ahum

by S S

Submission date: 26-Sep-2023 11:36AM (UTC-0700)
Submission ID: 2147482445
File name: Week_2_Part_3.docx (17.48K)
Word count: 1367
Character count: 7632

Introduction

As card payments are becoming popular daily and globally, we are shifting towards cashless payment systems. It is necessary to encounter the challenges this system faces, and one of the most important is card fraud. It is one of the most challenging things the modern payment system faces. According to the (ECB, 2020), the total value for all SEPA transactions was around 4.84 trillion, out of which 1.80 billion was fraudulent. Considering the challenge, the ECB governing board approved a framework to dig deep insight into these payments so that statistical information is collected.

In this essay, we will cover all the essential points related to the evolution of card fraud and the factors affecting it. We will cover all essential forms, geographic variances, and shits observed between 2008 and 2019. This report analyses the data provided by 23 card payment schemes, deeply observes all the trends and statistical data associated with these frauds, and evaluates each type of fraud and its impact on the overall financial system. Our investigation also covers the critical role of payment card tokenization in enhancing systems security. We have gained insights into the preventive measures we should take to safeguard the financial system from the ever-adaptive strategies of fraudsters.

Evolution of Card Fraud

The card fraud landscape has changed due to evolving technologies, consumer behaviour and changing regulations. As we look deep into these frauds, we get all the answers to these fundamental questions, which helps us to get a comprehensive knowledge of card frauds.

Types of Card Fraud

There are multiple types of card fraud that the financial systems are facing globally. A few significant contributors to this system are “card present fraud”, in which either cards are counterfeit or stolen and used for unauthorized transactions, and “card not present fraud”, in which online payments are made from card details acquired through data breaches.

Geographical Variations

There is an interesting pattern when it comes to the geographic variations. Within the Single Euro Payment Area (SEPA), a notable shift occurred between 2014 and 2018, with domestic card transactions remaining the dominant mode of payment at 89% of the total transactions. The popularity of cross-border card transactions also increased rapidly and contributed 12.11% of the total in 2018, indicating the growing purchase of the cross-border e-commerce market. This shift in the geography of purchases also impacted the fraud cases overall. Within SEPA, border transactions became the primary source of fraud, accounting for 49% of cases, with a considerable increase of 86.61% per cent in the last five years. There is a straightforward type of location-based pattern as counterfeit card fraud was majorly happening outside SEPA, while lost and stolen card cases were majorly domestic.

In 2018, within SEPA, cross-border transactions occurred as a significant source of fraudulent activities, constituting 49% of all card fraud cases. As it varies from country to country, France and the United Kingdom have the highest rates, while rates in Romania and Poland are the lowest.

Pattern in Fraud Landscape

There is an evident variation in fraud cases from 2008 to 2019. There was an initial increase from 2012 to 2015, followed by a reversal trend until 2017 and increases again in 2018. These variations are due to many factors, including the global financial crisis, technological advancements and changing consumer preference

Notable Increase in Fraud

There has been a noticeable increase in specific types of fraud during the last decade. This rapid growth clearly indicates how hackers and criminals are adapting to new technologies and exploiting emerging trends. The second primary reason is that people shift towards E-commerce shopping as it makes them more reachable to hackers. One of the most notable ones is card-not-present (CNP), which usually occurs when someone makes a fraudulent transaction using stolen card details.

Transaction Landscape and Technology Advancement

For the last five years, from 2014-18, card fraud at ATMs and POS terminals decreased rapidly by 52%, while card not received fraud decreased by 14.4%.In the same period, lost and stolen card fraud decreased by 4%, which shows that we have been able to minimize the percentage of a few types of fraud due to advanced technology. This reduction is due to the following reasons.

- EMV Chip Cards (as of 2015) By creating distinct transaction codes, the widespread use of EMV chip cards decreased card-present (CP) fraud, generating unique transaction codes.
- PCI DSS Updates Constant revisions to PCI DSS requirements required more stringent security safeguards while managing card data.
- From 2014 onwards, Tokenization technology replaced card data with tokens, improving security for card-not-present (CNP) transactions.
- Advanced Fraud Detection Systems backed by AI and machine learning have enhanced real-time fraud detection.
- Consumer education initiatives: initiatives to inform customers about safe practices and phishing awareness.
- Global Regulations Organizations must protect customer data by stricter cyber security and protection laws.

During this period, the following transactions became very popular.

- Mobile payments, such as Google Pay after its launch in 2015

- Recurring billing and subscription-based payments such as Netflix and Amazon payments.
- Contactless payments have become common, which you have to tap and go via card quickly.
- Small and Micropayments such as public transport fares.

Highly Risky Transaction

These transactions can cause huge losses, such as CNP transactions, recurring payments, international transactions and high-value purchases. After the introduction of EMV chips, many types of fraud were reduced, which led to an increase in CNP fraud. The landscape was also impacted by improved fraud detection, legal reforms, tokenization, and consumer awareness, and fraudsters adjusted their strategies appropriately.

Effect of E-commerce on Card Fraud

During this period, the shopping style underwent a significant change as people started to prefer online shopping rather than the traditional one, which led to more CNP transactions, making it easier for criminals to access sensitive information. That is why CNP fraud has been the foremost leading fraud in the last few years, making it easier for fraudsters to misuse them for financial transactions. High-profile data breaches, which lead to exposing details of card details and using them for financial gains, also had a significant impact on financial systems. However, adopting EMV chips and improved AI algorithms for fraud detection and real-time monitoring significantly improved the system's security. Advanced machine learning and AI algorithms also significantly impact the detection these fraudulent activities.

Data breaches in Card Fraud:

Protecting and preventing data is one the most essential things for financial safety nowadays. It is one of the most crucial things preventing card fraud as they are the primary source of stolen card information. When criminals access sensitive data through data breaches, they use it to gain financial benefits.

The reasons why preventing data breaches is one of the most critical aspects.

- Large quantities of credit card numbers, expiration dates, and cardholder identities are frequently stolen in data breaches. For scammers, this stolen information is a gold mine they can exploit to conduct unlawful transactions.
- Stolen card information from data breaches can be used to make fake physical cards, which helps with card fraud that occurs in person. Card cloning is reduced when breaches are avoided.
- Data leaks can damage trust in businesses and financial institutions. Customers are less reluctant to use their cards at businesses with a history of breaches, which affects sales and reputation.

Payment card tokenization is a practical model to prevent fraud and enhance card data security. The following are reasons why it is more effective.

- Tokenization substitutes a unique, randomly created token for the actual card data. This token is useless to fraudsters because it does not contain the critical data from the original card.

- Dynamic tokens, which alter with each transaction, are used in some tokenization systems. Given that the token is useless for subsequent transactions, this offers additional protection.
- T tokenization technologies prevent data breaches, frequently isolating sensitive card data in protected settings.
- Tokenization is adaptable to diverse payment ecosystems and may be utilized with various platforms and payment methods.

One of this system's most essential and interesting aspects is that in case of a data breach, the stolen cards are useless without the original cards' data, making this system more secure. It also encounters the privacy concerns of a customer, which leads to adding an extra security layer.

ahum

ORIGINALITY REPORT

3%	3%	0%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.ecb.europa.eu Internet Source	3%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		