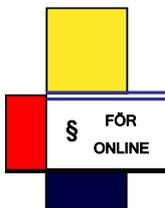


## Informations- und Datenschutzrecht

### Modul 8

# CyLaw-Report V : „Sicherheit von ec-Karten“



## CyLaw-Report V : „Sicherheit von ec-Karten“

### A. Haftung bei gestohlener ec-Karte - „Clear Case“

#### I. Sachverhalt

#### II. Zahlungsanspruch der K gegen B

#### III. Gegenansprüche der Bank?

1. Aufwendungsersatzanspruch (§§ 670, 675 Abs. 1, 676 f BGB)

2. Schadensersatzanspruch (§ 280 Abs. 1 BGB)

#### IV. Ergebnis

### B. Sicherheit von ec-Karten – „Hard Case“

#### I. Sachverhalt

#### II. Zahlungsanspruch der K gegen B

#### III. Aufwendungsersatzanspruch der B gegen K als Gegenanspruch

### IV. Schadensersatzanspruch der B gegen K als Gegenanspruch

#### 1. Pflichtverletzung

- a. Pflichtverletzung durch Weitergabe der PIN oder Selbstabhebung
- b. Pflichtverletzung durch sorgfaltswidrige Aufbewahrung
- c. Pflichtverletzung durch Vermerken der PIN auf der ec-Karte
- d. Pflichtverletzung durch gemeinsame Aufbewahrung von PIN und ec-Karte

#### 2. Anscheinsbeweis für eine Pflichtverletzung?

- a. Begriff des Anscheinsbeweises
- b. Typischer Geschehensablauf
- c. Erschütterung des Anscheinsbeweises

#### 3. Verschulden

#### 4. Ergebnis

### C. Schlussfolgerungen

## A. Haftung bei gestohlener ec-Karte - „Clear Case“

### I. Sachverhalt

Die Kundin K hat bei der Bank B ein Girokonto. In diesem Rahmen verfügt K auch über eine ec-Karte. Zur Benutzung der ec-Karte wurde K von B eine persönliche Geheimzahl (Persönliche Identifikationsnummer – PIN) per Post mitgeteilt. K merkt sich die PIN und vernichtet den Zettel, auf dem diese vermerkt war.

Der hoch verschuldete Mitarbeiter M von B hat aber zuvor heimlich den Umschlag mit der PIN geöffnet, sich diese gemerkt, den Umschlag – in für andere nicht erkennbarer Weise - wieder verschlossen und ihn erst dann an K geschickt. Um nicht entdeckt zu werden, wartet M einige Monate ab und verkauft dann die PIN an einen unbekanntenen Dieb D. D stiehlt der K bei der nächsten Gelegenheit die ec-Karte unbemerkt aus der Handtasche und hebt mit der Karte und der korrekten PIN sofort am nächsten Geldautomat 1.000 € ab.

B belastet das Girokonto der K mit den 1.000 €. K ist demgegenüber der Meinung, sie müsse nicht für den Fehlbetrag haften. Da D unbekannt ist und vom verschuldeten M auch keine Rückzahlung zu erwarten ist, verlangt K die Rückzahlung der 1.000 € von B.

## II. Zahlungsanspruch der K gegen B

§ FÜR  
ONLINE

Anspruch gem. §§ §§ 667, 675 Abs. 1, 676f BGB

### § 667 BGB [Herausgabepflicht]

Der Beauftragte ist verpflichtet, dem Auftraggeber alles, was er zur Ausführung des Auftrags erhält und was er aus der Geschäftsbesorgung erlangt, herauszugeben.

### § 675 BGB [Entgeltliche Geschäftsbesorgung]

(1) Auf einen Dienstvertrag oder einen Werkvertrag, der eine Geschäftsbesorgung zum Gegenstand hat, finden, soweit in diesem Untertitel nichts Abweichendes bestimmt wird, die Vorschriften der §§ 663, 665 bis 670, 672 bis 674 und, wenn dem Verpflichteten das Recht zusteht, ohne Einhaltung einer Kündigungsfrist zu kündigen, auch die Vorschrift des § 671 Abs. 2 entsprechende Anwendung.

(...)

5

## II. Zahlungsanspruch der K gegen B

§ FÜR  
ONLINE

### § 676f BGB [Vertragstypische Pflichten beim Girovertrag]

Durch den Girovertrag wird das Kreditinstitut verpflichtet, für den Kunden ein Konto einzurichten, eingehende Zahlungen auf dem Konto gutzuschreiben und abgeschlossene Überweisungsverträge zu Lasten dieses Kontos abzuwickeln. Es hat dem Kunden eine weitergeleitete Angabe zur Person des Überweisenden und zum Verwendungszweck mitzuteilen.

6

## II. Zahlungsanspruch der K gegen B

§ FÜR  
ONLINE

Für eine Einordnung des Girovertrages als Geschäftsbesorgungsvertrag sprechen folgende Argumente:

- Das mit „Girovertrag“ überschriebene Kapitel des BGB ist Bestandteil des Untertitels „Geschäftsbesorgungsvertrag“.
- Die Normen über den Girovertrag (§§ 676 f - h) enthalten keine Anspruchsgrundlage für die Kundin K, weshalb es eines Rückgriffs auf Geschäftsbesorgungsvertragsrecht bedarf.
- Eine Geschäftsbesorgung ist jede selbständige Tätigkeit wirtschaftlicher Art zur Wahrnehmung fremder Vermögensinteressen. Eine Bank ist selbständig im wirtschaftlichen Bereich tätig. Im Rahmen eines Girovertrages nimmt sie fremde Vermögensinteressen wahr. Die Bank führt Überweisungen für die Kunden aus und schreibt Zahlungseingänge auf deren Konten gut. Der Girovertrag stellt also einen Geschäftsbesorgungsvertrag dar.

7

## II. Zahlungsanspruch der K gegen B

§ FÜR  
ONLINE

- Die Herausgabeverpflichtung aus § 667 BGB ist im Girovertragsverhältnis anwendbar (§ 675 Abs. 1 BGB), weil B verpflichtet ist, alles herauszugeben, was sie zur Ausführung erhält oder aus der Geschäftsführung erlangt (§ 667 BGB). Hierunter fallen alle Geldbeträge, die K selbst oder ein Dritter auf das Girokonto einzahlt oder überweist. B muss das eingezahlte oder überwiesene Geld an K herausgeben. Die von D vorgenommene Abhebung an einem Geldautomaten war dabei noch keine Herausgabe, wie sie § 667 BGB fordert, denn die Auszahlung erfolgte weder an K noch aufgrund ihrer Anweisung. K hat also grundsätzlich einen Anspruch gegen B auf Zahlung von 1.000 € (§§ 667, 675 Abs. 1, 676f BGB).

8

### III. Gegenansprüche der Bank?

§ FÜR  
ONLINE

#### 1. Aufwendungsersatzanspruch (§§ 670, 675 Abs. 1, 676 f BGB)

##### § 670 BGB [Ersatz von Aufwendungen]

Macht der Beauftragte zum Zwecke der Ausführung des Auftrags Aufwendungen, die er den Umständen nach für erforderlich halten darf, so ist der Auftraggeber zum Ersatz verpflichtet.

##### § 676h BGB [Missbrauch von Zahlungskarten]

Das Kreditinstitut kann Aufwendungsersatz für die Verwendung von Zahlungskarten oder von deren Daten nur verlangen, wenn diese nicht von einem Dritten missbräuchlich verwendet wurden. (...)

##### § 675 BGB [Entgeltliche Geschäftsbesorgung]

(1) Auf einen Dienstvertrag oder einen Werkvertrag, der eine Geschäftsbesorgung zum Gegenstand hat, finden, soweit in diesem Untertitel nichts Abweichendes bestimmt wird, die Vorschriften der §§ 663, 665 bis 670, 672 bis 674 und, wenn dem Verpflichteten das Recht zusteht, ohne Einhaltung einer Kündigungsfrist zu kündigen, auch die Vorschrift des § 671 Abs. 2 entsprechende Anwendung.  
(...)

9

### III. Gegenansprüche der Bank?

§ FÜR  
ONLINE

#### 1. Aufwendungsersatzanspruch (§§ 670, 675 Abs. 1, 676 f BGB)

Die Bank, die die Ausgestaltung und Sicherheit des ec-Karten-Systems im Gegensatz zum Bankkunden beeinflussen und mitgestalten kann, trägt grundsätzlich das Missbrauchsrisiko. Im „Clear Case“-Szenario ist evident, dass es sich um einen Missbrauch handelt. B hat also keinen Aufwendungsersatzanspruch.

10

### III. Gegenansprüche der Bank?

§ FÜR  
ONLINE

#### 2. Schadensersatzanspruch (§ 280 Abs. 1 i.V.m § 276 BGB)

Nach Auffassung des BGH könnte B – auch wenn ihr kein Aufwendungsersatzanspruch zusteht – ein Schadensersatzanspruch zustehen (§ 280 Abs. 1 BGB) . Dieser ist nicht durch § 676h S. 1 BGB ausgeschlossen – setzt aber eine schuldhaft Verletzung vertraglicher Pflichten durch den Kunden voraus.

##### § 280 BGB [Schadensersatz wegen Pflichtverletzung]

(1) Verletzt der Schuldner eine Pflicht aus dem Schuldverhältnis, so kann der Gläubiger Ersatz des hierdurch entstehenden Schadens verlangen. Dies gilt nicht, wenn der Schuldner die Pflichtverletzung nicht zu vertreten hat. (...)

##### § 276 BGB [Verantwortlichkeit des Schuldners]

(1) Der Schuldner hat Vorsatz und Fahrlässigkeit zu vertreten, wenn eine strengere oder mildere Haftung weder bestimmt noch aus dem sonstigen Inhalt des Schuldverhältnisses, insbesondere aus der Übernahme einer Garantie oder eines Beschaffungsrisikos, zu entnehmen ist. (...)

(2) Fahrlässig handelt, wer die im Verkehr erforderliche Sorgfalt außer Acht lässt. (...)

11

### III. Gegenansprüche der Bank?

§ FÜR  
ONLINE

#### 2. Schadensersatzanspruch (§ 280 Abs. 1 i.V.m § 276 BGB)

Demzufolge hat die Bank bei schuldhaftem Fehlverhalten des Kunden, das einen Missbrauch ermöglicht, einen Gegenanspruch und muss im Ergebnis nicht haften. Anhaltspunkte für eine Pflichtverletzung der K, die zu dem Missbrauch geführt oder ihn begünstigt haben könnte, sind nicht ersichtlich. Das bloße Mitnehmen der ec-Karte in der Handtasche kann nach Ansicht des BGH – ohne das Hinzutreten weiterer Umstände - kein schuldhaftes Fehlverhalten darstellen, das eine Schadensersatzpflicht auslöst. Diese Rechtsprechung überzeugt, da die ec-Karte gerade dazu dient, mitgenommen zu werden, um sich vor dem Diebstahl von Bargeld zu schützen. Der Missbrauch wurde im Gegenteil durch eine Ursache aus der Sphäre der Bank – das Verhalten des M – ermöglicht.

12

Da Gegenansprüche der B ausscheiden, hat K einen Anspruch auf Zahlung von 1.000 € gegen B (§§ 667, 675 Abs. 1, 676f BGB).

## B. Sicherheit von ec-Karten – „Hard Case“

### I. Sachverhalt

Die Kundin K unterhält bei der Bank B ein Girokonto. Im November 1999 erhält K von B auch eine ec-Karte und die zugehörige PIN. Dabei weist B auf ihre Allgemeinen Geschäftsbedingungen (AGB) hin. Diese enthalten folgende Regelungen:

*„Für Schäden, die vor der Verlustanzeige entstanden sind, haftet der Kontoinhaber, wenn sie auf einer schuldhaften Verletzung seiner Sorgfalts- und Mitwirkungspflichten beruhen. (...)*

*Die Sparkasse übernimmt auch die vom Kontoinhaber zu tragenden Schäden, die vor der Verlustanzeige entstanden sind, sofern der Karteninhaber seine Sorgfalts- und Mitwirkungspflichten (...) nicht grob fahrlässig verletzt hat.*

*Grobe Fahrlässigkeit des Karteninhabers liegt insbesondere vor, wenn*

- die persönliche Geheimzahl auf der ec-Karte vermerkt oder zusammen mit der ec-Karte verwahrt war (z.B. der Originalbrief, in dem die PIN dem Karteninhaber mitgeteilt wurde),*
- die persönliche Geheimzahl einer anderen Person mitgeteilt und der Missbrauch dadurch verursacht wurde, (...)*“

## B. Sicherheit von ec-Karten – „Hard Case“

§ FÜR  
ONLINE

### I. Sachverhalt

Am 23.09.2000 zwischen 15.00 Uhr und 17.00 Uhr werden K auf einem Stadtfest ihr Portemonnaie und die darin befindliche ec-Karte gestohlen. Gegen 17.30 Uhr werden mit der ec-Karte der K je 500 DM an den Geldautomaten zweier Banken abgehoben, wobei jeweils ohne Fehlversuch sofort die richtige PIN eingegeben wird. Am Morgen des 24.09.2000 werden weitere 1.000 DM abgehoben, wiederum unter Verwendung der richtigen PIN ohne Fehlversuch. Am 25.09.2000 veranlasst K die Sperrung ihrer ec-Karte. B belastet das Girokonto der K mit den insgesamt abgehobenen 2.000 DM. K verlangt von B die Rückzahlung des Geldes.

15

### II. Zahlungsanspruch der K gegen B

§ FÜR  
ONLINE

K hat zunächst einen Anspruch gegen B auf Zahlung von 2.000 DM (§§ 667, 675 Abs. 1, 676f BGB). Die auf dem Girokonto der K eingehenden Geldbeträge erlangt B nur in Ausführung der Vermögensgeschäfte der K. B muss das aus der Geschäftsführung Erlangte an K herausgeben (siehe oben unter A II)

16

### III. Aufwendungsersatzanspruch der B gegen K als Gegenanspruch (§§ 670, 675 Abs. 1, 676f BGB)

§ FÜR ONLINE

Ein Anspruch auf Aufwendungsersatz (§§ 670, 675 Abs. 1, 676f BGB) gegen K steht B nicht zu. Das ergibt sich aus § 676h S. 1 BGB. Da die ec-Karte gestohlen wurde, handelte es sich um unbefugte Abhebungen, hinsichtlich derer § 676h BGB den Ersatz von Aufwendungen ausschließt.

17

### IV. Schadensersatzanspruch der B gegen K als Gegenanspruch (§ 280 Abs. 1 i.V.m § 276 BGB)

§ FÜR ONLINE

#### 1. Pflichtverletzung: a. Pflichtverletzung durch Weitergabe der PIN oder Selbstabhebung

**BGH:**

„Die Beklagte hat nicht bewiesen, dass die hier in Rede stehenden Geldabhebungen von der Klägerin selbst oder mit ihrem Einverständnis durch einen Dritten vorgenommen worden sind. Vielmehr ist das Berufungsgericht zu der Feststellung gelangt, dass die Geldabhebungen durch einen unbefugten Dritten, nämlich den Dieb oder einen Komplizen mit Hilfe der Original-ec-Karte, erfolgt sind.“

18

## 1. Pflichtverletzung

§ FÜR  
ONLINE

### b. Pflichtverletzung durch sorgfaltswidrige Aufbewahrung

K könnte durch eine unsachgemäße Aufbewahrung der ec-Karte eine Pflichtverletzung begangen haben. Die Aufbewahrung der ec-Karte im Portemonnaie könnte sorgfaltswidrig gewesen sein. Allerdings ist ungewiss, wie genau K das Portemonnaie und die ec-Karte zum Zeitpunkt des Diebstahls aufbewahrt hatte. Allein aus der Tatsache, dass K das Portemonnaie auf dem Stadtfest entwendet wurde, kann nach dem BGH noch kein Rückschluss darauf gezogen werden, dass K den Diebstahl irgendwie durch sorgfaltswidrigen Umgang mit der ec-Karte begünstigt hat.

19

## 1. Pflichtverletzung

§ FÜR  
ONLINE

### c. Pflichtverletzung durch Vermerken der PIN auf der ec-Karte

#### **K behauptet:**

„Ihre persönliche Geheimzahl habe sie nirgendwo notiert, sondern ausschließlich als Telefonnummer in ihrem Mobiltelefon gespeichert gehabt. Dieses sei nicht gestohlen worden. Der Dieb müsse die persönliche Geheimzahl entschlüsselt haben oder Mängel des Sicherheitssystems der Beklagten zur Geheimhaltung des Institutsschlüssels ausgenutzt haben.“

Nach dieser Darstellung der K läge keine Pflichtverletzung vor, da sie die PIN nicht auf der ec-Karte notiert hatte. Die Speicherung im Mobiltelefon kann keine Pflichtverletzung begründen, da das Notieren oder Speichern der PIN nicht grundsätzlich eine Pflichtverletzung darstellt. Nur die gemeinsame Verwahrung mit der ec-Karte wäre eine Pflichtverletzung.

20

## 1. Pflichtverletzung

§ FÜR  
ONLINE

### d. Pflichtverletzung durch gemeinsame Aufbewahrung von PIN und ec-Karte

K könnte durch die gemeinsame Aufbewahrung von PIN und ec-Karte eine Pflichtverletzung begangen haben. In der gemeinsamen Aufbewahrung wäre nach den AGB eine Pflichtverletzung zu sehen. K bestreitet aber eine gemeinsame Aufbewahrung von PIN und ec-Karte. Danach läge keine Pflichtverletzung vor.

21

## 2. Anscheinsbeweis für eine Pflichtverletzung?

§ FÜR  
ONLINE

### a. Begriff des Anscheinsbeweises

Das Verhalten der K ist für das Gericht nicht feststellbar. Die Vorgehensweise des Diebes, die ebenfalls darüber Aufschluss geben könnte, ob ein sorgfaltswidriges Verhalten der K ausgenutzt wurde, ist unbekannt. Da die Bank B einen Schadensersatzanspruch gegen K geltend macht, muss die Bank B als Anspruchstellerin ihren Anspruch vor Gericht beweisen. Dazu ist aber die Bank, die im Gegensatz zu K und dem Dieb an dem schädigenden Vorgang überhaupt nicht beteiligt war, am allerwenigsten in der Lage. Zu Gunsten der Bank könnte ein Anscheinsbeweis in Betracht kommen. Grundlage eines Anscheinsbeweises ist ein typischer Geschehensablauf, der nach der allgemeinen Lebenserfahrung den Schluss auf eine bestimmte Ursache oder einen bestimmten Erfolg zulässt, da andere Möglichkeiten als fern liegend anzusehen sind.

22

## 2. Anscheinsbeweis für eine Pflichtverletzung?

§ FÖR  
ONLINE

### a. Begriff des Anscheinsbeweises

#### **BGH:**

„Nach ständiger Rechtsprechung des Bundesgerichtshofs sind die Grundsätze über den Beweis des ersten Anscheins nur bei typischen Geschehensabläufen anwendbar, d.h. in Fällen, in denen ein bestimmter Sachverhalt feststeht, der nach der allgemeinen Lebenserfahrung auf eine bestimmte Ursache oder auf einen bestimmten Ablauf als maßgeblich für den Eintritt eines bestimmten Erfolges hinweist. Dabei bedeutet Typizität nicht, dass die Ursächlichkeit einer bestimmten Tatsache für einen bestimmten Erfolg bei allen Sachverhalten dieser Fallgruppe notwendig immer vorhanden ist; sie muss aber so häufig gegeben sein, dass die Wahrscheinlichkeit, einen solchen Fall vor sich zu haben, sehr groß ist.“

23

## 2. Anscheinsbeweis für eine Pflichtverletzung?

§ FÖR  
ONLINE

### b. Typischer Geschehensablauf

Fraglich ist, ob sich aus der Tatsache, dass der Dieb die korrekte PIN ohne Fehlversuch zur Geldabhebung benutzte, der Rückschluss ziehen lässt, dass der Dieb die PIN – weil sie von K auf der ec-Karte vermerkt oder mit dieser zusammen verwahrt wurde – durch das Verhalten der K erlangt hat. Ob sich dieser Rückschluss ziehen lässt, ist anhand der möglichen Geschehensabläufe zu beurteilen. Ergeben sich danach für derartige Fälle keine sonstigen ernsthaft in Betracht kommenden Geschehensabläufe, liegt die für einen Anscheinbeweis erforderliche Typizität vor. K könnte eine Reihe von Einwänden vorbringen:

24

## 2. Anscheinsbeweis für eine Pflichtverletzung?

§ FÜR  
ONLINE

### b. Typischer Geschehensablauf

#### ➤ Entschlüsseln der PIN

Der Täter könnte die PIN entschlüsselt haben. Auf dem Magnetstreifen einer ec-Karte sind Daten vorhanden, die zur Authentifizierung des Berechtigten dienen. Diese Daten sind sehr einfach mit einem Kartenlesegerät auslesbar. Der Täter könnte also auf mathematischem Wege die PIN herausgefunden haben. Nach Aussagen von Sachverständigen war dies zum Tatzeitpunkt unmöglich, jedenfalls nicht innerhalb von 2 ½ Stunden, die vorliegend höchstens zwischen Diebstahl und erster Abhebung vergangen sind. Die PIN kann nicht aus den auf der Karte enthaltenen Daten errechnet werden.

25

## 2. Anscheinsbeweis für eine Pflichtverletzung?

§ FÜR  
ONLINE

### b. Typischer Geschehensablauf

Dazu ist der Institutsschlüssel der jeweiligen Bank nötig. Dieser 128-Bit-Schlüssel konnte nach den Aussagen des Sachverständigen zum damaligen Zeitpunkt – selbst bei größtem technischem und finanziellem Aufwand – nicht errechnet werden. Das verwendete Verschlüsselungsverfahren Triple-DES gilt – anders als das bis 1997 verwendete DES-Verfahren mit 56-Bit-Institutsschlüssel – als sicher. Insoweit kommt es auch nicht auf den technischen Fortschritt an, der auch das derzeitige Verfahren unsicher werden lassen könnte. Jedenfalls zum damaligen Zeitpunkt war das Verfahren – soweit ersichtlich – sicher. Nach Ansicht des BGH scheidet eine Entschlüsselung der PIN als möglicher Geschehensablauf aus.

26

## 2. Anscheinsbeweis für eine Pflichtverletzung?

§ FÜR  
ONLINE

### b. Typischer Geschehensablauf

#### ➤ Ausspähen der PIN

Ein weiterer denkbarer Geschehensablauf könnte auch ein vorheriges Ausspähen der PIN durch den Täter sein. Dies ist in vielen Fällen einfach möglich, entweder durch Nutzung von Bankautomaten oder PIN-Eingabeterminals in Geschäften, die keinen Sichtschutz bieten, oder durch eigene Unvorsicht des Karteninhabers. Auch mit verdeckten Kameras arbeiten Täter. Ein Ausspähen ist zwar leicht möglich, K hat dies in der Entscheidung des BGH aber für ausgeschlossen gehalten. Laut BGH ist ein Ausspähen jedenfalls nur dann als ernsthaft möglicher Geschehensablauf anzusehen, wenn ein näherer zeitlicher Zusammenhang zwischen dem Kartendiebstahl und einer Ausspähung Gelegenheit besteht:

27

## 2. Anscheinsbeweis für eine Pflichtverletzung?

§ FÜR  
ONLINE

### b. Typischer Geschehensablauf

#### **BGH:**

„Als ernsthafte Möglichkeit einer Schadensursache, die den Beweis des ersten Anscheins für eine grob fahrlässige gemeinsame Verwahrung von ec-Karte und PIN durch den Karteninhaber bei Eingabe der zutreffenden PIN durch einen unbefugten Dritten entfallen lässt, kommt ein Ausspähen der PIN aber nur dann in Betracht, wenn die ec-Karte in einem näheren zeitlichen Zusammenhang mit der Eingabe der PIN durch den Karteninhaber entwendet worden ist. Durch Ausspähen erlangt der Täter zunächst nur Kenntnis von der PIN, gelangt aber nicht in den Besitz der ec-Karte. Da er den Karteninhaber regelmäßig nicht persönlich kennt, muss er die ec-Karte alsbald nach dem Ausspähen der PIN entwenden.“

28

## 2. Anscheinsbeweis für eine Pflichtverletzung?

§ FÜR  
ONLINE

### b. Typischer Geschehensablauf

#### ➤ Erraten der PIN

Auch ein Erraten der PIN kommt mit dem neuen PIN-Verfahren nicht mehr ernsthaft als Geschehensablauf in Betracht. Während mit dem alten Verfahren die Wahrscheinlichkeit, die PIN zu erraten, unter Umständen auf 1:150 sinken konnte, ist dies mit dem aktuellen Verfahren nicht möglich. Bei einer vierstelligen PIN ergeben sich 10.000 mögliche Kombinationen. Da die PIN „0000“ nicht vergeben wird und jeweils drei Versuche zur Eingabe der PIN freistehen, besteht eine theoretische Wahrscheinlichkeit von 1:3.333, die PIN zu erraten. Da das genaue Verfahren von den Banken nicht offen gelegt wird, ist unklar, ob die theoretische Wahrscheinlichkeit auch höher liegen kann.

Der BGH ist in seiner Entscheidung auf diese Möglichkeit nicht näher eingegangen. Der Geschehensablauf des Erratens der PIN könnte aber im Hinblick auf die – auf die Masse der Fälle bezogen – geringe Wahrscheinlichkeit als atypisches Geschehen angesehen werden.

29

## 2. Anscheinsbeweis für eine Pflichtverletzung?

§ FÜR  
ONLINE

### b. Typischer Geschehensablauf

#### ➤ „Innentäterattacke“ und Substantiierungspflicht der Bank

In Betracht kommen auch „Innentäterattacken“, das heißt Angriffe von Bankmitarbeitern gegen den Institutsschlüssel. Die Sicherheit des Verschlüsselungsverfahrens zur Generierung der PIN und Authentifizierung des Berechtigten hängt neben der Sicherheit des verwendeten mathematischen Verfahrens maßgeblich von der organisatorischen Sicherheit ab. Der BGH hat insoweit die Ausführungen des Sachverständigen in der vorangegangenen Instanz für ausreichend erachtet, zumal es keinerlei konkrete Hinweise auf eine solche Innentäterattacke (etwa eine Häufung der Diebstähle von ec-Karten einer bestimmten Bank) gab. Der BGH hat dabei erkannt, dass der nicht in die internen Abläufe der Bank eingeweihte Karteninhaber oftmals Schwierigkeiten haben wird, Sicherheitslücken aufzudecken. Der BGH fordert von der Bank, dass sie über interne Abläufe Auskunft geben muss:

30

## 2. Anscheinsbeweis für eine Pflichtverletzung?

§ FÜR  
ONLINE

### b. Typischer Geschehensablauf

#### **BGH:**

„Nach ständiger Rechtsprechung des Bundesgerichtshofs zur sekundären Darlegungslast kann es Sache einer nicht primär darlegungs- und beweispflichtigen Partei sein, sich im Rahmen der ihr nach § 138 Abs. 2 ZPO obliegenden Erklärungspflicht zu den Behauptungen der beweispflichtigen Partei konkret zu äußern, wenn diese außerhalb des von ihr vorzutragenden Geschehensablaufs steht und keine nähere Kenntnis der maßgebenden Tatsachen besitzt, ihr Prozessgegner aber die wesentlichen Umstände kennt und es ihm zumutbar ist, dazu nähere Angaben zu machen. Das gilt auch für das kartenausgebende Kreditinstitut hinsichtlich der von ihm – im Rahmen des Zumutbaren und gegebenenfalls in verallgemeinernder Weise – darzulegenden Sicherheitsvorkehrungen. Dadurch wird der Karteninhaber in die Lage versetzt, Beweis für von ihm vermutete Sicherheitsmängel antreten zu können. Das Kreditinstitut wird zudem aus dem mit dem Karteninhaber bestehenden Girovertrag regelmäßig als verpflichtet anzusehen sein, sämtliche in seinem Besitz befindlichen technischen Aufzeichnungen, die die streitigen oder vorangegangene Auszahlungsvorgänge betreffen oder hierüber Aufschluss geben können, bis zur Klärung der Angelegenheit aufzuheben und dem Kontoinhaber gegebenenfalls auch zugänglich zu machen.“

31

## 2. Anscheinsbeweis für eine Pflichtverletzung?

§ FÜR  
ONLINE

### b. Typischer Geschehensablauf

Die Bank kann aber nach Ansicht des BGH nicht auf Grund von jeder entfernten, rein theoretischen Möglichkeit einer Sicherheitslücke zur Auskunft verpflichtet werden. K hätte ihre Behauptung anhand irgendwelcher Anhaltspunkte näher darlegen müssen. Ansonsten könnte der Karteninhaber ja immer „ins Blaue hinein“ Sicherheitsmängel behaupten und so die Bank zur Offenbarung des Systems zwingen, um dann erst nach einer Schwachstelle darin zu suchen.

Eine Innentäterattacke scheidet hier als anderer Geschehensablauf aus.

32

## 2. Anscheinsbeweis für eine Pflichtverletzung?

§ FÜR  
ONLINE

### b. Typischer Geschehensablauf

#### ➤ **Bekanntheit des Institutsschlüssels**

Auch eine Bekanntheit des Institutsschlüssels in kriminellen Kreisen, etwa auf Grund einer Innentäterattacke, ist nach Ansicht des BGH, mangels irgendwelcher Anhaltspunkte hierfür, kein denkbarer abweichender Geschehensablauf.

33

## 2. Anscheinsbeweis für eine Pflichtverletzung?

§ FÜR  
ONLINE

### b. Typischer Geschehensablauf

#### ➤ **Ergebnis**

Der BGH kommt daher zu dem Ergebnis, dass ein typischer Geschehensablauf gegeben ist, dergestalt, dass die Kenntnis des Täters von der PIN typischerweise auf dem Vermerk der PIN auf der Karte oder einer gemeinsamen Aufbewahrung beruht.

#### **BGH:**

„Die Grundsätze über den Anscheinsbeweis sind entgegen der Auffassung der Revision nicht deshalb unanwendbar, weil es mehrere theoretische und praktische Möglichkeiten der Kenntniserlangung von der persönlichen Geheimzahl durch einen Dritten gibt. Zu Recht ist das Berufungsgericht vielmehr zu dem Ergebnis gelangt, dass die hier in Rede stehenden Bargeldabhebungen mit Hilfe der Original-ec-Karte und richtiger PIN durch einen unbefugten Dritten anders als durch ein grob fahrlässiges Verhalten der Klägerin nicht zu erklären seien, weil andere Ursachen zwar theoretisch möglich seien, bei wertender Betrachtung aber außerhalb der Lebenserfahrung lägen.“

34

## 2. Anscheinsbeweis für eine Pflichtverletzung?

§ FÜR  
ONLINE

### c. Erschütterung des Anscheinsbeweises

#### **BGH:**

„Spricht ein Anscheinsbeweis für einen bestimmten Ursachenverlauf, kann der Inanspruchgenommene diesen entkräften, indem er Tatsachen darlegt und gegebenenfalls beweist, die die ernsthafte, ebenfalls in Betracht kommende Möglichkeit einer anderen Ursache nahelegen. Der Anscheinsbeweis kann auch erschüttert werden, wenn unstreitig oder vom Inanspruchgenommenen bewiesen ist, dass ein schädigendes Ereignis durch zwei verschiedene Ursachen mit jeweils typischen Geschehensabläufen herbeigeführt worden sein kann und jede für sich allein den Schaden verursacht haben kann; haftet der Inanspruchgenommene in einem solchen Fall nur für eine der möglichen Ursachen, sind die Regeln über den Anscheinsbeweis nicht anwendbar. Dabei kommt es nicht darauf an, ob die eine oder andere Verursachungsmöglichkeit nach den Erfahrungen des täglichen Lebens die wahrscheinlichere ist.“

35

## 2. Anscheinsbeweis für eine Pflichtverletzung?

§ FÜR  
ONLINE

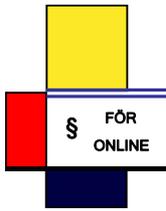
### c. Erschütterung des Anscheinsbeweises

Diese Erschütterung des Beweises des ersten Anscheins ist K aber nicht gelungen. Die von ihr behaupteten Geschehensabläufe

- Entschlüsselung der PIN,
- Ausspähen der PIN,
- Erraten der PIN,
- Innentäterattacke oder
- Bekanntheit des Institutsschlüssels

waren nach Ansicht des BGH entweder nicht oder so pauschal nicht geeignet, einen anderen Geschehensablauf als so ernsthaft möglich erscheinen zu lassen, dass der Anscheinsbeweis entkräftet wird.

36



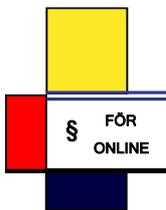
### 3. Verschulden

K müsste schuldhaft gehandelt haben. K haftet nach den AGB der B nur für Vorsatz und grobe Fahrlässigkeit. Beide typischen Geschehensabläufe – das Notieren der PIN auf der ec-Karte wie die gemeinsame Aufbewahrung von beidem – müssten als grob fahrlässig anzusehen sein. In der Kommentarliteratur:

*„Grobe Fahrlässigkeit liegt vor, wenn die verkehrserforderliche Sorgfalt in besonders schwerem Maße verletzt wird. Das ist der Fall, wenn schon einfachste, ganz nahe liegende Überlegungen nicht angestellt werden und das nicht beachtet wird, was im gegebenen Fall jedem hätte einleuchten müssen.“*

Die AGB der B stufen beide Verhaltensweisen als grob fahrlässig ein. Auch der BGH nimmt grobe Fahrlässigkeit an:

37



### 3. Verschulden

**BGH:**

„Das Vermerken der persönlichen Geheimzahl auf der ec-Karte oder ihre Verwahrung zusammen mit dieser stellt – wovon auch Nr. A. III. 2.4 der Bedingungen für die Verwendung der ec-Karte ausgeht – eine grobe Fahrlässigkeit des Karteninhabers dar; dabei trägt die Bewertung dieser Handlungsweisen als grob fahrlässig dem Umstand Rechnung, daß dadurch der besondere Schutz, den die für Abhebungen neben der ec-Karte zusätzlich benötigte Geheimnummer bietet, aufgehoben wird, weil ein Unbefugter, dem ec-Karte und Geheimnummer gemeinsam in die Hände fallen, ohne weiteres Abhebungen vornehmen kann.“

38

## 4. Ergebnis

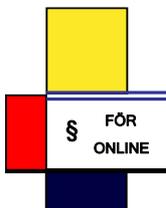


B hat daher einen Schadensersatzanspruch gegen K in Höhe von 2.000 DM wegen Verletzung von Sorgfaltspflichten (§ 280 Abs. 1 BGB). Diesen Anspruch durfte B in das Kontokorrent des Girokontos der K einstellen und das Konto entsprechend belasten.

K hat keinen Anspruch gegen B auf Rückzahlung dieser 2.000 DM.

39

## C. Schlussfolgerungen



➤ Wird bei der Verwendung einer gestohlenen ec-Karte vom Täter die korrekte PIN ohne Fehlversuch eingegeben, spricht ein Anscheinsbeweis dafür, dass der Karteninhaber entweder die PIN auf der ec-Karte notiert hatte oder die PIN mit der ec-Karte gemeinsam aufbewahrt hat.

➤ Ein Ausspähen der PIN kommt nur dann als möglicher anderer Geschehensablauf ernsthaft in Betracht, wenn der Diebstahl der ec-Karte in einem näheren zeitlichen Zusammenhang mit einer PIN-Eingabe steht.

➤ Das ec-Karten-Verfahren ist hinsichtlich der zur Generierung der PIN und zur Authentifizierung des Berechtigten verwendeten kryptographischen Verfahrens als sicher anzusehen.

➤ Um den Anscheinsbeweis wegen sonstiger organisatorischer Sicherheitsmängel des ec-Karten-Systems zu erschüttern, muss der Karteninhaber konkret darlegen, worin diese Sicherheitsmängel bestehen sollen. Die Bank ist dann im Rahmen der so genannten sekundären Darlegungslast verpflichtet, ihre Sicherheitsvorkehrungen offen zu legen.

40



Prof. Dr. Viola Schmid, LL.M.

Fachgebiet Öffentliches Recht

## Informations- und Datenschutzrecht

### Modul

# CyLaw-Report V : „Sicherheit von ec-Karten“