

**Berlin, 06. Februar 2009**

**Gesetz zur Umsetzung der aufsichtsrechtlichen Vorschriften  
der Zahlungsdiensterichtlinie**

**Stellungnahme des Verbraucherzentrale Bundesverbandes**

**zum Regierungsentwurf vom 16.01.2009**

## I. Zusammenfassung

Der Verbraucherzentrale Bundesverband (vzbv) begrüßt das Bestreben zur Schaffung eines einheitlichen Zahlungsverkehrs, auch wenn nicht alle Regelungen, die die Richtlinie dazu im Rahmen eines maximal harmonisierten Ansatzes dem deutschen Gesetzgeber vorgibt, im Interesse unseres bereits erreichten Schutz- und Vertrauensstandards sind. Diese Kritik am Entwurf zielt dabei schwerpunktmäßig auf den zivilrechtlichen Teil ab, zu dem wir uns im Rahmen des entsprechenden Verfahrens noch äußern werden.

Auch der aufsichtsrechtliche Teil impliziert aber bereits Aspekte von höchster Relevanz auch gegenüber dem Verbraucher. Wir beschränken uns nachfolgend auf diese besonderen Aspekte und weisen im Übrigen auf das Interesse der Verbraucher an Zahlungsdienstleistern hin, die zu jeder Zeit gewährleisten können, dass die Zahlungsbeträge tatsächlich dem Zugriff anderer, etwa von Gläubigern der Zahlungsdienstleister, entzogen sind.

### **Wesentliche Aspekte in der Zusammenfassung:**

#### **Verhinderung des Zahlungsverkehrs als ungeregelte Kreditverträge missbraucht werden können.** (Beispiel Kreditkarte)

Hier bedarf es im Wesentlichen nur einer treffenderen Formulierung der Norm, da die Bundesregierung in ihrer Begründung die Argumente aus unserer Sicht zutreffend dargestellt hat. Wir sprechen uns auch dafür aus, als Zahlungsdienstleistungen mit einer gewissen Kreditfunktion wirklich nur kurze Abrechnungszeiträume, d.h. vier statt der vorgeschlagenen zwölf Monate zuzulassen. Längere Kreditrahmen bleiben möglich, müssen dann aber von einem richtigen Kreditinstitut angeboten werden.

**Der Bundesrat will das Informationsfreiheitsgesetz gegenüber der Finanzaufsicht ausschließen, das Gegenteil wäre erforderlich.** Eine solche Einschränkung sieht die Richtlinie nicht vor und wir fordern umgekehrt, wie bisher leider nur bei den Versicherungen geregelt, den Schutz auch der Nutzer und der Funktionsfähigkeit des Zahlungsverkehrs als Aufgabe der Aufsicht zu verankern. Ferner brauchen wir neue Handlungsoptionen, wie die Warnung.

Eine Ergänzung betrifft ein Sicherheitsproblem von Anbietern, die sich heute schon z.B. PIN und TAN zur Abwicklung von Zahlungsdienstleistungen geben lassen. Dieses Angebot führt Verbraucher in ein großes Haftungsrisiko, ist aber nicht verboten. Für den Laien ist damit aber kaum erkennbar, wann er sich bei der Nutzung eines offen angebotenen Bezahlfahrgangs selbst gefährdet. **Wir brauchen eine Maßgabe, dass Anbieter auch in der Konkurrenzsituation die Sicherheitsvorgaben anderer Systeme achten und keine für den Verbraucher kaum noch nachvollziehbaren Risiken durch Zahlungsprodukte entstehen.**

## II. Handlungsbedarf im Einzelnen

### a) Verhinderung von Umgehungen der Vorgaben zum Kreditgeschäft

§ 1 Abs. 2 Ziff. 3 ZAG-E regelt, dass Zahlungsdienste auch Zahlungsvorgänge mit einer Kreditgewährung sein können. Einschränkungen zur Kreditgewährung sind in § 2 Abs. 3 ZAG-E festgelegt. Zahlungsdienstleistungen dürfen nicht zu einem verdeckten Kreditgeschäft mutieren. Die in der Begründung zum Gesetzentwurf zu Recht aufgeführten Abgrenzungskriterien finden sich in der Formulierung der Norm nicht wieder, so dass die Missbrauchsgefahr weiter besteht.

An Kreditkarten lässt sich das Problem heute am plastischsten erläutern.

Bei der Kreditkarte kennen wir in Deutschland heute zwei unterschiedliche Konzepte am Markt. Zum einen die Karte mit überwiegender Zahlungsfunktion, die Zahlungen des in der Regel laufenden Monats zusammenfasst und dann insgesamt und vollständig abrechnet. Hier tritt der Kredit hinter der Zahlungsfunktion zurück. Diese Karte hat zunächst bei uns Verbreitung gefunden.

Ferner gibt es zunehmend Angebote von Karten mit Teilzahlungsfunktion, die auch über einen kurzen Abrechnungszeitraum Beträge meist sehr hoch verzinst kreditieren und die von einer bestimmten Mindestbuchung abgesehen aktiv vom Verbraucher zurückzuführen sind.

Diese revolvingierenden Kredite sind dabei besonders schwer für den Verbraucher zu durchschauen, weil man sich nicht alleine über den ausstehenden Gesamtbetrag ein Bild über die Kreditverpflichtung und die anlaufenden Zinskosten machen kann. Vielmehr muss man jede einzelne Zahlung im Blick behalten, weil von deren Zeitpunkt mit abhängt, wie hoch und zu welchem Zeitpunkt ein Teilbetrag des Darlehensgesamtbetrages verzinst wird. Bei der Rückzahlung in Teilbeträgen kann dann schnell jeder Überblick verloren gehen. Die fehlende Transparenz dieses Konzeptes stellt eine Gefahr dar, sich zu überschulden, aber auch schlicht mehr als nötig zu zahlen. Gerade hier bedarf es der Informationspflichten und weiteren Anforderungen des Verbraucherkreditrechts und mit Sicherheit auch der Überwachung des nicht zu vernachlässigenden Kreditrisikos.

Es gilt streng zu vermeiden, dass auch kurzfristige Kreditmärkte, über solche Karten gestaltet und als Zahlungsdienste deklariert werden können, um den größeren Anforderungen, die von ein Kreditunternehmen gegenüber Verbraucher und Aufsicht zu erbringen sind, zu entgehen.

Die Zahlungsdiensterichtlinie hat dieses Problem erkannt und dazu Vorgaben formuliert, die es in der Praxis abzusichern gilt. Im 13. Erwägungsgrund der Richtlinie 2006/64/EU wird klargestellt, dass das Verbraucherkreditrecht im Verhältnis zu diesen Zahlungsdienstleistungen unberührt bleiben soll. Es sollen also keine Umgehungen gestaltet werden können.

Die erste Vorgabe, dass der Kredit nur eine Nebentätigkeit zum Zahlungsvorgang darstellen darf, wäre bereits nicht mehr erfüllt, wenn dem Kartenvertrag mehr als nur ein „technischer Kredit“ zu Grunde gelegt wird. In der Zusammenfassung zur Begründung dieser Norm wird dies deutlicher als im Normtext. Um diese Deutlichkeit

auch im Gesetz sicherzustellen, sollte überprüft werden, wie man insbesondere § 2 Abs. 3 Ziff. 2 ZAG-E strenger formulieren kann.

Zum einen sollte hier der Begriff „Kreditvertrag“ entfallen, weil damit ein Vertrag mit einem Kreditzweck und eben nicht primär einem Zahlungszweck konstatiert wird. Wesentlich vorsichtiger ist hier der Wortlaut der Richtlinie selbst, bei der Art. 16 Abs. 3 b) vom „mit der Zahlung gewährten Kredit“ spricht.

Die Rückzahlungsfrist hat „kurz“ zu sein und in keinem Fall 12 Monate zu überschreiten. Daher stellt es die Richtlinie frei, eine erheblich kürzere Frist als 12 Monate festzusetzen. Dabei soll diese Regelung auch verhindern, das Zahlungskarten z.B. eine langfristige jährliche Abrechnung gestalten und den mit einer solchen Zahlung verbundenen echten Kredit dann statt über einen Zins über eine entsprechende „Kartengebühr“ vergüten. Schon dies wird aber nur unvollständig mit einer 12 Monatsfrist verhindert.

**Wir fordern, dass der mit der Zahlung verbundene Kredit nicht länger als für vier Monate eingeräumt und in dieser Zeit jeweils vollständig zurückgeführt wird.**

Wir gehen bei unserem Ansatz davon aus, dass Zahlungsziele, die erheblich über ein Quartal hinaus gehen, bei uns keinen abrechnungstechnischen Hintergrund mehr haben, sondern das Ziel der Kreditierung überwiegt.

#### **b) Die Möglichkeiten der Finanzdienstleistungsaufsicht effektivieren, nicht einschränken**

Das in § 28 ZAG-E entworfene Beschwerdeverfahren reicht für sich noch nicht aus, Missstände in einem Zahlungsinstitut mit Ausstrahlung auf die Nutzer zu verhindern oder zu beseitigen. Strenggenommen gibt dieser Paragraph erstmal nur das verfassungsrechtlich ohnehin zu gewährleistenden Petitionsrecht wieder. Nicht einmal eine Antwort oder Reaktionsmöglichkeit wird darin vorgesehen.

Auch die in den §§ 3, 4, 5 und 6 ZAG-E geregelten Maßgaben über die Art der Aufsichtsführung und die Verschwiegenheitspflicht lassen eine effektiven Schutz auch des Marktes in Bezug Zahlungsdienstleistungen nicht zu.

Die Aufsicht hat zwar in § 3 Abs. 2 ZAG-E den Auftrag, nicht nur Verstöße gegen aufsichtsrechtliche Bestimmungen zu unterbinden, sondern auch die Sicherheit der anvertrauten Vermögenswerte zu sichern und Beeinträchtigungen der ordnungsgemäßen Durchführung der Zahlungsdienste abzuwenden. Die nachfolgenden Befugnisse stellen dann aber allesamt alleine auf unerlaubte Zahlungsdienstleistungen ab.

Generell sind wir überzeugt, dass die Ausklammerung der Marktnutzer aus der Aufgabensphäre einer Aufsicht keine adäquate Aufsichtsführung ermöglicht, um rechtzeitig auf Gefahren im Markt und für den Markt reagieren zu können. Bisher ist lediglich im Versicherungsbereich für die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) festgelegt, dass die Aufsicht auch die Wahrung des Interesses der Versicherten mit einschließt.

Nichts anderes muss aber gerade auch für den Zahlungsmarkt gelten. Risiken entstehen nicht alleine durch die wirtschaftlichen Engpässe der Anbieter, vielmehr führt jede sonstige Störung des Zahlungsverkehres zu einer Gefahr für seine Nutzer und den übrigen Markt. Nicht nur dem Verlust von Zahlungen ist vorzubeugen, sondern auch der verzögerten oder fehlerhaften Bearbeitung. Das Risiko ist jedenfalls nutzerbezogen genug, um sich hier unbedingt am Vorbild des § 81 VAG zu orientieren und **die Belange der Nutzer und die zuverlässige Funktionsfähigkeit der Zahlungsdienste** im Aufgabenkanon des § 3 ZAG-E ausdrücklich aufzunehmen.

Bei der Ausgestaltung der Eingriffsbefugnisse müssen wir mit Verwunderung feststellen, dass der Entwurf mehr Risiken für den Bundeshaushalt in Bezug auf eine Staatshaftung schafft, als erforderlich. Es ist davon auszugehen das BaFin und Bundesbank nach dem Grundsatz der Verhältnismäßigkeit generell die bisherigen Möglichkeiten als geringeren Eingriff einsetzen werden. Das gänzliche Fehlen von Auskunfts- und Warnrechten in den Normen dieser Aufsicht führt aber dazu, dass die Aufsicht nicht einmal in eindeutigen Fällen einer rechtswidrigen Schädigung Betroffenen helfen und andere warnen kann, ohne selbst Gefahr zu laufen, durch das Fehlen einer eindeutigen Befugnis hierzu von Nutzer schädigenden Unternehmen auch noch in Staatshaftung genommen zu werden.

In diesem Kontext verwahren wir uns gegen den Vorschlag von Seiten des Bundesrates, der genau diese Wirkung noch erhöht. Gerichte und der Bundesbeauftragte für den Datenschutz und das Informationsfreiheitsrecht sehen durchaus eine Auskunftspflicht der BaFin nach dem Informationsfreiheitsgesetz (IFG). Das IFG selbst wahrt dabei die berechtigten Interessen Dritter und betroffener Unternehmen. Ein Schutz vor der Entdeckung rechtswidriger Handlungen darf es aber nicht geben, zumal wenn Dritte dadurch geschädigt werden. **Das IFG muss auch für die Finanzdienstleistungsaufsicht weiter anwendbar bleiben.** Es gibt über die dort bereits vorgesehenen Einschränkungen keine weitere Notwendigkeit, eine Branche gegenüber allen anderen Branchen zu privilegieren. Nach der Finanzmarktkrise erscheint das nun sogar geradezu gefährlich.

Wenn Polizei und Ordnungsbehörden nicht in der Lage wären, wenigstens nach Abschluss der Ermittlungen, ermittelte Schädiger und bestimmte für die Abwicklung von Haftungsansprüchen nötige Informationen an Geschädigte weiterleiten zu können, wäre der Ausgleich gegenüber den Opfern erheblich gestört. Das Entschädigung wirklich zu leisten ist, hat schließlich **auch den generalpräventiven Effekt** andere erst gar nicht zu schädigen und dies **unterstützt dann auch die Stabilität und damit die Aufsichtszwecke der Finanzaufsicht.**

**Wir fordern daher, den Aufsichtsbehörden das Recht zur öffentlichen Warnung der Nutzer zu verschaffen, wenn anders eine Störung oder Gefahr für die Aufsichtsziele nach ihrem Ermessen nicht hinreichend sicher effektiv oder rechtzeitig genug abzuwenden ist.**

Ferner ist in Bezug auf die Verschwiegenheit zu § 6 ZAG-E klarzustellen, dass **Geschäfts- und Betriebsgeheimnisse die eine rechtswidrige Schädigung Dritter betreffen, vor dem Gesetz keinen Schutz genießen.**

### c) Sicherheitsmaßnahmen besser schützen

Für Verbraucher besteht die Gefahr, dass unbefugt Zahlungen in ihrem Namen getätigt werden. Neben der Betrugsgefahr besteht dabei auch das Risiko, unfreiwillig in einen Geldwäschevorgang einbezogen zu werden. Diese Gefahr wird erhöht, wenn die von einem Anbieter in seinem Sicherheitskonzept vorgesehenen Maßnahmen von einem anderen Anbieter aufgegriffen und zweckentfremdet werden dürfen. Die Aufsicht hat noch keine erkennbare Befugnis und Aufgabe dem entgegenzusteuern.

Es ist uns bereits in einem Fall ein konkretes Geschäftsmodell bekannt geworden, das die Sicherheitsmerkmale anderer Anbieter in einer Weise nutzt, das Sicherheitsgefahren bewirkt und den Verbraucher in ein besonderes Haftungsrisiko setzt. Dies betrifft das Geschäftsmodell eines Zahlungsdienstleisters, der für Internethändler ein Bezahlverfahren gestaltet, bei dem die Verbraucher ihre PIN und TAN zum Onlinebanking angeben sollen, damit der Anbieter anstelle des befugten Verbrauchers eine Überweisung ausführt und dem Anbieter die in der Regel nicht revidierbare Überweisung bestätigen kann. Man kann sich das etwa so vorstellen, dass sich der Händler vom Verbraucher einen unterschriebenen Blankoscheck ausstellen lässt, den er dann einlöst. Auf der Ebene einer Netzanwendung wird die Konsequenz dieser Methode aber nicht jedermann so deutlich. Leider besteht ergänzend noch die Verwechslungsgefahr mit einem anderen Modell, bei dem der Händler den Verbraucher auf dessen Bankseite leitet und seine Kontoangaben und den Zahlungsbetrag ähnlich wie bei einem vorbereiteten Überweisungsformular dabei zur Verfügung stellt. Auch hier „zahlt“ der Verbraucher mit seinen Onlinebanking Daten.

Weil diese Praxis aber nicht per se unzulässig ist, und damit angeboten werden kann, ahnt der Verbraucher als juristischer Laie nicht, dass ihm dieser Zahlungsdienst als Bruch seiner Sorgfaltspflicht und Verstoß gegen Sicherheitspflichten aus dem Kontovertrag vorgehalten werden kann.

**Die Verwendung von bestimmten Sicherheitsmerkmalen außerhalb des eigentlichen Verwendungszwecks schafft Tätern Angriffsflächen und kann zu einer vom Verbraucher nicht vermuteten Haftungsumkehr zu seinen Lasten führen.** Das technische und rechtliche Verständnis wird man nicht immer voraussetzen können, um die Gefahren selbst erkennen zu können. Eine allgemeine Praxis nivelliert zudem zusätzlich für den Laien die Erkennbarkeit einer Gefahr.

Ein zusätzliches Risiko für den Nutzer ergibt sich zu dem durch Geldwäsche. Aus Verbrauchersicht geht es dabei um die erhöhte Gefahr eines Identitätsdiebstahles. Im dargestellten Modell wäre der Mißbrauch zur Geldwäsche nämlich möglich, wenn ein unseriöser Anbieter das Modell kopiert oder ähnlich auf den Markt bringen würde. Die sogenannten Authentifizierungsmittel eines Verbrauchers könnten dann genutzt werden, um eine ganz andere Zahlung zu bewirken und den Vorgang gegenüber dem betroffenen Verbraucher als Fehler darzustellen, den man auch sofort wieder ausgleicht. Über diesen Weg wäre ein Zahlungsvorgang so verschleiert, dass eine Geldwäsche tatbestandlich vollzogen wäre.

Verbraucher sind auf praktikable und verständliche Sicherheitsvorkehrungen angewiesen. Und damit diese nicht unnötig selbst zur Gefahr werden, sollte es einen Schutz davor geben, dass diese Systeme nicht durch andere Modelle gefährdet

werden können. Allerdings darf ein Sicherheitssystem auch nicht verwendet werden, um damit Zugangsbarrieren für Konkurrenten aufzubauen. Einen solchen Zugangsschutz sieht aber § 7 ZAG-E bereits vor.

Der Gesetzentwurf formuliert auch technische Anforderungen an die Zahlungsdienstleister. Wir fordern, dass darin die **Wahrung der Integrität von Sicherheitsmaßnahmen auch Dritter zu beachten ist. Aus Dienstleistungen dürfen für den Verbraucher weder zusätzliche Betrugs- noch Identitätsdiebstahlsgefahren bei anderen Dienstleistungen erwachsen. Verbraucher dürfen auch nicht Opfer eines rechtlichen Haftungsrisikos werden, weil die Wahrnehmung eines zulässigen Angebots auf dem Markt gleichzeitig den Verstoß gegen die Obliegenheitspflichten gegenüber dem anderen Anbieter bedeuten würde.**