**summary**

The evolution of card fraud has changed a lot during the period from 2008 to 2019. Overall, fraudulent transactions involving physical cards and fraudulent transactions conducted remotely are the main card fraud categories, and compromised application fraud and account takeover are the secondary card fraud categories. Cross-border transactions within SEPA account for the largest proportion of fraudulent transactions, followed by domestic fraud and cross-border fraud outside SEPA. Moreover, the countries with high percent card market like France and the UK have higher fraud rate, those countries with low percent like Romania and Poland have low fraud rate.

From 2008 to 2019, the overall absolute value of transactions is increasing, and the absolute value of fraud is also increasing, but the relative value of fraud is decreasing. This is because new technologies and laws have been added to prevent fraud. Among them, CNP fraud and card fraud at POS terminals increased significantly. Some technical and regulations have effects to card fraud, including increased adoption of chip and PIN transactions at ATMs outside of Europe, card tokenization, amended the Payment Services Directive and more comprehensive supervision.

The transaction landscape at the same period has changed a lot. The overall number of card transactions and the CNP payments related to online transactions are increasing, but the overall growth of card fraud is lower than the growth of normal card payments and has even stagnated in recent years. The cross-border transactions become more popular and the cross-border transactions within the SEPK framework have high fraud risk. At the beginning, counterfeit fraud was the main form of card fraud, but now it has dropped significantly and is more common in cross-border transactions.

The development of internet and e-commence provides convenience for credit card fraud in cross-border transactions.

To prevent card fraud, avoiding the data breach is a good solution. Because data breach will cause compromised application fraud and account takeover, which enables fraudsters to apply for credit cards and spend money in other people’s name and impersonating the real cardholder. Another solution is payment card tokenisation. It can serve as a payment credential. Compared to traditional primary account numbers, compromised tokens are less sensitive, less vulnerable to exploitation, and easier to replace. This makes them less attractive to fraudsters and helps reduce the risks and costs associated with credit card data breaches. I've found that adding electronic, encrypted security credentials can help reduce fraud.