

# Keine Strafbarkeit durch Auswerten und Systematisieren der Videoaufzeichnungen der PIN-Eingaben sowie Erfassen der ausgelesenen Kartendaten der Kunden auf einem Datenträger wegen Fälschung von Zahlungskarten mit Garantiefunktion

**Gericht**

BGH

**Datum**

29.01.2014

**Aktenzeichen**

29.01.2014

**Branche/ Lebenslage**

Skimming, Fälschung von Zahlungskarten

**Akteure**

Täter, Staat

**Wer haftet?**

Keine Strafbarkeit wegen Versuchs der Fälschung von Zahlungskarten, allerdings Strafbarkeit wegen der Verabredung hierzu

**Haftungsart**

-

**Haftungsumfang**

-

**Haftungsbegründendes Verhalten**

Verabredung, die Fälschung von Zahlungskarten durch Videoaufnahmen der PIN-Eingabe durch Berechtigte beim Zahlungsvorgang zu unterstützen

**Technische Umstände**

Mittels abgegriffenen Magnetstreifendaten sowie Aufzeichnung der PIN-Eingabe lassen sich funktionierende Duplikate der Zahlungskarten erstellen

**Persönliche Umstände**

-

**Möglichkeiten der Haftungsvermeidung**

-

## Zitate, Zusammenfassende Würdigung, Strategien zur Haftungsvermeidung

Der BGH hatte die Frage zu klären, ob der Angeklagte durch Videoaufzeichnungen der PIN-Eingabe von Zahlungskartennutzern und deren teilweisen Auswertung bereits zur Begehung einer Fälschung von Zahlungskarten (§§ 152a, 152b [StGB](#)) angesetzt hatte (Versuchsstrafbarkeit).

Bei dieser als Skimming bezeichneten Tat werden durch (regelmäßig) Manipulation von Geldautomaten oder elektronischer Kassen von den Tätern beim Einsatz der Zahlkarten durch die Berechtigten die zugehörigen PINs (oft mittels Videoaufzeichnung der PIN-Eingabe) sowie die auf den Magnetstreifen der Karten gespeicherten Daten erfasst. Mittels PIN und Magnetstreifendaten lassen sich dann Kartendoubletten erstellen, die die unberechtigte Abhebung von Geldern ermöglichen.

Dem BGH nach wird zur Tat der Fälschung von Zahlungskarten, § 152a StGB und § 152b StGB, noch nicht angesetzt, wenn mittels Skimming Daten und Informationen erfasst und anschließend ausgewertet werden:

*Weder mit dem Verwenden der „Skimming-Gerätschaften“ an den Geldautomaten noch mit dem Auswerten der Videoaufzeichnungen, dem systematischen Erfassen der so ermittelten PINs oder dem Aufspielen der ausgelesenen Kartendaten auf einen Datenträger haben der Angeklagte oder der Mitangeklagte [...] unmittelbar zu der Begehung einer Tat gemäß § 152b Abs. 1, Abs. 2, Abs. 4 i.V.m. § 152a Abs. 1 Nr. 1 StGB angesetzt.*

## ANMERKUNGEN

Der BGH hatte sich mit der strafrechtlichen Beurteilung des sog. „Skimming“ zu befassen, ob mit der Auswertung der erlangten Kartendaten bereits zu einer Fälschung von Zahlungskarten (§§ 152a und 152b StGB) angesetzt wird.

Eine Strafbarkeit nach §§ 152a, 152b StGB, obgleich regelmäßig Ziel des Skimmings, wurde zwar abgelehnt, das Gericht bestätigte aber den Schuldspruch hinsichtlich der Verabredung zur Fälschung von Zahlungskarten, gem. §§ 152b Abs. 1, Abs. 2 und Abs. 4, § 152a Abs. 1 Nr. 1, § 30 Abs. 2 StGB.

Bereits in anderen Entscheidungen war der BGH davon ausgegangen, dass das Anbringen von Skimming-Gerätschaften an einem Geldautomaten noch kein unmittelbares Ansetzen zur Fälschung von Zahlungskarten ist (BGH, 11.08.2011, 2 StR 91/11, BGH, 14.10.2010, 5 StR 336/10, BGH, 15.03.2011, 3 StR 15/11). Die vorliegende Entscheidung sah ein unmittelbares Ansetzen auch noch nicht darin, dass die erhobenen Daten bereits ausgewertet wurden. In einer anderen Entscheidung eines Strafsenats des BGH war zumindest für den Fall, dass die erhobenen und ausgewerteten Daten bereits an diejenigen weitergeleitet wurden, die mit Hilfe der ausgewerteten Daten die Erstellung der Karten-Doubletten vornahmen, das unmittelbare Ansetzen bejaht worden (BGH, 27.01.2011, 4 StR 338/10). Auch die Hinweise des BGH in dieser Entscheidung lassen vermuten, dass eine Versuchsstrafbarkeit zumindest zum Zeitpunkt der Weitergabe der ausgewerteten Daten an weitere Tatbeteiligte besteht.