

Pour ces motifs, la cour,

Reçoit l'appel.

Le dit non fondé sauf en ce qui concerne le taux d'intérêt conventionnel qui est de 12% l'an.

Délaisse à The Good Bike SA ses frais de requête d'appel et la condamne à payer à la SA Atos Worldline l'indemnité de procédure de 2.500 EUR.

(...)

### Observations

Un paiement par carte implique l'intervention de différentes parties<sup>37</sup>:

- l'émetteur de la carte (qui peut être ou non la banque dans laquelle le titulaire de la carte a ouvert un compte);
- l'acquéreur (acquiescer) qui conclut un contrat de prestation de services avec un commerçant (BCC/Atos, dans le cas d'espèce);
- le titulaire de la carte;
- le commerçant bénéficiaire du paiement par carte;
- la banque du titulaire (qui peut être ou non l'émetteur) et celle du commerçant;
- les différentes banques intermédiaires;
- les processeurs de systèmes (le processing pouvant être assuré ou non par l'acquéreur lui-même).

En cas d'utilisation régulière de la carte, et si certaines conditions sont respectées, le commerçant a la garantie d'être payé. C'est l'émetteur de la carte qui au final garantit la bonne fin de l'opération, cette garantie s'exécutant en cascade, par le fait d'adhésions successives au système par les différentes parties: l'acquéreur garantit le commerçant et est lui-même garanti par l'émetteur lequel se rembourse par débit du compte de son client ou auprès de la banque chez qui le paiement est domicilié.

Lorsqu'un paiement par carte est initié, l'acquéreur – le cas échéant à l'intervention du processeur du système si l'acquéreur ne remplit pas lui-même ce rôle – opère certaines vérifications et autorise la transaction. Il crédite ensuite le compte du bénéficiaire du montant de la transaction autorisée et se fait rembourser par l'émetteur.

Les relations entre parties sont contractuelles. Elles s'inscrivent par ailleurs dans un ensemble de règles qui font partie intégrante des contrats, sous le contrôle d'une organisation responsable du schéma de paiement<sup>38</sup>.

La bonne fin de l'opération suppose, en principe, que soient respectées différentes techniques de sécurisation<sup>39</sup>:

- certification du terminal utilisé et en particulier de son module de sécurité;

- authentification du marchand et de l'acquéreur et intégrité du système;
- authentification de la carte (piste magnétique, puce électronique, ...);
- authentification du porteur de la carte (par signature d'un voucher ou utilisation d'un code secret, ...).

Dans le cadre d'une opération de paiement classique effectuée par le titulaire de la carte sur un terminal de paiement installé chez un commerçant, le titulaire de la carte est physiquement présent, il est donc possible de lui demander de signer un ticket relatif à l'opération ou de lui faire introduire son code secret.

Il n'en va pas de même lors de ventes à distance via Internet par exemple.

En pareille hypothèse, il peut être pallié à l'absence de contact 'face to face' par le recours à la signature électronique<sup>40</sup> ou à de nouveaux procédés de sécurisation (3D Secure proposé par Visa et MasterCard par exemple) qui visent à n'autoriser une transaction qu'après authentification du porteur.

En dehors de l'utilisation de ces nouvelles technologies d'authentification, d'autres vérifications tendent à limiter les risques sans toutefois les éliminer.

Ainsi, dans le cas qui fait l'objet de la présente note d'observation, le vendeur se limitait à demander le numéro de la carte et sa date d'expiration. Ces données étaient transmises à BCC qui vérifiait l'absence d'opposition notifiée par le titulaire en raison d'une perte ou d'un vol de la carte et le fait que la transaction n'excédait pas les limites du crédit lié à la carte. Dans la mesure où ces vérifications ne révélaient pas d'obstacle, une autorisation – ou une "non-opposition" – était envoyée au vendeur. Les vérifications opérées ne permettaient toutefois pas de s'assurer de ce que l'utilisateur de la carte dans le cadre de l'opération considérée était bien le titulaire légitime de ladite carte.

Les responsabilités en cas d'utilisation frauduleuse d'une carte de paiement ou de crédit sont actuellement régies en

<sup>37</sup>. Voy. pour une architecture plus complète des paiements par carte dans l'environnement belge: P. BELLENS, "Aspects généraux du paiement électronique par carte bancaire" in *Aspects juridiques du paiement électronique – Juridische aspecten van elektronische betaling*, T. I, Banksys, Kluwer, 2004, pp. 23 et s.

<sup>38</sup>. Et détentrice de la marque Visa, MasterCard, etc.

<sup>39</sup>. J.-P. BUYLE et O. CREPLET, "La responsabilité des gestionnaires des systèmes de paiement électronique, appréciée dans le contexte global de ceux-ci" in *Aspects juridiques du paiement électronique – Juridische aspecten van elektronische betaling*, T. II, Banksys, Kluwer, 2004, pp. 42 et s.

<sup>40</sup>. E. ROGER FRANCE et E. DE GROOTE, "La valeur probante des signatures électroniques – Réseaux fermés, réseaux ouverts et opérations effectuées au moyen d'instruments de transfert électronique de fonds" in *Aspects juridiques du paiement électronique – Juridische aspecten van elektronische betaling*, T. III, Banksys, Kluwer, 2004, pp. 133 et s.

Belgique par la loi du 17 juillet 2002 relative aux opérations effectuées au moyen d'instruments de transfert électronique de fonds<sup>41</sup> (loi ITEF).

Cette loi met différentes obligations à charge respectivement du titulaire de la carte et de l'émetteur<sup>42</sup>.

L'émetteur – défini<sup>43</sup> comme “*toute personne qui, dans le cadre de son activité commerciale, met un instrument de transfert électronique de fonds à la disposition d'une autre personne conformément à un contrat conclu avec celle-ci*” – doit notamment<sup>44</sup> informer régulièrement le titulaire sur les opérations réalisées au moyen de l'instrument de transfert électronique de fonds; – lui donner la possibilité de vérifier ces opérations; et – fournir périodiquement au titulaire des conseils de prudence destinés à éviter tout usage abusif. L'émetteur doit également<sup>45</sup> – garantir le secret du numéro d'identification ou code d'identification du titulaire; – mettre à la disposition de ce dernier les moyens appropriés lui permettant de notifier le vol ou la perte de l'instrument ou l'imputation sur son relevé de compte de toute opération effectuée sans son accord et plus généralement, toute erreur ou irrégularité constatée dans ledit relevé; et – empêcher toute utilisation de l'instrument de transfert électronique de fonds après notification de la perte ou du vol par le titulaire.

Le titulaire doit<sup>46</sup> prendre des précautions raisonnables pour assurer la sécurité de l'instrument de transfert électronique de fonds et des moyens qui en permettent l'utilisation. Il doit notifier dès qu'il en a connaissance à l'émetteur la perte ou le vol de l'instrument, les opérations non autorisées dont il a constaté l'imputation sur son extrait de compte et toute irrégularité constatée sur ledit extrait.

Jusqu'à la notification, le titulaire de la carte est responsable des conséquences liées à sa perte ou son vol à concurrence d'un maximum de 150 EUR seulement, à moins qu'il n'y ait eu de sa part fraude ou négligence grave auquel cas ce plafond n'est pas applicable<sup>47</sup>.

Après la notification et sauf si l'émetteur apporte la preuve de ce que le titulaire a agi frauduleusement, ce dernier n'est plus responsable de rien<sup>48</sup>.

La loi du 17 juillet 2002 ne règle pas les relations entre acquéreur<sup>49</sup> et commerçant et ne protège pas le commerçant en cas d'utilisation frauduleuse de la carte. Seul le titulaire de la carte est protégé par son droit à obtenir le remboursement des opérations frauduleuses dans les limites prévues par la loi.

Les relations entre acquéreur et commerçant sont régies exclusivement par le contrat qu'ils ont conclu, les conditions générales relatives à ce contrat et les principes généraux du droit des obligations.

De tels contrats opèrent une distinction très nette entre l'hypothèse d'un paiement effectué dans le cadre d'un système sécurisé – signature manuscrite ou électronique ou utilisation d'un code ou procédé d'identification – et les cas où il n'est pas possible de s'assurer de ce que l'identité de l'utilisateur de l'instrument de paiement coïncide avec celle du titulaire de cet instrument: cas de vente à distance où seuls le numéro et la date de validité de la carte sont communiqués.

Dans le premier cas, le commerçant est en principe sauf fraude ou négligence de sa part protégé par la garantie de paiement à laquelle tant l'émetteur que l'acquéreur se sont contractuellement engagés.

Les efforts consentis par la doctrine pour faire entrer cette garantie de paiement dans le cadre d'une des figures classiques du droit des obligations nous paraissent aussi inutiles qu'insatisfaisants dans leurs résultats.

La majorité des auteurs<sup>50</sup> qui se sont exprimés sur le sujet y voient l'application d'un mécanisme de délégation imparfaite dans lequel le titulaire de la carte serait délégant, l'acquéreur délégué et le commerçant délégataire<sup>51</sup>. Cette analyse nous semble erronée en considération tant des relations – ou de l'absence de relation – entre les parties en présence que de la volonté exprimée par celles-ci. Dans la mesure où il n'existe pas de relation contractuelle directe entre le titulaire de la carte et l'acquéreur, comment imaginer que le titulaire, considérant l'acquéreur comme son débiteur lui demande de s'engager envers le commerçant créancier? En fait, le titulaire de la carte ignore même, dans la majorité

41. MB 17 août 2002; M. GUSTIN, “La loi du 17 juillet 2002 relative aux opérations effectuées au moyen d'instruments de transfert électronique de fonds” in *Aspects juridiques du paiement électronique – Juridische aspecten van elektronische betaling*, T. III, Banksys, Kluwer, 2004, pp. 67 et s.; R. STEENNOT, “De wet betreffende de transacties uitgevoerd met instrumenten voor de elektronische overmaking van geldmiddelen”, *Dr. banc. fin.* 2002, pp. 255 et s. et A. SALAUN, “Une nouvelle pierre à l'édifice de protection des consommateurs: la loi sur les instruments de transfert électronique de fonds”, *JT* 2003, pp. 205 et s.

42. T. LAMBERT, “La loi du 17 juillet 2002 relative aux opérations effectuées au moyen d'instruments de transfert électronique de fonds”, *RDCB* 2003, pp. 573 à 588.

43. A l'art. 2 de la loi du 17 juillet 2002.

44. Art. 5 de la loi du 17 juillet 2002.

45. Art. 6 de la loi du 17 juillet 2002.

46. Art. 8 de la loi du 17 juillet 2002.

47. Art. 8 § 2 de la loi du 17 juillet 2002.

48. Art. 8 § 2 de la loi du 17 juillet 2002.

49. L'acquéreur lui-même n'est pas visé par la loi puisqu'il ne s'agit pas de la contrepartie directe du titulaire de l'instrument de transfert électronique de fonds: *Exposé des motifs* de la loi du 17 juillet 2002, *Trav. parl.* Chambre 2000-01, n° 1389/001, 11-12.

50. Notamment, R. STEENNOT, *Elektronisch betalingsverkeer – Een toepassing van de klassieke principes*, Anvers, Intersentia, 2002 p. 156 et réf. citées.

51. Sur l'application de ce mécanisme aux transferts électroniques de fonds et sur les limites que présente une telle analyse, voy. notamment X. THUNIS, *Responsabilité du banquier et automatisation des paiements*, Presses Universitaires de Namur, 1996, pp. 101 et s.

des cas, dans quelle mesure le fournisseur est garanti<sup>52</sup>. Ce n'est, comme rappelé ci-dessus, que par une cascade d'engagements bilatéraux et d'adhésions successives au système, que le solde du compte du titulaire ou l'ouverture de crédit dont il dispose auprès de sa banque sert à apurer le paiement.

L'exercice est au surplus totalement vain, les contrats passés entre parties délimitant soigneusement tant les droits et obligations réciproques que les responsabilités encourues, de manière telle que la qualification juridique de ces contrats est sans utilité pratique.

Ce qui est certain, c'est que dans l'hypothèse où un commerçant se contente de la communication du numéro de la carte et de sa date d'expiration sans recourir à un procédé d'identification sécurisé du titulaire, l'acquéreur se réserve contractuellement le droit de redébiter le compte du commerçant en cas de contestation de l'opération par le titulaire de la carte.

Cette clause contractuelle est du reste dans la logique de la loi du 17 juillet 2002 puisque ladite loi exclut expressément toute responsabilité du titulaire lorsque l'instrument de transfert électronique de fonds a été utilisé sans présentation physique et sans identification électronique<sup>53</sup>. En pareille hypothèse et en cas de contestation de l'opération par le titulaire de la carte, l'émetteur a l'obligation de recréditer immédiatement le compte du titulaire. Il redébitera donc corrélativement le compte de l'acquéreur qui à son tour se retournera contre le commerçant.

En l'absence de présentation physique ou d'identification électronique, les avenants 'mail orders (MO)' et 'telephone orders (TO)' limitent certains risques en assurant certaines vérifications quant à l'absence de vol ou de perte notifiée et quant aux limites de validité et de crédit lié à la carte mais rien de plus. Les contrats sont clairs sur ce point.

La cour d'appel ne s'y est pas trompée. Dans la décision commentée, la cour, d'une part rejette à bon droit toute référence à la loi du 17 juillet 2002 qui comme nous l'avons rappelé ne s'applique que dans les relations entre titulaire et émetteur de carte – ce que l'acquéreur n'est pas – d'autre part, constate que l'acquéreur n'a en l'espèce commis aucune faute ou manquement à son devoir d'information ou de conseil ni à l'obligation d'exécution de bonne foi des conventions.

La cour souligne que le code d'autorisation donné par l'acquéreur n'est pas une reconnaissance absolue de la validité de la transaction ni une garantie certaine de paiement dès lors que l'acquéreur n'est pas en mesure de vérifier que la carte a effectivement été utilisée par son titulaire légitime et considère comme normal que ce soit le commerçant qui supporte le risque d'une malveillance de son client – contre lequel il lui appartient de se retourner – dès lors que c'est lui qui a décidé d'accepter un paiement par carte sans présence physique du titulaire, se privant ainsi de la possibilité d'opérer les vérifications requises et d'obtenir la signature de l'intéressé.

Le fait que le commerçant n'ait lui-même commis aucune faute dans l'exécution du contrat est irrelevante puisque l'objet même du contrat exclut toute garantie de paiement en cas de contestation de l'opération par le titulaire de la carte et autorise expressément l'acquéreur à re-débiter, en pareil cas, le compte du commerçant.

Cette décision est conforme à la jurisprudence antérieure de la cour<sup>54</sup>. Elle a depuis été encore confirmée par une décision du 10 mars 2009<sup>55</sup>.

L'entrée en vigueur de la Directive PSD<sup>56</sup> modifiera-t-elle la donne en ce qui concerne le sort du commerçant bénéficiaire de paiement<sup>57</sup>?

Le champ d'application de la directive PSD est plus large que celui de la loi du 17 juillet 2002 puisque, au lieu de se limiter à l'émetteur et au titulaire des instruments de transfert électronique de fonds, elle vise tout utilisateur de services de paiement et tout prestataire de services de paiement.

L'utilisateur de services de paiement est défini à l'article 4(10) de la directive comme "toute personne physique ou morale qui utilise un service de paiement en qualité de payeur ou de bénéficiaire, ou des deux".

Quant aux services de paiement, il s'agit de toute activité exercée à titre professionnel énumérée dans l'annexe de la directive et parmi lesquelles figure expressément l'acquisition (acquiring) d'instruments de paiement<sup>58</sup>.

Toutefois, la directive vise les opérations de paiement autorisées par le payeur.

L'article 54 de la directive stipule à propos du consentement relatif à une opération de paiement que "les états membres veillent à ce qu'une opération de paiement ne soit réputée

<sup>52</sup> F. GRUA, *Contrats bancaires*, T. I, Paris, Economica, 1990, p. 177.

<sup>53</sup> Art. 8 § 4 de la loi du 17 juillet 2002. Voir également F. DE CLIPPELE, "Qui va payer? Ou questions quant à la responsabilité de l'émetteur de carte en cas de transfert électronique de fonds", *Aspects juridiques du paiement électronique – Juridische aspecten van elektronische betaling*, T. III, Banksys, Kluwer, 2004, pp. 39 et s. en particulier p. 56.

<sup>54</sup> Bruxelles 19 décembre 2006, RG 2004/AR/1715 et Bruxelles décembre 2007, RG 2005/AR/1411.

<sup>55</sup> Bruxelles 10 mars 2009, *Dr.banc.fin.* 2009, p. 173 avec les observations de R. STEENNOT.

<sup>56</sup> Directive 2007/64/CE du Parlement et du Conseil du 13 novembre 2007 concernant les services de paiement dans le marché intérieur, JO L. 319 du 5 décembre 2007, pp. 0001 à 0036. Transposée en droit belge par la loi du 10 décembre 2009, MB 15 janvier 2010, entrée en vigueur le 1<sup>er</sup> avril 2010.

<sup>57</sup> Voy. à ce propos, G. HENNARD, "L'exécution d'opérations de paiement non autorisées et l'inexécution ou l'exécution incorrecte d'opérations de paiement – Analyse des dispositions de la PSD et comparaison avec le droit belge en vigueur", *Dr.banc.fin.* 2009, pp. 3 à 21.

<sup>58</sup> Art. 4(3) et annexe point 5 de la directive.

autorisée que si le payeur a donné son consentement”, ce consentement étant donné “sous la forme convenue entre le payeur et son prestataire de services de paiement”.

L'instrument de paiement est par ailleurs défini à l'article 4(23) de la directive comme “tout dispositif personnalisé et/ou ensemble de procédures convenue entre l'utilisateur de services de paiement et le prestataire de services de paiement auquel l'utilisateur de services de paiement a recours pour initier un ordre de paiement.” Cette disposition renvoie donc à la liberté contractuelle pour définir le dispositif personnalisé ou les procédures qui doivent permettre l'exécution d'un ordre de paiement. C'est entre l'utilisateur et le prestataire de services avec lequel il est en relation que le dispositif ou les procédures en questions doivent être convenues. Rappelons qu'à ce niveau, il n'existe aucune relation directe entre le titulaire de carte qui initie un ordre de paiement et l'acquéreur.

En cas d'opération non autorisée, c'est le payeur seul qui est protégé par les dispositions de la directive.

En vertu de l'article 59 de la directive, “les Etats membres exigent que lorsque l'utilisateur de services de paiement nie avoir autorisé une opération de paiement...il incombe à son prestataire de services de paiement de prouver que l'opération a été authentifiée”<sup>59</sup> et en vertu de l'article 60, “les Etats membres veillent à ce qu'en cas d'opération de paiement non autorisée, le prestataire de services de paiement du payeur rembourse immédiatement au payeur le montant de cette opération”.

En cas d'opération de paiement initié par ou via le bénéficiaire du paiement<sup>60</sup>, la responsabilité de son prestataire de services à son égard se limite à la transmission de l'ordre de paiement au prestataire de services de paiement du payeur dans les délais convenus entre eux<sup>61</sup>, à la mise à disposition

des fonds immédiatement après leur réception et au respect d'une date valeur qui “ne peut être postérieure à celle du jour ouvrable au cours duquel le montant de l'opération de paiement est crédité sur le compte du prestataire de services de paiement du bénéficiaire”<sup>62</sup>. Enfin, le prestataire de services du bénéficiaire doit en tout état de cause “s'efforcer, à la demande du bénéficiaire, de retrouver la trace de l'opération de paiement” non exécutée ou mal exécutée “et de notifier le résultat de sa recherche au bénéficiaire”<sup>63</sup>.

Notons enfin qu'en vertu de l'article 51 de la directive, lorsque l'utilisateur du service de paiement (payeur ou bénéficiaire) n'est pas un consommateur, les parties peuvent décider d'écarter, en tout ou en partie toute une série de dispositions de la directive et notamment l'article 75.

Pour toutes les questions non réglées par la directive ou pour celles à propos desquelles l'application des dispositions de la directive a été valablement écartée, c'est aux parties qu'il appartient de régler leur relation. Ce sera notamment le cas sur le point de savoir qui, du prestataire de services de paiement ou du bénéficiaire du paiement, supporte les risques d'utilisation frauduleuse de l'instrument de paiement, dans quelles limites et selon quelles conditions.

Rien dans le projet de loi relatif aux services de paiement qui transpose en droit belge les dispositions de la directive PSD ne permet de penser que le législateur belge s'écartera sur les points qui viennent d'être évoqués, du prescrit de la directive.

Tout porte donc à croire que le commerçant qui accepte un paiement par carte sans présence physique du titulaire et sans recourir à un système de signature sécurisé continuera à en supporter les risques.

Martine Delierneux et Jean-Pierre Buyle

<sup>59</sup>. L'art. 4(19) définit l'authentification comme étant “la procédure permettant au prestataire de services de paiement de vérifier l'utilisation d'un instrument de paiement donné, y compris ses dispositifs de sécurité personnalisés”.

<sup>60</sup>. Art. 75 (2) de la directive.

<sup>61</sup>. Art. 69 (3).

<sup>62</sup>. Art. 73 de la directive.

<sup>63</sup>. Art. 75 de la directive.