LEARNING NUGGET
#5

Card Fraud Made Difficult

Introduction and insights into card misuse and combating it successfully.

Debit cards are and remain very secure. The previous payment options (e.g. at the sale terminal in stores) have an extremely low fraud rate thanks to the latest technologies. With the use of cards in the area of e-commerce, the topic of fraud without a physical card is, however, gaining in importance on an ongoing basis. Most types of fraud target the biggest vulnerability: cardholders themselves.

Introduction

Card misuse – also referred to as fraud - is completed or attempted fraud committed by using a payment card such as a credit card or debit card. The fraudster's objective may be to obtain goods, services or cash. Fraud involving payment cards is as old as payment cards themselves. It happened initially only in the case of card-present transactions, which are also referred to as face-to-face transactions.

Since the option to use payment cards as a means of payment for online shopping has existed and more and more cardholders have been using this function, the focus of fraud with payment cards has also shifted to card-not-present and online transactions.

- **card present – around 6% of all fraudulent transactions:** The physical card is used (via a magnetic strip or chip) to make a payment on the spot, such as at an ATM, in a retail store, in a restaurant, or in a supermarket.

- **card not present (CNP) – around 94% of all fraudulent transactions:** When only the card data is used but the physical card itself is not presented. Examples: Manual entry of the data at a terminal in a store, on the phone, or on the Internet.

Thanks to modern, self-learning prevention systems and sophisticated rules, as well as the many years of experience accumulated by fraud analysts and technical experts, these types of fraud can be greatly reduced.

Increasing use of e-commerce has an impact on fraudulent behavior

In 2018, 10% of all transactions worldwide were conducted online, e-commerce expenditure will account for 17% of all global sales by 2022. (Source: Ravelin Insights)

Online transactions increased sharply again in 2020 due to lockdowns during the coronavirus pandemic and other factors. At the same time, changes in the fraud pattern were observed that were confirmed by internal analyses produced by the acquiring service provider Worldline and by SIX. While the number of fraudulent transactions is increasing overall, the average fraudulent amount per transaction has declined compared with previous years. Fraudsters adapt their processes to non-suspicious looking payment patterns of cardholders, which makes the fraud more difficult to identify. An example of this is the fraud attack adopted by the "hungry fraudster". This involves orders to a food delivery service for numerous but small amounts that are specifically spread over several days. It is possible that the card debits will not be noticed or noticed only later.

It is a constant race between the fraudsters on one side and the payment industry on the other. Fraudsters are constantly looking for new ways to defraud and issuers and acquirers are continuously required to adopt new protective measures and successfully thwart against attacks.

Fraudsters and their fraud attacks

The darknet is understood as an anonymous network that is a hidden part of the public Internet. Criminals – fraudsters – can interact anonymously with each other here. By doing so, they try to avoid being detected by the police. Fraudsters buy and sell card data on darknets and exchange information about how they commit a fraud and which tools should be used to do so. It is a growing form of organized crime with its own business model and efficient division of labor.

What elements facilitate this form of criminality?

Opportunity and low barriers to entry: the ability to download a suitable browser anonymously, to access relevant sites on the darknet and to purchase card data in crypto-currency is relatively straightforward.

Changed structures: The image of the refined hacker who uses extraordinary skills to take control of a server is outdated in part. Nowadays, card misuse is crimes that do not require any special skills or abilities other than just entering data on websites or in apps. It is striking that the entire sector is becoming more and more professional and offers actual service packages, which offer everything needed to carry out a hacker attack in addition to programmed malware.

Lack of stigmatization: An entire generation has grown up with online piracy, which is the free but illegal downloading of films, music, games and software. The step to illegal procurement is not always easy to see, and inhibitions around online fraud may have been reduced as a result.

Dealing carelessly with personal data, especially in social networks: Card fraudsters have a marked preference to obtain cardholders' personal data from social media. Examples are listed in the 'social engineering' type of fraud below. It is therefore all the more crucial that cardholders take basic security measures and exercise caution in dealing with and disclosing personal information.

Lack of cooperation: Card fraud is classified as an ex officio crime, which law enforcement agencies must officially prosecute. By notifying the police, their investigations and search for potential fraudsters will be supported. However, nowhere near all offenses are reported to the police. It is more difficult to provide evidence of an online offense than of a theft from a store. It is often difficult to identify perpetrators, especially if the person committing fraud or the person harmed is located in a different country from the online merchant. Cooperation between all the parties involved (cardholder, issuer, acquirer, card schemes, authorities) is therefore all the more important.

Overview of common approaches of perpetrators

The increasing shift in card misuse to the e-commerce sector can be seen below from the most frequently attempted frauds:

Social Engineering:

- **Phishing**: Method aimed at obtaining private information fraudulently. Usually the fraudster sends an e-mail message that appears to come from a respectable company such as a bank or card company. The sender asks for a confirmation of information and warns there will be serious consequences if this is not provided. The message may also contain a link to a fraudulent website does not appear suspicious. Other examples here include parcel notifications ("To be able to deliver your parcel…") and fake competitions ("You have won…").
- **Spear-phishing**: This method differs from other phishing attacks in that significantly individualized e-mail messages are sent to selected end users. To appear more convincing, the fraudsters carry out additional investigations into potential victims beforehand.
- **Vishing (voice-phishing):** Is the criminal intention of using social engineering by phone to obtain private, personal and financial information.
- **Smishing or SMS-phishing:** This method uses mobile phone SMS messages to convince victims to disclose personal or confidential data.

Data compromise (fake offers and malware):

- **Fake apps:** Apps for mobile devices, which induce users to download and install them. The apps look like original, attractive apps that offer interesting services. However, they can cause a lot of damage as soon as they are installed on a mobile device.
- **Fake Websites:** Customers are induced to disclose confidential information, download malware or buy products that never arrive.
- **Malware:** Software that is specially designed to disrupt a computer system, to harm it, or give access to it.

Additional well-known approaches

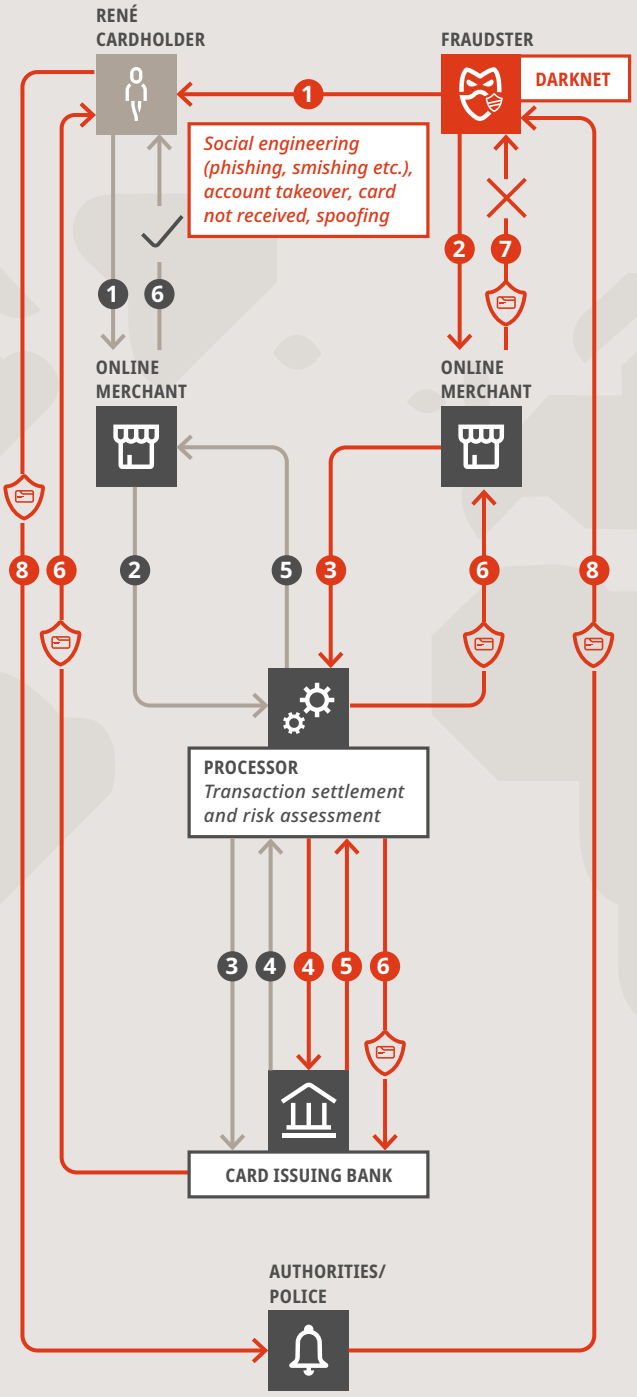
- **E-skimming:** In this case, the purchase procedure of online shops is infected with malware to uncover customers' payment and personal data during the payment process.
- **Attack on the card number:** The fraudsters use the first six to eight digits of a payment card and use software to calculate the remaining possible figures.
- **Account hijacking:** A form of identity theft when the criminals succeed in obtaining access to the log-in data for a user account.
- **Chargeback fraud or friendly fraud**: In this case, a cardholder claims that neither they nor anyone in their household made a purchase online for goods or services or that they did not receive them in order to receive a chargeback.
- **Smurfing:** In this case, the fraudsters carry out several small transactions over a longer period to remain undiscovered (also often used as an approach in money laundering).
- **Data theft:** Data is stolen from a system without the owner of the system knowing about this or having authorized it.
- **Spoofing:** In this approach, a communication process (such as e-mail messages, phone calls) is disguised in a technical way from an unknown source (sender, caller's telephone number) as if it was received from a known and trusted source.

How and how card fraud may arise?

If fraudsters have card data and possibly passwords or PINs, a fraud attempt could take place as follows (legitimate transaction/improper transaction):

Legitimate card transaction

1. René acquires a new mobile phone online.
2. The online merchant transmits the transaction request via his processor for review. The authorization request runs through the stored rules automatically.
3. The authorization request is passed to the card issuing bank.
4. Following successful verification by the bank, authorization is fed back to the processor.
5. The processor consolidates the feedback from the bank and the risk systems and reports to the merchant that the transaction has been authorized.
6. The purchase can then be settled successfully.



Improper card transaction

1. The fraudster succeeds in getting René's personal card data and his access data.
2. The fraudster orders goods improperly on the Internet.
3. The online merchant transmits the transaction request via his processor for review. The authorization request runs through the stored rules automatically.
4. The authorization request is passed to the card issuing bank.
5. Following successful verification by the bank, authorization is fed back to the processor.
6. The processor consolidates the feedback from the bank and the risk systems. The transaction is rejected preemptively because the review indicates that this is unusual purchasing behavior for this card profile. Depending on how the rules are defined, the card may also be blocked temporarily. A fraud alert is triggered in the monitoring tool, which is reviewed by analysts. The card issuing bank is informed of the transaction and contacts the cardholder to analyze the case further and to agree on any future action.
7. The online merchant rejects the purchase. The attempted fraud has been successfully prevented.
8. By notifying the police, cardholders support them with their investigations and search for potential criminals and fraudsters.

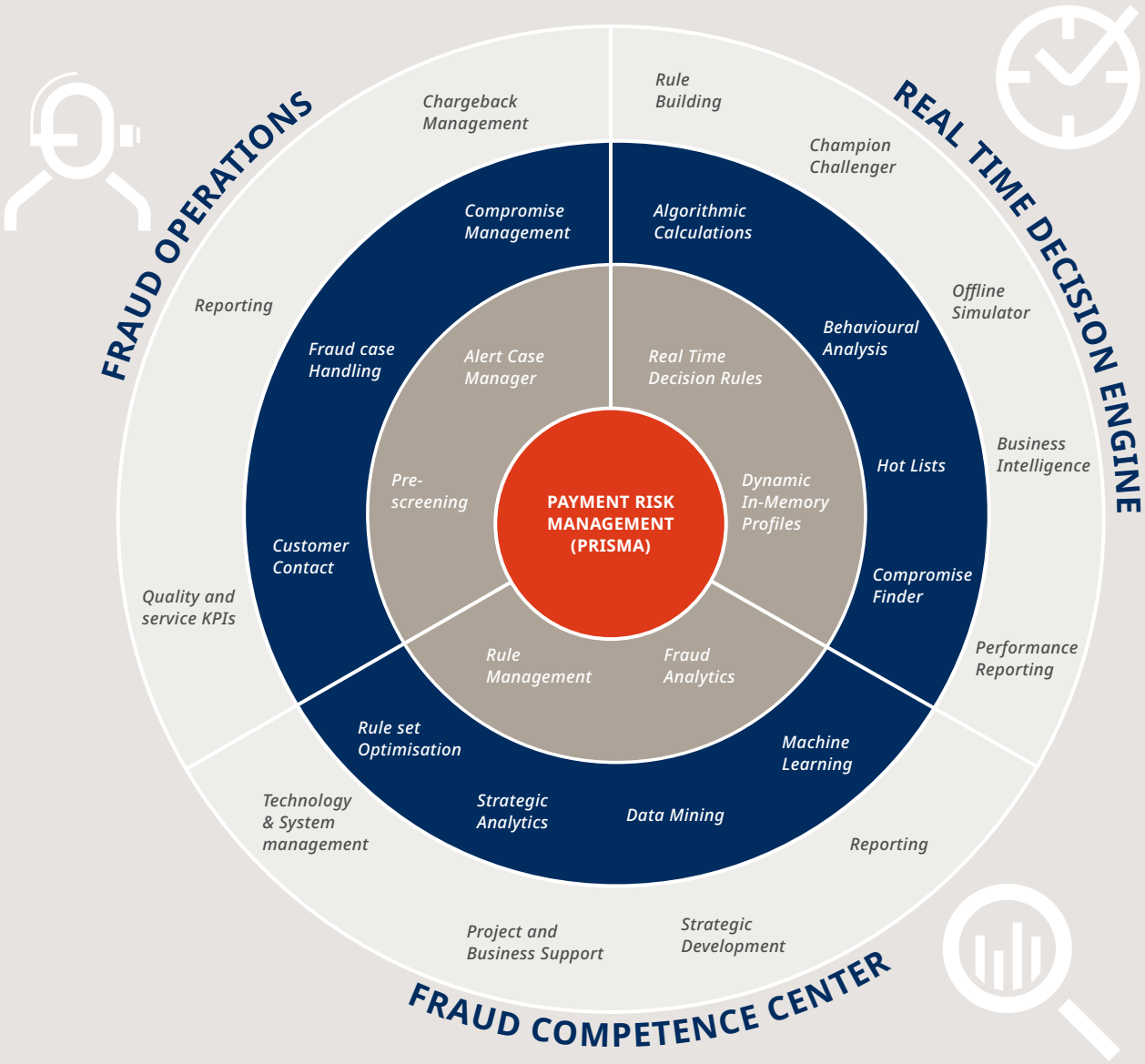
How can fraud be successfully combatted?

In combating fraud, payment providers rely on real-time systems, which react dynamically and quickly to new fraud patterns thanks to the use of self-learning technologies and active rule management.

Fraud experts (data scientists, rule administrators and fraud analysts) can fight new and changing fraud trends promptly and minimize them proactively. The effectiveness of the rules used is optimized continuously to recognize fraud so that the highest security requirements are guaranteed.

Together with the Fraud Operations teams, which act as the interface between the Fraud Competence Center, card issuers and card schemes, we ensure that cardholders are proactively contacted in the event of suspicious transactions or receive optimum support in the event of confirmed card misuse.

Illustration based on the PRISMA model (Payment Risk Management) operated by SIX



Selected measures to detect and prevent card fraud successfully

Cardholder	Processor/issuer	
	Technology used:	Human intelligence: experience of fraud experts
– Activate 3DS (see Learning Nugget 3D Secure) – Adjust geographical settings for the region in which the card is used (geo-blocking) – Set limits on the card, such as daily or monthly limits – Treating card numbers and passwords/PINs confidentially – When opening or answering e-mails or SMS messages (phishing, smishing), treat them with a healthy degree of skepticism. Check the sender carefully and hover the mouse over links before clicking on them – Make purchases from trustworthy websites only – Use strong, different passwords on different websites – Ensure software and devices are always up-to-date (i.e. always use current software versions for the operating system, applications and anti-virus programs, etc.) – Be careful with phone calls (if you are unsure, call back yourself directly on the official phone number)	**Use "state-of-the-art" software:** – Real time monitoring of all payment authorizations – Near-real time monitoring of all authorizations and clearing transactions – Profiling transaction histories – Automated card-blocking – Automated rejection of suspicious and/or improper transactions – Regularly update the rules in the fraud monitoring tool (if needed, change daily) in response to new modus operandi and analyses (e.g. unrecognized fraud) or indicators from fraud investigators. The rules may also have to be amended in response to new card schemes' requirements – White/gray/blacklist – Intensive exchange of information among the involved parties if there is an event (suspicion, card misuse, new MOs) – Use tokenization mechanism to encrypt card information (for more information, see Learning Nugget 'Tokenization for Debit Cards') – Incoming transactions are reviewed with the aid of artificial intelligence: taking account of all rules, known improper transactions, patterns of behavior and modus operandi. If there are any discrepancies, the system triggers an alarm immediately	**Fraud Analysts:** – Review all alerts generated in the system (alarm) – Recognize new patterns of fraud – Intensive knowledge sharing among fraud experts to keep up-to-date at all times – Analyze similar fraud cases to discover features in common, i.e. CPP (common point of purchase – where was the card compromised), to discover other cards that have been used improperly but not yet reported – Input adjustments to rules – Intensive dialog with issuers (card-issuing banks) – Support from authorities in connection with card misuse **Fraud Rule Administrators & Data Scientists:** – Analyze newly reported improper transactions – Analyze input from Fraud Analysts – Simulate and test new rules and adjustments to rules – Complex analyses taking account of all available data – Create statistics/reports – Create models relating to artificial intelligence

CONCLUSION: DEBIT CARDS ARE AND REMAIN SECURE

Debit cards are and remain very secure. The previous payment options (e.g. at the sale terminal in stores) have an extremely low fraud rate thanks to the latest technologies. With the use of cards in e-commerce, the topic of fraud without a physical card is gaining in importance.

In combating fraud, payment providers rely on real-time systems, which react dynamically and quickly to new fraud patterns thanks to the use of self-learning technologies and active rule management.

Close interaction between technology and human expertise is at the heart of combating card misuse successfully.

Thanks to solid networks among payment providers and coordinated action with authorities such as Europol and Interpol, we regularly succeed in stopping internationally active gangs from seizing marketplaces in the darknet and also in arresting criminals.

Prevention offers the best protection against fraud. SIX has been working very closely with the police for years. Together with card issuers, we operate the prevention platform card-security.ch, which informs cardholders and the public about the topic of card security via various channels and highlights how to protect themselves against misuse.

LEARN MORE

SIX BBS Ltd
Hardturmstrasse 201
P. O. Box
8021 Zurich
T +41 58 399 4012