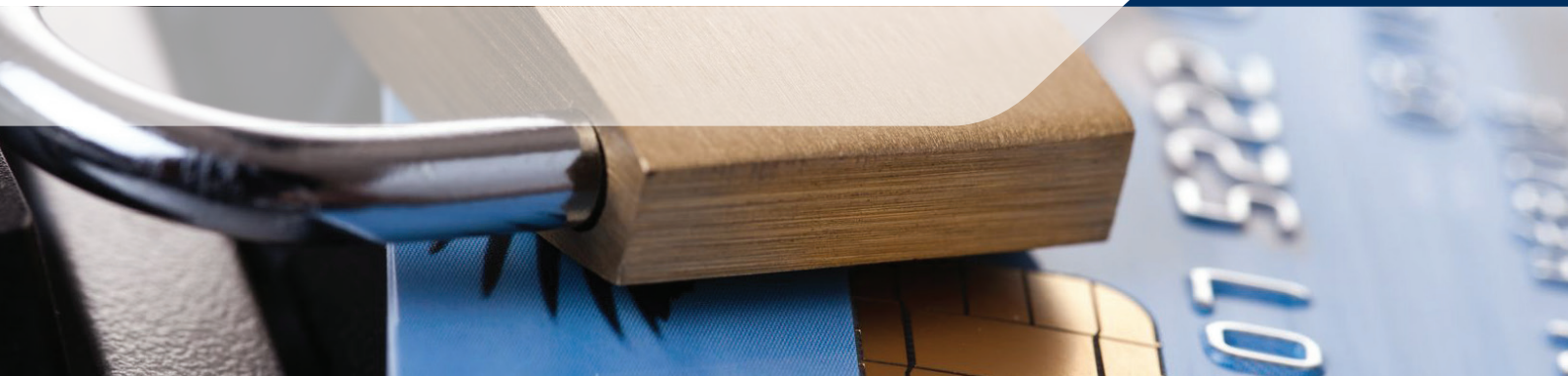


Geoblocking as an effective anti-fraud method

Success Story



As all aspects of life are becoming global and digitized, card fraud has become more popular than ever for organized criminals. Their attempts to defraud bear witness to the invention and technical know-how of the fraud rings. In Germany alone, the Federal Criminal Police Office estimated that the losses totalled EUR 35 million in 2011. This illustrates the challenging demands for prevention and countermeasures from specialists in the card industry.

Countering fraud with Fraud Control

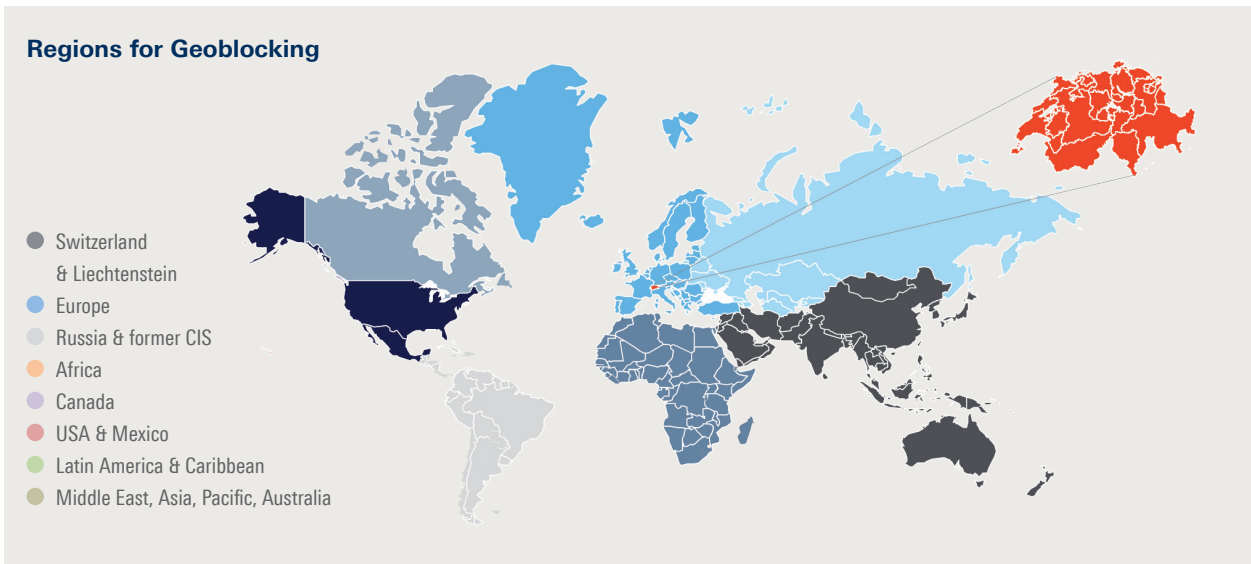
With Fraud Control, SIX Payment Services offers effective functions to combat misuse to issuers of Maestro cards in Switzerland and Liechtenstein. All authorization requests that correspond to pre-defined patterns suggesting the possibility of fraud are refused during the authorization process. Where cards used suspiciously had to be revoked for security reasons in the past, today the cardholder is usually left in peace. Thanks to sophisticated logic, Fraud Control identifies and prevents possible attempts to defraud and ensures that the legitimate owner can keep on using the card. Skimming is the form of fraud seen most frequently. Fraudsters manipulate ATMs to obtain the card data on the magnetic stripe, and also get hold of the PIN. This complete card data is passed outside Europe, from where the account is ultimately raided. Since the introduction of the EMV chip the illicitly duplicated cards have become almost worthless in Europe.

Caught in the tension between security and usability

While almost all card transactions in Europe are carried out using the copy-proof EMV chip, the magnetic stripe is indispensable for international use of the card. It is and remains the card's weak point. There will continue to be attempts at skimming so long as countries like the United States and Russia do not apply the chip technology and the magnetic stripe remains essential.

«Credit card fraud is everyone's business. Together, banks, retailers and cardholders can fight effectively against fraudulent card use. With Geoblocking, SIX Payment Services has made it possible to align regional card use with cardholders' personal requirements. This has helped us card issuers to significantly reduce the losses incurred by the use of skimmed cards abroad. At the same time, we're meeting our cardholders' demands for individual card protection.»

Otmar Wiederkehr
Head of Group Investigation Unit
Verwaltungs- und Privat-Bank
Aktiengesellschaft
Vaduz, Liechtenstein



Geoblocking – both simple and effective

In order to ensure global card usability, SIX Payment Services enriched its Fraud Control services for card issuers with Geoblocking, a highly effective system-based mechanism in the joint fight against card misuse. With Geoblocking, the bank can align the area where each individual card can be used with travel and usage habits at the request of the cardholder, and restrict usability individually on a geographical basis. For instance, a card can be blocked for relatively insecure regions such as North and South America, Asia or Africa. For e.g. a holiday trip, Geoblocking can be temporarily suspended in these regions. This significantly reduces the fraudsters’ options to use the datasets after a possible skimming attack.

Ease of use for the cardholder is essential for effectiveness. Geoblocking can be integrated as a function in e-banking. This enables customers to actively change settings for their cards without have to contact their bank. This control option is already available to 4.5 of 6 million cardholders in Switzerland and Liechtenstein.

The staged model in practice

The criteria for rejecting a transaction under Geoblocking are defined in several stages. In each case, a country/region list that is identical for all card issuers serves as the basis. The card management interface is used to control the functionality, meaning this takes place at the level of the individual physical card.

- At card level: the cardholder or the card issuer can define the regions where the card may be used for each Maestro card.
- At the client level: the card issuer can use a Fraud Control pattern to exclude individual countries in addition to regions.

Fraud Control patterns

Besides excluding countries, the card issuer can restrict use of its cards at client level in line with the following parameters:

Parameter	Description	Examples
Country	Geographical restriction by country	428 – Latvia 440 – Lithuania
Technology	Technology used to register the card data at the terminal (Point of Service Entry Mode)	EMV Magnetic stripe Magnetic stripe (EMV fallback)
MCC – Merchant Category Code	The MCC is a four-digit industry code developed by credit card organisations that serves to classify the merchant’s activities	7992 – Golf Courses, Public 7993 – Video Amusement Game Supplies 7994 – Video Game Arcades / Establishments

Your personal contact: www.six-payment-services.com/contact

SIX Payment Services Ltd
Hardturmstrasse 201
P.O. Box
CH-8021 Zurich

SIX Payment Services (Europe) S.A.
10, rue Gabriel Lippmann
5365 Munsbach
Luxemburg

SIX Payment Services (Austria) GmbH
Marxergasse 1B
1030 Wien
Austria

