

## **REGULATIONS REGARDING SALES WITH PAYMENT BY CREDIT CARD UNMANNED TERMINALS<sup>1</sup>**

*These regulations, the “Unmanned Terminal Regulations”, apply to sales in which payment is made by Credit Card at unmanned terminals, such as petrol pumps, parking machines and toll road stations.*

*The 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 Regulations, the Regulations shall take precedence.*

### **1. Types of Terminals for unmanned environments**

**Type 1** means Unmanned Terminals, e.g. vending machines or petrol pumps, where verification takes place through use of a PIN code and authorisation is from SEK 0. Where the final amount is not approved in conjunction with authorisation, Euroline’s routines description in force from time to time shall apply. The amount in conjunction with payment by Credit Card in this environment may not exceed the equivalent of SEK 600.

**Type 2** means Unmanned Terminals which lack the possibility for PIN code verification but with authorisation from the equivalent of SEK 0.

**Type 3** means Unmanned Terminals where checks regarding blocked cards take place against a local blocked cards register in the Merchant’s system. Routines for such handling such blocked cards are specified in an appendix to the Agreement. The amount in conjunction with payment by Credit Card in this environment may not exceed the equivalent of SEK 500.

### **2. Customer receipts**

Customer receipts must always be provided and contain the following information:

- the Merchant’s name, city and company number;
- the date;
- the Credit Card number shall be stated in truncated form, i.e. only the (4) final digits shall be written out; introductory positions shall be truncated with ‘\*’;
- the type of transaction (payment or return/crediting) in clear text;
- the amount;
- information regarding value added tax;
- reference/trace back number (unique identity of the Transaction).

### **3. Use of PIN Code**

Where the Terminal handles PIN codes, the Cardholder shall be allowed three (3) attempts to identify himself by means of a PIN code. Where the wrong PIN code is entered three (3) times in succession, the equipment shall have the possibility to retain the card. Such cards shall be cut in two and sent to the relevant card issuer. The Cardholder shall have the possibility to cancel a Transaction instead of making additional attempts with the PIN code.

Where PIN codes are not permitted for the type of card, the card cannot be used in self-service equipment with PIN-verification.

---

<sup>1</sup> ELCRC 2008-12-02

## 4. Transactions Capture

Capture of purchase transactions made by Credit Card on which a name and/or number are not embossed (e.g. Credit Cards bearing the Maestro and Electron trade marks) may take place only in Type 1 Terminals.

## 5. Reporting

### 5.1 Submission of purchase transactions

Electronically captured purchase transactions must be submitted to Euroline within two (2) days from the date of payment. "Date of payment" means the date of authorisation.

### 5.2 Transaction journal

The Merchant shall maintain a separate journal of all Transactions in which a Credit Card has been used, i.e. both executed and cancelled Transactions. Such journal shall record:

- the manner in which the Transaction was executed;
- the Merchant's name (company name), city and company number;
- the date and time;
- the Credit Card's number (where so supported by the Terminal, this shall take place in truncated form);
- the method of payment (see section 2.1, second paragraph above);
- the type of transaction (payment or return/crediting) in clear text;
- the cash register identity;
- the verification number as evidence of authorisation;
- the amount to be debited;
- reference/trace back number; and
- the reply code.

### 5.3 Storage

The Merchant shall store the Transaction Journal in accordance with the most recently applicable PCI DSS regulations (see section 6.1 below) for not less than eighteen (18) months. Upon request by Euroline, the Merchant must be able to provide a receipt with respect to an individual Transaction within five (5) days. The aforesaid shall apply notwithstanding that the Merchant's acquiring agreement with Euroline has otherwise terminated.

## 6. Security

### 6.1 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.

#### *6.2 Approval of systems*

Terminals which submit Transactions to Euroline must be approved by Euroline or a third party designated by Euroline. Euroline may impose requirements regarding special examination of components that are sensitive from a security perspective.

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

Where the Merchant retains a third party (node or Payment Service Provider) as part of its payment solution for processing Transactions, the Merchant must ensure that such party satisfies all PCI DSS requirements.

#### *6.4 Changes to equipment, etc.*

The Merchant shall notify Euroline prior to every installation, relocation or dismantling of equipment which is technically connected to Euroline or another capturer of Transactions.

Changes to Terminals which affect the conditions that applied on the date of approval may not be undertaken without Euroline's consent.

Prior to submission of transactions to Euroline, the Merchant shall perform such a test of its connection to Euroline's receipt system as designated by Euroline.

*6.5 Specifically regarding cash register systems with integrated card readers/Security instructions*

Merchants who use cash register systems with integrated card readers shall also ensure compliance with Security Instructions specifically issued by Euroline from time to time.

*6.6 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.

## **7. Liability Shift**

With respect to Transactions undertaken as from 1 January 2009, Euroline will apply what is referred to as a Liability Shift. Accordingly, as from the aforesaid date the Merchant shall, in its relationship with Euroline pursuant to the Agreement, bear the risk of all losses attributable to magnetic strip-read Transactions undertaken through the use of cards presented without authorisation, where the correct Credit Card, i.e. the Credit Card issued by an authorised/licensed card issuer bearing the same card number as the card presented without authorisation, is equipped with an EMV chip.