Paiement par carte de crédit détourné frauduleusement

Sujet: **Abus et escroquerie** Numéro de cas: **2020/10**

> La cliente a reçu un courrier électronique prétendument envoyé par la Poste, dans lequel elle était invitée à cliquer sur un lien afin de payer 2.99 CHF pour la livraison d'un paquet. Dans l'attente d'un paquet Zalando, elle a suivi les instructions. Elle a été redirigée vers un site internet, qu'elle a pris pour celui de la Poste et où elle a saisi les données de sa carte de crédit. L'émettrice de la carte de crédit lui a ensuite envoyé un code par SMS, que la cliente a également saisi sur le site internet. Peu après, l'émettrice de la carte de crédit lui a envoyé une confirmation faisant état d'un paiement de 1500 CHF. La cliente a immédiatement contacté l'émettrice, qui a clarifié l'incident tout en refusant de dédommager la cliente. Celle-ci s'est alors tournée vers l'Ombudsman. Dans le cadre de la procédure de médiation, l'émettrice de la carte de crédit a finalement accepté d'indemniser la cliente à hauteur de 800 CHF, une offre que celle-ci a acceptée.

Malheureusement, ce schéma d'escroquerie visant principalement les clients de la Poste ou d'autres services de coursiers est connu. Sous prétexte qu'ils doivent payer un petit montant pour recevoir un colis, un SMS ou un courrier électronique redirige les clients vers un site internet falsifié, afin qu'ils saisissent les données de leur carte de crédit. Cette pratique est appelée «hameçonnage» (phishing). En réalité, grâce aux données ainsi volées, les escrocs déclenchent un paiement beaucoup plus élevé. En l'espèce, la carte de crédit de la cliente a été débitée de 1500 CHF en vue de payer une facture émise par une agence de voyage étrangère. Bien que la cliente ait immédiatement découvert et notifié l'escroquerie, grâce à une fonctionnalité de l'émettrice l'informant par SMS à chaque fois que sa carte est débitée, l'émettrice de la carte de crédit n'a pas été en mesure d'empêcher l'exécution de la transaction effectuée par les escrocs au moyen des données de la cliente. Cette impossibilité s'explique par une règle du réseau de cartes de crédit concerné, selon laquelle l'annulation d'une telle transaction dans le cadre d'une procédure de rétrofacturation ne peut pas être demandée si le titulaire de la carte a autorisé cette transaction par un processus d'authentification à deux facteurs.

Dans le cadre d'un processus d'authentification à deux facteurs, le titulaire de la carte est invité à confirmer une transaction par carte de crédit effectuée en ligne au moyen d'une application ou d'un code envoyé par SMS à un numéro qu'il a préalablement enregistré auprès de l'émettrice de la carte de crédit. Selon certains systèmes d'authentification, l'appareil du titulaire de la carte est lui aussi préalablement enregistré, en sus du numéro de téléphone. En utilisant un tel système, un commerçant se protège contre une éventuelle demande en restitution et s'assure de pouvoir conserver le montant débité de la carte de crédit.

En l'espèce, les conditions applicables aux cartes de crédit prévoyaient que l'émettrice de la carte de crédit réponde des dommages découlant d'une utilisation abusive de la carte à condition que le client ait rempli toutes les obligations lui incombant en vertu desdites conditions (notamment ses obligations de diligence), et qu'aucune faute ne puisse lui être imputée. Or, de l'avis de l'émettrice de la carte de crédit, la cliente a violé une obligation de diligence majeure dans la mesure où elle a transmis aux escrocs, et donc à des tiers inconnus, les données de la carte ainsi que le code de confirmation en les saisissant sur le site internet truqué, qu'elle avait pris pour le site légitime de la Poste.

Au sujet de l’objection soulevée par l’Ombudsman selon laquelle la cliente s’est contentée de saisir les données nécessaires à un paiement et ne s’est pas rendu compte que le site internet était un faux, l’émettrice de la carte de crédit a répondu que, selon elle, tout client se faisant prendre par un tel site d’hameçonnage commet une violation de son devoir de diligence. Tout le monde sait qu’il ne faut pas cliquer sur des liens envoyés par des expéditeurs inconnus. En l’espèce, l’adresse de l’expéditeur du courrier électronique indiquait clairement qu’il ne s’agissait pas de la Poste. En cliquant sur l’URL du site internet, la cliente aurait également pu voir que cette adresse était celle de la Poste de prime abord seulement, la véritable adresse du site d’hameçonnage apparaissant en arrière-plan. De plus, il était inhabituel que des montants non arrondis soient exigés en lien avec la livraison de colis. Toujours selon l’émettrice de la carte de crédit, la cliente a utilisé le code de confirmation qui lui a été envoyé par SMS et qui indiquait: «Votre code pour le paiement est: XXX». L’émettrice de la carte de crédit a en outre renvoyé à une application qui aurait pu simplifier davantage le processus de confirmation. Le fait que ni le montant du paiement ni l’identité du prestataire n’apparaissaient dans le SMS correspondait aux pratiques alors en vigueur. Toujours selon l’émettrice de la carte, des modifications avaient été entre-temps apportées de telle sorte que le montant et le prestataire soient communiqués en même temps que le code exigé.

L’Ombudsman a invité l’émettrice de la carte de crédit à reconsidérer sa position. En effet, elle exigeait des clients une certaine connaissance technique dont, de l’avis de l’Ombudsman, ne dispose généralement pas le large public. De surcroît, l’absence d’indications dans le SMS quant au montant du paiement et au prestataire a largement contribué au succès de l’escroquerie. Finalement, l’émettrice de la carte de crédit a offert à la cliente de lui rembourser 800 CHF, soit un peu plus de la moitié du dommage, ce que la cliente a accepté.