

Sicherheit

## Kartenmissbrauch: Sicherheitslücke Sepa

Das Thema Kartenmissbrauch ist bekanntlich eines, über das niemand gern spricht – die Emittenten schon gar nicht. Aus Sorge um die Wahrnehmung beim Kunden und negative Auswirkungen auf das Geschäft zählen Informationen über erlittene Betrugsschäden zu den bestgehüteten Geheimnissen im Kartengeschäft. Auch in einer First-Data-Studie zum Thema Kartenmissbrauch möchte ein Fünftel der Befragten die jährlichen Missbrauchsschäden nicht angeben (oder kennt sie nicht im Einzelnen). Genau dadurch aber, dass bekannt gewordene Fälle verschwiegen werden, wird die Möglichkeit der Betrugsbekämpfung eingeschränkt. Denn nur wenn auftretende Betrugsmodelle erkannt werden, können die Betrugsversuche schon im Ansatz entdeckt werden.

Eben hier liegt nämlich die Schwäche der Kartenkriminalität. Gerade weil dieser Tatbestand zunehmend professionell organisiert wird, gibt es Betrugsmuster, die von einem Teil der Welt in den anderen weitergegeben werden und kann die Finanzbranche mitunter antizipieren, welche Betrugsversuche demnächst zu erwarten sind, um daraufhin Präventivmaßnahmen zu ergreifen. Nur 31 Prozent der Befragten stimmten in der Studie der These zu, dass der Betrug völlig unvorher-

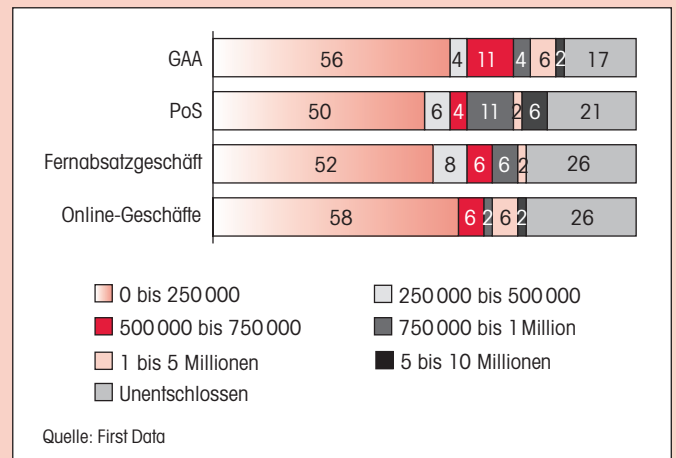
sehbar sei. Mit Lücken im Informationsfluss innerhalb der Branche spielt man insofern den Kriminellen in die Hände.

Die Emittenten befinden sich also in einer Zwickmühle: Einerseits sind sie sich bewusst, dass der Informationsaustausch mit anderen Banken und Ermittlungsbehörden zu den wichtigsten Aspekten im Zusammenhang mit der Aufdeckung von Kartenmissbrauch zählen (beinahe 46 beziehungsweise 44 Prozent der Befragten bezeichnen dies als sehr wichtig oder wichtig); andererseits scheuen sie sich davor, allzu viele Informationen über die eigenen Missbrauchserfahrungen preiszugeben.

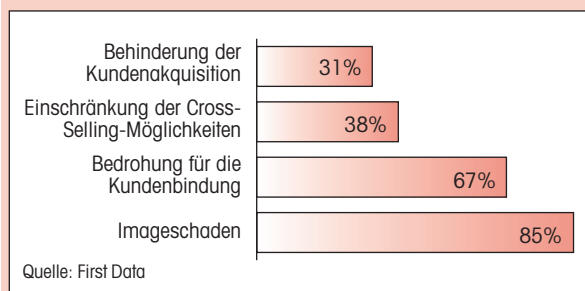
Stärker noch als auf die Zusammenarbeit innerhalb der Branche wird deshalb auf Technologie gesetzt. Das ist gewiss nicht verkehrt, denn auch die Täter arbeiten mittlerweile auf höchstem technischen Niveau. Die Zusammenarbeit mit anderen Banken kann das aber sicher nicht ersetzen – denn auch die besten technischen Systeme müssen schließlich zunächst einmal mit Informationen gefüttert werden. Der Chip allein wird das Ruder sicher nicht herumreißen, zumal die Risiken vor allem aus den Bereichen Fernabsatz und Internet kommen.

Den vielleicht noch nötigen Motivationschub zu einem verbesserten Informationsaustausch könnte Sepa liefern. Denn durch die Öffnung der nationalen Debitsysteme, die teilweise über hoch entwickelte Lösungen zur Missbrauchsprävention verfügen, wird auch das Debitgeschäft anfälliger für Attacken als bisher.

**Geschätzte jährliche Nettoverluste von Banken durch Kartenbetrug (in Euro)**



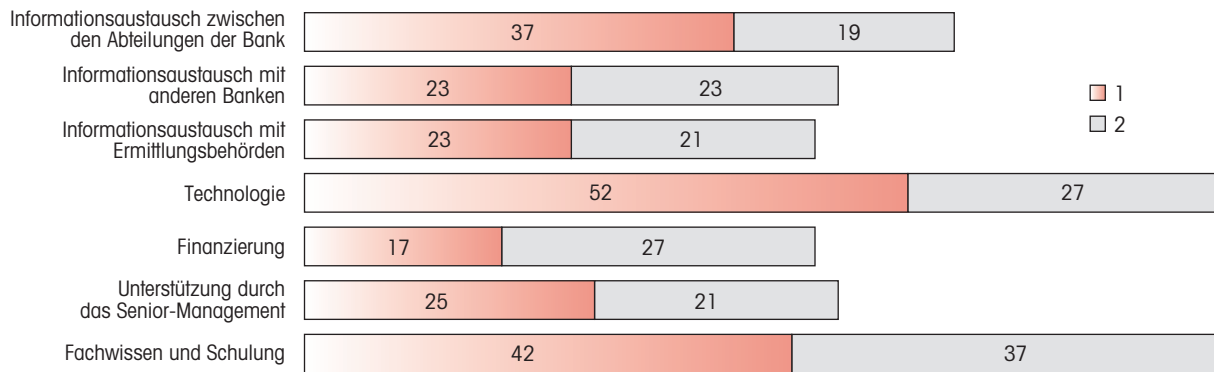
### Welches sind die schwerwiegendsten Betrugsauswirkungen für die Unternehmen?



Die EU Fraud Prevention Expert Group (FPEG) hat bereits im Dezember 2006 davor gewarnt, dass Betrüger die Fragmentierung der EU-Mitgliedsstaaten nutzen könnten.

Mit der Einführung Sepa-konformer Programme müssten deshalb auch paneuropäische Datenbanken aufgebaut werden. Davon kann aber bislang keine Rede sein – schon allein, weil die existierenden Datenschutzbestimmungen noch nicht an die Sepa-Welt angepasst wurden. Bald könnte sich der Datenschutz also womöglich gegen die Verbraucher kehren, die er eigentlich schützen sollte. Die professionellen Kartenbetrüger wird's freuen. **sb**

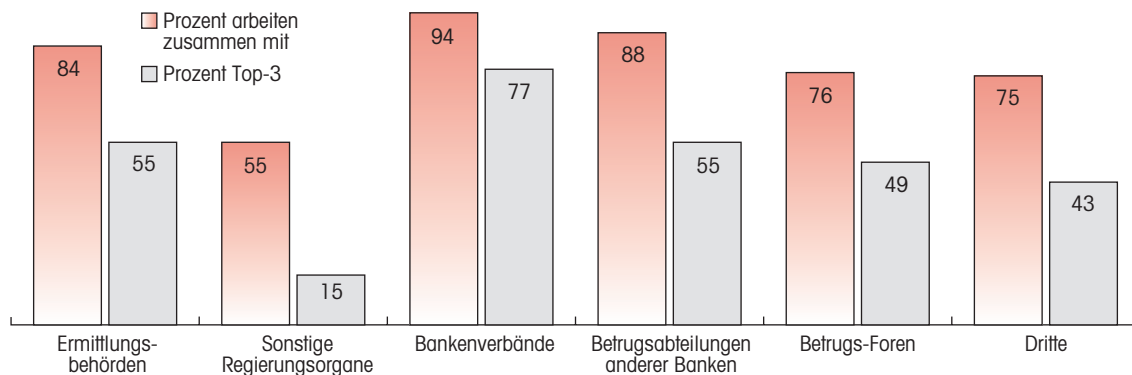
### Die wichtigsten Aspekte aus Bankensicht im Zusammenhang mit der Aufdeckung von Kartenmissbrauch



In Prozent der Befragten mit Bewertung 1 oder 2; bei einer Skala von 1 = sehr wichtig bis 10 = unwichtig

Quelle: First Data

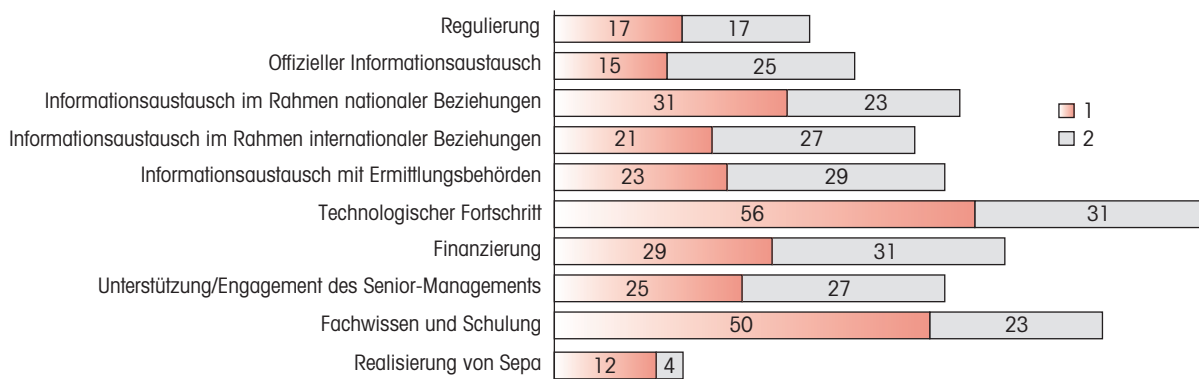
### Mit welchen Unternehmen/Gremien Banken im Kampf gegen Kartenbetrug zusammenarbeiten



In Prozent der Befragten

Quelle: First Data

### Wichtigkeit branchenweiter Maßnahmen in der Missbrauchsbekämpfung aus Bankensicht



In Prozent der Befragten mit Bewertung 1 oder 2; bei einer Skala von 1 = sehr wichtig bis 10 = unwichtig

Quelle: First Data