchase transactions, etc.*

Electronically captured purchase transactions must be submitted to Euroline within two (2) days from the date of payment. In those cases where sales slips are involved, e.g. in conjunction with mail orders and/or telephone orders, such must be submitted to Euroline or the party designated by Euroline within five (5) days from the date of payment. "Date of payment" means the day of authorisation.

In conjunction with Recurring Payments, the Merchant shall submit to Euroline the Merchant's URL and/or telephone number in the purchase transaction in accordance with the Instructions.

Purchase transactions shall be submitted to Euroline in accordance with the procedure agreed upon from time to time. Purchase transactions may not be submitted to Euroline for acquiring before delivery of the goods or service has commenced. "Delivery of service" also includes execution of binding agreements regarding services to be delivered/performed at a later time. Unless otherwise agreed in writing, delivery in conjunction with mail orders and/or telephone orders may only take place to the address provided by the Cardholder to his/her card issuer.

## *5.2 Transaction information and logs*

The Merchant shall, with respect to each Transaction by Credit Card, register the following transaction information in an electronic transaction log:

- the Merchant's name and customer number at Euroline;
- the Merchant's URL (only in conjunction with Internet orders);
- the currency and amount;
- information regarding value added tax;
- the date of payment (for Transactions which involve payment for a journey, event, etc. which is to take place at a future date, the date of the journey, event, etc. must be stated);
- the unique transaction number;
- the Cardholder's name and, where appropriate, customer number at the Merchant;
- the verification number as evidence of authorisation;
- the type of transaction (payment or return/crediting) in clear text);
- description of purchased/returned services/goods;
- method of payment (see section 4.1, second paragraph above).

## **6. Specifically regarding sales over the Internet**

In conjunction with sales over the Internet, 3D Secure, i.e. Verified by Visa or MasterCard SecureCode, shall be applied in accordance with the Instructions.

Where the Merchant has implemented 3D Secure and has coded the Transactions in accordance with the Instructions, Euroline shall be entitled to charge back disputed amounts which have been the subject of complaints as constituting fraudulent or by unauthorised purchases, only in accordance with Visa's and or MasterCard's regulations in force from time to time.

Visa and MasterCard may also prescribe from time to time that Euroline shall not be entitled to charge back disputed amounts which are the subject of a complaint as constituting fraudulent or by unauthorised purchases, notwithstanding that the Cardholder has not identified him-/herself vis-à-vis his/her card issuer.

With respect to amounts which are the subject of a complaint based other than on such constituting a fraudulent or unauthorised purchase, Euroline shall be entitled to charge back in accordance with section 1 above notwithstanding that the Merchant has implemented 3D Secure.

Certain MasterCard and Visa products, as well as certain non-European cards currently do not have support for 3D Secure.

The Merchant shall also display the logos for Verified by Visa and MasterCard SecureCode on the payment page/checkout page.

Section 6 of the Main Document shall apply notwithstanding that the Merchant has implemented 3D Secure.

## **7. Security**

### *7.1 Processing of Credit Card Information*

In order to maintain a high level of security in the global card payment systems and to enhance confidence in Credit Cards as a means of payment, it is of the utmost importance that all who process Credit Card Information do so in a secure manner. "Credit Card Information" means information embossed or printed on the front or back of the Credit Card, including information which is stored in the Credit Card's magnetic strip or chip. For this reason, the industry has agreed on a joint industry standard for processing Credit Card Information. The standard is called Payment Card Industry (PCI) Data Security Standard (DSS) and is produced by the international card networks, Visa and MasterCard.

The Merchant undertakes to comply with the PCI DSS standard as published from time to time on [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

The aforesaid entails, *inter alia*, that the Merchant:

- may not, under any circumstances whatsoever, store or write out i) CVV/CVC (i.e. the code verification value in the Credit Card's magnetic strip); ii) CVV2/CVC2 (i.e. the security code normally found to the right of the signature panel on the back of the Credit Card; or iii) iCVV/iCVC (i.e. the verification value in a Credit Card which is equipped with a chip). The Merchant also undertakes not to store or write out any PVV (i.e. the verification value for PIN codes);
- may only store such Credit Card Information as is absolutely necessary for the Merchant's business (e.g. name, the Credit Card number and the Credit Card's valid thru date);
- shall file/store media containing Credit Card Information (e.g. logs, transaction reports, electronic receipts or contracts) in a secure place and in such a manner that only persons who necessarily require access to the material in question are afforded such access;
- shall handle all Credit Card Information confidentially and not to disclose to any third party the personal data (e.g. name and personal ID number) which may be obtained by the Merchant;
- shall store information regarding the Credit Card's number in such a manner that unauthorised use thereof cannot occur;
- shall ensure that electronic receipts and other media are protected from unauthorised access thereto;
- shall notify Euroline immediately upon discovery or suspicion of unauthorised use of Credit Card Information or that such information has otherwise been misused. In the event of suspicion of crime, the Merchant shall report the event to the police upon request by Euroline;
- shall ensure that the Credit Card number is not revealed to persons other than such personnel of the Merchant who necessarily require access thereto;
- shall ensure that documentation is in place regarding the manner in which Credit Card Information is protected in the Merchant's technical equipment;
- shall ensure that routines are in place for secure handling and distribution of Credit Card Information and that such routines are regularly monitored and reviewed. The routines, or information thereon, shall be destroyed in a secure manner, e.g. through a shredding machine, when the routines/information are no longer required in accordance with applicable legislation and/or the Instructions;
- shall ensure that a list is in place of all technical equipment and that such equipment is stored in a secure manner;
- shall ensure that information regarding Credit Cards and/or Cardholders is rendered unusable as soon as technical equipment and/or any other medium containing such information is no longer to be used by the Merchant.

#### *7.2 Approval of systems*

Systems that submit transactions to Euroline must be approved by Euroline or any third party designated by Euroline. Euroline may impose requirements regarding special examination of components that are sensitive from a security perspective. Such examination or scanning shall be carried out by a party selected in consultation with Euroline.

#### *7.3 Specifically regarding Nodes and Payment Service Providers*

Where the Merchant retains a third party (node or Payment Service Provider) for parts or all of its sales over the Internet, mail and telephone order, the Merchant must ensure that such party satisfies all PCI DSS requirements.

#### *7.4 Changes in systems, etc.*

Changes in the system which affect the conditions in force at the time of approval may not be undertaken without Euroline's approval.

Prior to submission of Transactions to Euroline, the Merchant shall carry out a test designated by Euroline regarding connection to Euroline's receipt system.

#### *7.5 Security instructions*

The Merchant shall ensure compliance with Security Instructions as specifically issued by Euroline from time to time.

#### *7.6 Computer hacking and IT forensic investigations*

In the event Euroline suspects that the Merchant's cash register system, computer system, etc. has been exposed to hacking, manipulation, etc. which, in Euroline's opinion, in any respect affects the Parties' cooperation pursuant to this Agreement, Euroline shall be entitled to carry out an IT forensic investigation (the "Investigation") of the equipment in question. The investigation may be carried out by Euroline or an IT forensic company retained by Euroline.

The time and associated issues/routines relating to the execution of the Investigation shall as far as possible be agreed upon by the Parties, unless Euroline considers this to be inappropriate. However, Euroline shall also be entitled to visit the Merchant and carry out the Investigation without prior notice to the Merchant where, in Euroline's opinion, this constitutes the most appropriate course of action.

The Merchant shall be obliged, to a reasonable extent, to assist in the Investigation and facilitate the execution thereof in order that the purpose of the Investigation, i.e. establishing whether hacking/manipulation has occurred, can be achieved.

In the event the Investigation establishes that the Merchant's cash register system, computer system, etc. has been exposed to hacking, manipulation, etc. the Merchant shall be liable, upon request by Euroline, to reimburse Euroline for the costs of the Investigation.