Haftungsfall Skimming

Die Zahlen sprechen für sich: Die vom Bundeskriminalamt für 2009 herausgegebene polizeiliche Kriminalstatistik verzeichnet beim Betrug mittels rechtswidrig erlangter Daten von Zahlungskarten 17 072 Fälle und damit einen Zuwachs um 68,6 Prozent gegenüber 10 124 Fällen im Jahr 2008. Das Ausspähen von EC-Kartendaten an Geldautomaten – das so genannte Skimming – scheint ein Kinderspiel zu sein; die dadurch angerichteten Schäden sind immens. Für die betroffenen Banken und ihre Kunden stellt sich die Haftungsfrage. Die NJW hat *Prof. Dr. Thomas Hoeren* von der Universität Münster hierzu befragt.

NJW: Was versteht man unter Skimming und wie gehen die Täter typischerweise vor?

Hoeren: Der Begriff „Skimming" stammt vom englischen „to skim" ab, was üblicherweise mit „abschöpfen" übersetzt wird. Dies bezeichnet eine Methode zum Auslesen von Kredit- oder EC-Kartendaten an Geldautomaten oder Bezahlterminals. Karten- bzw. Kontonummer sind für gewöhnlich auf den jeweiligen Magnetstreifen gespeichert. Um diese Daten zu bekommen, bringen die Täter meist ein unauffälliges Lesegerät über dem Kartenschlitz an. Die PIN wird typischerweise durch weitere technische Hilfsmittel ausgespäht, zum Beispiel mit Hilfe einer Kamera oder – seltener – eines aufgesetzten Tastenfelds. Mit den erlangten Daten stellen die Täter dann Kartenfälschungen her, so genannte Dubletten, und heben normalerweise im Ausland große Summen ab.

NJW: Durch Skimming können dem Karteninhaber beachtliche finanzielle Verluste entstehen. Wer haftet dafür?

Hoeren: Grundsätzlich haftet natürlich zunächst einmal der Täter selbst, sollte man seiner habhaft werden können. Im Verhältnis der Bank zum Kunden ist allerdings die Bank nach § 675 u BGB verpflichtet, bei nicht autorisierten Zahlungsvorgängen dem Karteninhaber den vollen Betrag zu erstatten. Nur in Ausnahmefällen muss der Karteninhaber haften.

NJW: Bis zum 31. 10. 2009 galt § 676 h BGB, der das Risiko des Missbrauchs von Zahlungskarten der die Karte ausgebenden Bank zugewiesen hat. Wegen § 675 u BGB ist es aus Sicht des Bankkunden also nicht bedauerlich, dass diese Vorschrift nicht mehr gilt?

Hoeren: Nein. Trotz Gesetzesänderung hat sich an dieser Haftungsfrage nichts geändert. Nach dem neuen § 675 u BGB ist die Bank verpflichtet, dem Kunden den Betrag unverzüglich zu erstatten. Die Entscheidung des Gesetzgebers, das Haftungsrisiko weitgehend den Banken aufzuerlegen, ist aus meiner Sicht übrigens sehr zu begrüßen.

NJW: Was muss ein Skimming-Opfer tun bzw. darlegen, um eine Korrektur von Kontobelastungen nach einer missbräuchlichen Verwendung der Daten seiner ec-Karte zu erreichen?

Hoeren: Das Opfer muss sofort handeln. Der Bankkunde ist gem. § 676 l BGB verpflichtet, das Kreditinstitut unverzüglich zu unterrichten, nachdem er Kenntnis von dem nicht autorisierten Zahlungsvorgang erlangt hat. Tut er dies nicht, kann er auf dem gesamten Schaden sitzen bleiben. Behauptet die Bank, der Zahlungsvorgang sei ordnungsgemäß autorisiert worden, hat sie das gem. § 675 w BGB nachzuweisen. Das erleichtert dem Karteninhaber die Durchsetzung seiner Ansprüche.

NJW: Können Sie sich Fälle vorstellen, in denen sich die Bank auf ein Mitverschulden des betroffenen Kunden berufen kann?

Hoeren: Die betroffenen Kunden sind im Regelfall auf der sicheren Seite. Die Fälle, in denen ein Mitverschulden in Betracht kommt, sind sehr eng umgrenzt. Hat der Kunde seine Karte verloren, kann er bis zu einem Betrag von höchstens 150 Euro in Anspruch genommen werden. Wichtig ist, dass die Kunden ihre Geheimzahl sorgfältig vor fremden Zugriffen schützen. Ansonsten muss der Kunde möglicherweise nach § 675 v BGB in voller Höhe haften. Jedenfalls kann dem Kunden aus meiner Sicht kein Vorwurf daraus gemacht werden, dass er seine PIN bei der Eingabe nicht mit der anderen Hand abgedeckt hat.

NJW: Machen es die Banken den Skimmern nicht zu leicht? Die Zahlen aus der Kriminalstatistik scheinen ja insoweit eine eindeutige Sprache zu sprechen?

Hoeren: Ich denke nicht. Vielmehr verhält es sich beim Skimming so, dass sich Geschädigter und Schädiger regelrecht ein Wettrennen liefern. Zwar haben die Banken das Problem erkannt und versuchen sowohl durch Aufklärung als auch durch den Einsatz besonderer Antiskimming-Maßnahmen wie etwa dem Jittering (eine Technik, bei der der Karteneinzug ruckelnd erfolgt, was verhindern soll, dass ein Skimming-Modul die Daten auf dem Magnetstreifen der Karte ablesen kann) des Problems Herr zu werden. Die Täter entwickeln aber andersherum auch immer wieder (technisch) neue Wege, um an die entsprechenden Daten zu gelangen. So bringen sie das Skimming-Modul in einigen Fällen bereits am Kartenschloss an, mit dem die Banken ihre Automatenräume abriegeln.

NJW: Smartcards, bei denen die für die Nutzung von Geldautomaten erforderlichen Daten nicht auf einem Magnetstreifen, sondern auf einem Chip gespeichert sind, gelten hinsichtlich des Ausspähens von Daten gemeinhin als sicherer. Ist das so?

Hoeren: Prinzipiell schon. Denn es ist tatsächlich deutlich schwerer und aufwändiger, die auf einem solchen Chip gespeicherten Daten auszulesen. Trotzdem gibt es eine Sicherheitslücke, die die Täter sich zu Nutze machen: Die derzeit von den Banken ausgegebenen Karten verfügen nämlich weiterhin zusätzlich über einen Magnetstreifen, da sich die Smartcards vor allem im außereuropäischen Ausland noch nicht durchgesetzt haben und das bargeldlose Zahlen und Geldabheben unter Benutzung einer reinen Smartcard-Karte dort nicht möglich wäre. Durch diese Sicherheitslücke können die Täter aber hier in Deutschland den Magnetstreifen auslesen, eine Dublette der Karte anfertigen und in eben jenen Drittländern Abhebungen tätigen, an einem Automaten, der immer noch Magnetstreifen-Karten ohne Chip akzeptiert. Insofern lässt sich auch die Smartcard-Technologie umgehen, solange es keinen weltweit einheitlichen Sicherheitsstandard gibt.

NJW: Wie kann man sich effektiv vor Skimming schützen?

Hoeren: Die einfachste Art und Weise ist wohl, beim Eingeben der PIN den Vorgang mit der anderen Hand abzudecken. Denn wenn die Täter die PIN der Karte nicht erkennen können, ist die Dublette für sie wertlos. Sollten sie allerdings mit einem aufgesetzten Tastenfeld arbeiten, bringt auch diese Maßnahme nichts. ■