Evolution of card fraud

The European Central Bank BCB splits card fraud into two main groups. **Card not present** **CNP** fraud typically involving remote payments through websites mobile applications mail or phone that uses student card details to commit fraud. **Card present** **CP** fraud which happens at the point-of-sale terminal or through an ATM and is dominated by lost and stolen cards. Since the rise of chip technology, counterfeit cards observed a sharp decline while the CNP grew tremendously, about 79% of fraud in 2018 was done using CNP and by 2019 it grew to 80%. Globally many member states of the European union saw more than 90% of their fraud occur in cross-border settings, since the domestic transactions made-up about 89% of total payment value included only around 35% of fraud value. Cross-border inside the **single euro payments area** **SEPA** was only close to 9% of value yet about 51% of fraud, and cross-border outside SEPA was 2% of value but 14% of fraud, so large numbers of domestic markets such as France, UK, Ireland, and Germany show us somewhat bigger domestic shares simply because so much spending stays at home.

As EMV rolled out widely counterfeit fraud and physical terminals collapsed so attackers moved to CNP channels and leaned more on cross-border transactions where checks are harder throughout the decade, everyday card usage grew faster than fraud losses so the fraud rate trended downward even when the euro amount of fraud didn't change much year to year. A few of the regulations and technologies have had a great impact on reducing card fraud that includes, EMV, second payment services directive and it's strong customer authentication rules. Also, improvements to 3D secure, extra authentication step for online card payments and broader use of tokenization further limited the reuse of stolen details. There has been a massive increase in card payments from 2016 to 2019 from 75 billion to 101 billion respectively. Remote online ending up CNP transactions became the most popular growth channel and unsurprisingly carried the highest fraud risk. As buying moved online fraud followed, countries with heavier online card use tended to show higher relative fraud rates especially where authentication and merchant security was lacking.

Mostly CNP fraud starts with compromised credentials and more specifically the primary account number the expiry date and the CVV of the card that are often stolen from breached merchants or through phishing attacks. Here, tokenization plays a really important role in replacing those statics number with single user merchant bound network tokens that are useless if copied elsewhere and very easy to rotate. With the help of combining tokenization with strong customer authentication and modern 3D secure it helps cut down online fraud while keeping the check-out relatively smooth

References

<https://www.ecb.europa.eu/pub/pdf/cardfraud/cardfraudreport201207en.pdf>  
<https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport202008~521edb602b.en.html>  
<https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport202110~cac4c418e8.en.html>