

## Keine grobe Fahrlässigkeit bei gemeinsamer Aufbewahrung der EC-Karte mit hinreichend verschlüsselter Geheimzahl

– Katja Fohrer, Fachanwältin für Bank- und Kapitalmarktrecht, Kanzlei Mattil & Kollegen München –

Chipkartentechnik bietet keine ausreichende Sicherheit vor Missbrauch bei Kartendiebstahl – Geldabhebung auch ohne Original-PIN möglich. Im Streit um Erstattungsansprüche bei EC-Kartenmissbrauch gab das **AG München** der Klage eines Bankkunden auf Zahlung von 1.011 € überwiegend statt und verurteilte die beklagte Bank zur Zahlung in Höhe von 861 €. In diesem von der Verfasserin geführten Verfahren ging es u. a. um die Fragen, ob es eine grobe Fahrlässigkeit des Bankkunden darstellt, wenn er seine PIN hinreichend verschlüsselt notiert und zusammen mit seiner EC-/ oder Kreditkarte im Geldbeutel aufbewahrt, und ob es möglich ist, mit einer gestohlenen Zahlkarte ohne Kenntnis der PIN am Geldautomaten Geld abzuheben.

Der mathematisch versierte Kläger hatte seine PIN (4438) in Primzahlen (2, 7, 317) zerlegt, diese Primzahlen zusammenhanglos (27317) auf einem handschriftlichen Zettel zusammen mit Telefonnummern notiert und die Notiz zusammen mit der EC-Karte im Geldbeutel aufbewahrt. Nur 18 Minuten nach dem Diebstahl des Geldbeutels in Italien haben Diebe mit der EC-Karte 1.000 € am Geldautomaten abgehoben. Die Hausbank des Klägers verweigerte die Zahlung und berief sich auf grobe Fahrlässigkeit. Sie behauptete, der Kläger habe die PIN zusammen mit der Karte aufbewahrt, anders sei es nicht zu erklären, dass die Diebe mit der Karte unter Eingabe einer PIN Geld abheben konnten. Die Bank berief sich dabei auf eine alte Rechtsprechung des **BGH** zum sog. Anscheinsbeweis aus dem Jahr 2004 (BGH Urteil vom 5.10.2004, Az. XI ZR 210/03, BGH Urteil vom 29.11.2011, Az. XI ZR 370/10), wonach bei einem Kartendiebstahl und kurz darauf erfolgter Abhebung bei Einsatz der Originalkarte der erste Anschein dafür spreche, der Bankkunde habe die PIN zusammen mit der Karte aufbewahrt habe. Die Chipkartentechnik sei sicher, die PIN aus Chipkarten könne nicht ausgelesen werden. Sie verweigerte vehement die Rückzahlung, des relativ geringen Betrages (1.011 €, d. h. 2 x 500 € zzgl. 2 x Abhebegebühr im Ausland 5,50 €), obwohl sie seit über 40 Jahren die Hausbank des Kunden war.

Das AG München hat mit Urteil vom 02.06.2023, Az. 142 C 19233/19 entschieden, dass die Bank dem Kunden nach dem Kartendiebstahl von den Betrügern abgebuchten Betrag erstatten muss, abzgl. eines Betrages von 150,- € (eine Art gesetzlich vorgesehener Selbstbehalt, vgl. § 675 v Abs. 1 **BGB** a. F., der seit 2018 vom Gesetzgeber zugunsten der Verbraucher mittlerweile auf 50,- € reduziert wurde). Das Urteil ist noch nicht rechtskräftig.

Entgegen der Ansicht der Bank greife der nach der Rechtsprechung des **Bundesgerichtshofs** mögliche Anscheinsbeweis, der Kläger habe die persönliche Geheimzahl (unverschlüsselt) auf seiner EC-Karte vermerkt oder sie zusammen mit dieser verwahrt, im vorliegenden Fall nicht. Denn die Annahme des Anscheinsbeweises setze voraus, dass der Missbrauch unter Verwendung der Originalkarte und der zutreffenden Geheimzahl erfolgt sei. Da der Kläger diese Umstände bestritten habe, müsse die Bank den Beweis dafür erbringen.

Die beklagte Bank konnte nach Ansicht des Gerichts aber nicht nachweisen, dass die unbekanntes Täter auch die korrekte Geheimzahl des Klägers in Erfahrung gebracht und zur Auszahlung verwendet haben. Die von der Bank vorgelegten Vorgangsprotokolle und darin genannten Kürzel, die der Bank über einen externen Dienstleister zur Verfügung gestellt und von diesem ausgewertet wurden, sah das Gericht nicht als ausreichenden Nachweis für die Eingabe der korrekten Geheimzahl an, denn aus dem darin genannten Kürzel ergebe sich lediglich, dass eine Geheimzahl am Abhebeterminaleingabe wurde, aber nicht, welche Geheimzahl es war.

Ihr direkter Draht ...



**02602/9191-640**

Fax: 02602/9191-646

e-mail: [kmi@kmi-verlag.de](mailto:kmi@kmi-verlag.de)

... für den vertraulichen Kontakt

### Impressum

**kapital-markt intern** Verlag GmbH, Bahnallee 3, (Am ICE-Terminal), D-56410 Montabaur, Tel.: +49 (0)2602 9191 640, Fax: +49 (0)2602 9191 646. [www.kmi-verlag.de](http://www.kmi-verlag.de). Geschäftsführer: Dipl.-Kfm. Uwe Kremer, Rechtsanwalt Gerrit Weber, Dipl.-Ing. Günter Weber. Gerichtsstands Montabaur. Handelsregister HRB 28667. Vervielfältigung nur mit Genehmigung des Verlages.

**kapital-markt intern** Herausgeber: Dipl.-Ing. Günter Weber. Chefredakteur: Redaktionsdirektor Dipl.-Kfm. Uwe Kremer, Redaktionsdirektor Rechtsanwalt Gerrit Weber. Redaktionsbeirat: Dipl.-Ing. Dipl.-Oen. Erwin Hausen, Christian Prüßing M.A., Druck: Theodor Gruda, [www.gruda.de](http://www.gruda.de).

ISSN 0173-3516

Die Bank sei damit die Mindestanforderungen der Beweisführung gem. § 675 w S. 2 BGB a. F. beweisfällig geblieben, da für das Gericht nicht erkennbar sei, ob und mit Hilfe welchen Verfahrens sie die personalisierten Sicherheitsmerkmale des Zahlungsinstruments geprüft habe und zu welchem Ergebnis diese Prüfung geführt habe.

Die verschlüsselte Aufbewahrung der PIN des Klägers in dessen Portemonnaie gemeinsam mit der Zahlungskarte wertete das Gericht nicht als grobe oder einfache Fahrlässigkeit des Klägers. Als grob fahrlässig ist es in der Regel, wenn der Bankkunde seine persönliche Geheimzahl gemeinsam mit der Karte und nicht räumlich von dieser getrennt mit sich führt.

Nach diesen Maßstäben sah das Gericht die verschlüsselte Vorhaltung der PIN durch den Kläger als hinreichend sicher an, dies verstoße noch nicht einmal gegen einfache Sorgfaltspflichten. Nach Ansicht des Gerichts habe der Kläger, den das Gericht persönlich angehört hatte, eine komplexe, individuelle Verschlüsselungsmethode entwickelt, die – jedenfalls wenn man die Methode nicht kennt – auch dem Gericht als ausreichend sicher erschien. Der Kläger hatte die Zahlenfolge zudem zusammenhanglos auf einem Zettel mit Telefonnummern notiert ohne zugehörigen Hinweis, dass es sich um eine PIN handelt. Das Gericht konnte sich nicht vorstellen, dass es den Tätern innerhalb von nur wenigen Minuten gelungen sein soll, die PIN aus der notierten Primzahlzerlegung zu entschlüsseln.

Das Amtsgericht München hat an diesem Fall anschaulich gezeigt, dass es nicht Aufgabe des Bankkunden sein kann, zu beweisen, wie es dem Täter im konkreten Fall gelungen ist, ohne Kenntnis der PIN am Automaten Geld abzuheben. Vielmehr ist es Sache der Bank, erst einmal darzulegen und zu beweisen, dass tatsächlich die richtige PIN bei der Abhebung eingegeben wurde.

Dieses Urteil hat weit über den Einzelfall hinausgehende Bedeutung: Zum einen ist es gut zu wissen, dass man seine PIN hinreichend verschlüsselt aufbewahren darf. Wichtig ist dabei, dass es sich um eine hinreichend sichere Verschlüsselungsmethode handeln muss und die PIN als solche nicht notiert wird. Zum anderen verweigern Banken in solchen EC-Karten-Missbrauchsfällen häufig die Erstattung des abgebuchten Betrages mit dem Vorwurf, der Bankkunde habe sich grob fahrlässig verhalten.

Auch bei Online-Banking-Betrug (phishing) verweigern Banken oftmals die Erstattung und werfen den Kunden grobe Fahrlässigkeit vor. Doch auch hier sind die Banken für Datenlecks und ausreichende Sicherheit verantwortlich, und nicht die Kunden. Der Verfasserin sind Online-Banking-Missbrauchsfälle bekannt, in denen nach einer phishing-Attacke sogar Schäden von über 150.000 € entstanden sind. Die Kundin hatte lediglich ihre neue Kreditkarte auf der Online-Plattform registriert, die im Übersendungsschreiben ihrer Hausbank, mit dem sie ihre neue Kreditkarten erhielt, genannt war. Dort hatten sich die Täter offenbar eingehackt.

Durch dieses Urteil werden den Banken nun aber zu Recht die Grenzen aufgezeigt. Ein Bankkunde darf der von den Banken zur Personaleinsparung eingesetzten Technik nicht schutzlos ausgeliefert sein. Sicherheitslücken hat die Bank zu verantworten, nicht der Kunde. Und es bleibt die Erkenntnis, dass die Täter Geld mit der gestohlenen EC-Karte abheben konnten, obwohl sie die PIN gar nicht kannten. Und dies ist kein Einzelfall.

Die Banken behaupten zwar, dass die Chipkartentechnik sicher und eine Geldabhebung ohne Eingabe der richtigen PIN gar nicht möglich sei. Auch könne die PIN nicht aus dem Chip auf der Karte ausgelesen werden. Die zahlreichen Betrugsfälle in der Praxis mit Geldabhebung nach Kartendiebstahl beweisen aber das glatte Gegenteil. Bei bloßem Besitz der Original-Karte ist es den Tätern möglich, das Konto (bis zum Tageslimit) abzuräumen. Ob dies durch ein technisches Auslesen der PIN oder durch geschicktes Manipulieren des Abhebeterminals, z. B. das Aufspielen einer Malware, geschieht oder Datenlecks bestehen, und die individuellen Daten der Bankkunden im großen Stil aus dem Darknet erworben werden können, ist dabei unklar. Weil die Täter sich aber mit der bloßen Karte freien Zugang zum Konto verschaffen können, sollte man sein Tageslimit möglichst niedrig ansetzen, um im Betrugsfall den Schaden gering zu halten.

**Fazit:** Die seit einigen Jahren von Banken als angeblich sicher eingestufte Chipkartentechnik ist nicht sicher! Wer Opfer von EC-Kartenmissbrauch nach Kartendiebstahl oder von Online-Banking-Betrug geworden ist, sollte sich gegen den Vorwurf der Bank, man habe sich grob fahrlässig verhalten, unbedingt zur Wehr setzen und seine Ansprüche notfalls mit anwaltlicher Hilfe weiterverfolgen.

Namentlich gekennzeichnete Beiträge geben nicht in jedem Fall die Meinung der Redaktion wieder.

In Europas größter Informationsdienst-Verlagsgruppe...

steuerberater intern  
immobilien intern  
umsatzsteuer intern  
Ihr Steuerberater  
steuer-tip GmbH intern  
EXCLUSIV (Schweiz)



...erscheinen die wöchentlichen Branchenbriefe:

Bank intern  
kapital-markt intern  
finanz-tip  
versicherungstip  
investment intern  
inside track (USA)