DOI https://doi.org/10.32782/2663-5682/2022/37/05

M. O. Pyrkh
Postgraduate Student at the Department of International Economy, Natural Resources and Economics of International Tourism
Zaporizhzhya National University
Scientific supervisor: *O. V. Hamova*
Doctor of Economic Sciences, Professor,
Department of International Economy, Natural Resources and Economics of International Tourism
Zaporizhzhya National University
Zaporizhzhya, Ukraine

FRAUD PREVENTION TECHNIQUES FOR E-COMMERCE MERCHANTS, USING PAYMENT TRANSACTION RISK SCORES

Summary. *The purpose of this article is to go over various types of fraudulent actions that can be dangerous for merchants who sell their products and services online.The article describes efficient and common ways to avoid suspicious transactions, and identify fraudulent ones as well as ways to avoid certain most common fraud attempts.*

Key words: *fraud, SaaS, Risk management, fraud prevention, e-commerce, risk score, TC-40, SAFE, Payment Service Providers, friendly fraud.*

Context. Recent development of the technology has significantly reduced the distance in both geography and time between economic actors and increased efficiency of resource sharing. The share of e-commerce in total U.S. retail sales in the second quarter of 2022 was 14.5 percent, up from the previous quarter. Retail e-commerce sales in the United States reached nearly 258 billion US dollars from April to June 2022, the highest quarterly revenue in history. [1] The downside of economic growth is that we are seeing a significant increase in fraudulent activity. Furthermore, the increase in online sales and purchases as a result of the COVID-19 crisis opened up a new window of opportunity for fraudsters. The pandemic has had a negative impact on e-commerce fraud, according to a 2021 survey, with three-quarters of online merchants worldwide reporting a net increase in fraud attempts since the outbreak began. The industry suffered 20 billion US dollars in losses due to online payment fraud that year as a result of security breaches. As a result, the market for e-commerce fraud detection and prevention is expected to more than double between 2021 and 2025, reaching 70 billion US dollars. [2]

The term fraud is viewed by Cambridge dictionary as the crime of getting money by deceiving people, e.g. credit-card fraud. Anti-fraud professionals and researchers frequently rely on a concept known as the «fraud triangle» to predict the conditions that lead to a high risk of fraud. Steve Albrecht coined the term to model conditions that lead to a higher risk of fraud, based on criminological research by Edwin Sutherland and Donald R. Cressey.

The fraud triangle states that individuals are motivated to commit fraud when three elements come together:

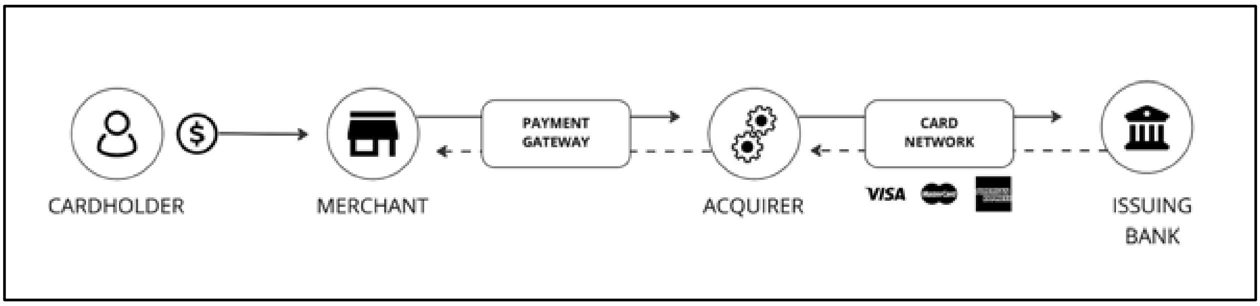
1. Opportunity, e.g., internal control system flaws.
2. Motivation, e.g., financial difficulty.
3. Rationalization, e.g., increased economic insecurity. [3]

However, in the case of the topic of this article, it makes more sense to review specific fraud type: e-commerce fraud. The term «e-commerce fraud» may seem obvious, but in reality, it covers the tactics used by fraudsters to target e-commerce sellers.

But before going into fraud, let's see how online payments work: how money goes from a client to the business and how banks support these payments.

Each online transaction involves multiple significant players:

1. **Cardholder:** the individual who makes use of a credit or debit card.
2. **Merchant:** the owner of a business that takes credit cards.



Graph 1. The key players in online payments

3. Acquirer: the financial institution that accepts card payments on behalf of the merchant and sends them to the issuing bank via the card networks. Acquirers may also collaborate with a third party to assist with payment processing.

4. Card Networks: Visa, Mastercard, and other card networks serve as the link between all of these players. They exchange transaction data, transfer transaction funds, and calculate the underlying costs of card transactions.

5. Issuing bank: the financial institution that offers banking or transaction service and, on behalf of the card networks, issues payment cards (such as credit, debit, or prepaid cards) to consumers or companies.

When the buyer does not approve the charge, the payment is **labeled fraudulent**. For example, if a fraudster makes a purchase on the merchant's website with a stolen card number that hasn't been reported, the payment may be successful. **The cardholder** would then file a chargeback with their bank if they discovered the unauthorized use of the card. While merchant can challenge the chargeback by providing evidence that the payment was legal, if it was a fraudulent transaction, the cardholder will win. If the merchant loses a dispute, they may be required to pay more than the original transaction amount. Fraud frequently results in **chargeback fees** (the cost of the bank reversing the card payment), higher network expenses due to disputes, higher operating costs due to examining charges or contesting disputes. [12]

Types of eCommerce Fraud.

The nature of e-commerce offers scammers many opportunities to target e-commerce suppliers and merchants. Let's review few most common types of e-commerce fraud.

1. Return fraud. Return fraud is the practice of bringing goods to a retailer that are not eligible for a return, thereby robbing the retailer. While some instances of return fraud turn out to be the result of a customer's honest error, the overall number of cases of return fraud involving malevolent intent is on the rise. [4]Because of the flood of returns merchants face after any major holiday in the US, this is a top priority for online retailers this. Unfortunately, 10.6% of those returns are fraudulent, a figure that is rising faster than e-commerce sales. [5]

2. Card Testing Fraud. Card testing fraud occurs when a fraudster obtains one or more credit card numbers illegally. Typically, fraudsters obtain these numbers by directly stealing them or purchasing them from specific parts of the internet. Small transactions are made to verify each card number's validity before larger purchases are made. This way, the fraudster may do it covertly and find out which cards are legitimate. Determining credit card limitations also involves smaller transactions. Fraudsters can begin making larger purchases after initial testing. By the time many merchants realize they've been a victim of card testing fraud, the fraudster has most likely made several large purchases.

3. Interception fraud. The fraudster uses a stolen credit card to purchase goods from your eCommerce website but avoids certain checks by providing legitimate, matching shipping and billing addresses. The goal after placing the order is to intercept the package before it reaches the address provided.

Fraudsters can use one of three methods to accomplish this:

- Contact the shipping company directly to reroute the package to a destination of their choosing.
- They can simply steal the package from the drop off location if they know the victim and live nearby.
- Contact merchant's company's customer service representative to change the shipping address before the item is ready to ship.

4. Chargeback Fraud. Chargeback fraud occurs when a customer purchases a product or service without first contacting their credit card company to cancel the transaction, resulting in a "chargeback." Chargeback fraud is a fascinating case because it can occur when a legitimate purchase is not recognized by the customer. This type of case is commonly referred to as **"friendly fraud."** However, friendly fraud is no less damaging to eCommerce merchants. It can still be detrimental to both the business and the customer relationship.

Fraudsters commit chargeback fraud to obtain free items with the knowledge that the purchase will be refunded to their credit card. Chargebacks lead to variety of losses: chargeback fees, lost items, shipping costs, penalties and administrative expenses, and bank penalties.

5. Phishing / Account takeover fraud (ATO)

Fraudsters can gain access to customer accounts through a variety of means. Purchasing stolen passwords and security codes, obtaining customer information from the internet, and implementing phishing schemes are just a few of the tactics available to a scammer. Once the account has been hijacked, fraudsters can do whatever they want, including:

- Changing Account Information
- Buying things
- Withdrawal of funds (if this functionality is present)
- Accessing the user's other accounts.

Account takeover is an Identity theft kind of fraud. Customers who have experienced account takeover fraud may never trust the provider again, and any customer relationship will be tarnished, if not destroyed. As a result, account takeover fraud is one of the most damaging types of eCommerce fraud. [5]Cybercriminals who commit account takeover get access to another person's internet account by using their login information. Cybercrime, including as account takeovers, has greatly expanded since the COVID-19 outbreak. [7]

Here's some statistical data about phishing: 23.6 percent of global phishing attempts targeted financial institutions in the first quarter of 2022. Furthermore, web-based software services and webmail accounted for 20.5 percent of all attacks, making these two industries the most targeted for phishing during the quarter under investigation. [10]

6. Refund fraud

Refund fraud occurs when a fraudster purchases a product or service with a stolen credit card and then has the purchase refunded to their credit card. One of the most common strategies is to inform the merchant that the refund must be processed on a new credit card because the old one has been closed.

Dealing with refund fraud is stressful for eCommerce merchants. It can be difficult to distinguish between legitimate and fraudulent claims, putting your relationship with your customers at risk. [5]

Fraud prevention techniques.

As we can see from various ways of fraud types protection against e-commerce fraud is critical for firms moving ahead. Here are several tactics and best practices for preventing e-commerce fraud.

1. E-commerce merchants should do regular, consistent site checks.

Conducting site checks might assist merchant in identifying security flaws before scammers can. Online retailers should go through the checklist below and take the following precautions:

– Maintain a valid SSL certificate and run malware scans on a regular basis.
– Backup your online store frequently.
– Create strong passwords for all password-protected accounts.
– Encrypt all communications between the store and its customers. [8]

2. PCI compliance is required for merchants who run an online store with credit card payments enabled.

PCI is an abbreviation for Payment Card Industry. The PCI Security Standards Council develops and manages PCI compliance standards to protect the security of credit card transactions in the payments sector. PCI compliance implies that an online store and business procedures adhere to the PCI requirements. This compliance is often provided by SaaS-based ecommerce shops, such as Shopify, Bigcommerce and others.

3. Merchants should monitor pament activity on their online shops.

To capture shoplifters, brick-and-mortar shops use fraud prevention personnel. Merchants can safeguard an online business from fraudulent purchases by keeping an eye out for unusual activities. It is also recommended checking payment accounts accounts and transactions for red flags such as contradictory billing and shipping information, as well as clients' actual location. Merchants need to track their client's IP addresses to get notified about any addresses from known fraudster hotspots. [9]

4. Card Verification Value Number must be activated for each website purchase.

Card Verification Value, or CVV for short, is a three-digit code found on the back of all Visa, MasterCard, and Discover credit cards. This code might be useful for retailers looking to crack down on fraudsters using stolen cards to purchase products or services. Because the code is on the back of the card, needing this number for all purchases implies that the user will need to have the physical card on hand.

5. Address Verification Services (AVS) should be used by merchants.

Many credit card providers provide an Address Verification Service to assist in comparing the address provided to the merchant with the bank's address on file. After the bank has completed this verification, an AVS code is provided to the merchant. These codes might indicate a variety of differences between the address given and the one on file. Merchants may better understand whether to accept, reject, or flag a transaction for suspected fraud by carefully studying these transactions and assessing the inconsistencies.

Naturally, internet fraud prevention has become more sophisticated. While rules engines formerly dominated the industry, machine learning now supplements most systems by adding speed and brilliance at recognizing patterns to a fraud system's efforts. This has allowed for more decisions to be automated and made more swiftly. Diverse providers of data enrichment for various types of data have emerged, although considering that a number of them have been purchased by larger firms in recent years, it will be fascinating to observe how this industry evolves. [10]

Comparison of Payment Gateways on risk scores, revealed to their clients.

Obviously it's hard for regular small and medium business owners to keep up with the technology and deep dive into machine learning. Therefore it's recommended to use payment service providers that have built-in services that provide a wide range of capabilities to track and manage fraud attempts, mark-false positive cases and monitor the payment activity on the website.

Let's review risk scores of several popular payment providers, available for usage in the United States, for online credit/debit card processing.

Risk score is a machine learning metric, that allows to rate the transaction and make appropriate steps to protect the business against fraud

№	Risk Score	Stripe [13]	Square[14]	Adyen [15], [16]
1	Billing address does not match cardholder address	Yes	Yes	Yes
2	Card/bank account holder name contains a non-alphabetic character	Yes	Yes	Yes
3	Liability shift status	Yes	Yes	Yes
4	Authorized transaction amount	Yes	Yes	Yes
5	Shopper IP	Yes	Yes	Yes
6	Shopper address	Yes	Yes	Yes
7	Early fraud notifications	Yes	N/A	Yes

1. **Billing address does not match cardholder address –** the Address Verification System (AVS) is a safety mechanism that checks the billing address supplied by the shopper to the cardholder address on file with the issuer.

2. **Card/bank account holder name contains a non-alphabetic character –** in the cardholder name box, fraudsters will occasionally enter strange characters. This rule is not activated by alphabetical characters in Roman, Hebrew, Cyrillic, or Chinese.

3. **Liability shift status –** when the obligation for chargebacks shifts from the merchant to the issuing bank, this is referred to as a liability shift. This occurs after the transaction has been validated by 3D Secure. The rule can be configured to activate exclusively for 3D Secure transactions or for all e-commerce credit card transactions.

4. **Authorized transaction amount** – fraudsters often are trying to purchase expensive items from e-commerce websites, in order to gain maximum value. This feature allows to indicate and to notify the merchant, when such an occasion happens, to avoid future issues.

5. **Shopper IP** – the billing address distance represents the risk associated with the distance between the billing address and the transaction's IP geolocation. A higher risk score for billing address distance implies that the transaction's IP geolocation is far from the billing address given by the client. If merchants see a higher billing address distance, they should investigate whether the client is using an anonymizer or another type of proxy that conceals their true location from IP geolocation. Merchants should also assess whether the consumer looks to be traveling, and whether it is usual for the merchant's company to have purchases made from areas that aren't very close to the billing address.

6. **Shopper Address –** a higher shipping address risk score might suggest that the provider has detected suspicious behavior linked with this shipping address throughout its machine learning network, or that the

address does not appear to be real for other reasons. If a retailer notices a higher delivery address risk score, they may want to investigate if the consumer misspelled their address or made an evident blunder. The merchant can also use a mapping program to verify the location, check the customer's order history, or determine if there is a history of fraudulent transactions with this address.

7. Early fraud notifications – card networks such as Visa TC40 and Mastercard SAFE (System to Avoid Fraud Effectively) have specific reports to inform payment providers of fraud activities. Providers are not obligated legally to pass this information to merchants, however it can give benefits for merchants to know about such events. Merchants suggested for the following actions:

– Actively evaluate such kind of notifications and offer refunds if needed (to avoid a chargeback).

– Cancel the order.

Adyen passes information about TC-40 and SAFE to their merchants, and call it notification of fraud. [16] Stripe does it as well, and calls this notification – early fraud warning. [17] Square does not expose publicly if TC-40 and SAFE protocols are used to notify their customers.

Pricing is the same for all 3 providers in the United States, and cost 2.9% + $0.3 per transaction. However for Square Risk Manager tool, merchant should pay additional $0.60 per transaction. [14]

Unfortunately, both brick-and-mortar retailers and e-commerce firms will face fraud in the future. People will always try to benefit from fraudulent transactions, whether they use stolen credit cards or any other form of illicit activities. This makes it more critical than ever to have best practices in place to combat fraudsters. Following listed above fraud prevention tactics, and use SaaS platforms that allow integration with payment providers with risk prevention tools, merchant can protect their businesses from fraudulent attempts and losses.

BIBLIOGRAPHY

1. Daniela Coppola, "Quarterly e-commerce share in total U.S. retail sales 2010-2022", Sep 16, 2022 URL: *https://www.statista.com/statistics/187439/share-of-e-commerce-sales-in-total-us-retail-sales-in-2010/#:~:text=Quarterly%20e%2Dcommerce%20share%20in%20total%20U.S.%20retail%20sales%202010%2D2022&text=In%20the%20second%20quarter%20of,up%20from%20the%20previous%20quarter. (дата звернення: 13.10.2022)*
2. Stephanie Chevalier, "E-commerce fraud – statistics & facts", Apr 1, 2022 URL: *https://www.statista.com/topics/9240/e-commerce-fraud/#dossierKeyfigures, (дата звернення: 13.10.2022)*
3. Albrecht, W. S., Romney, M. B., Cherrington, D. J. Payne, I. R., Roe, A. V. "How to Detect and Prevent Business Fraud", Prentice Hall, New Jersey, 1982.
4. Forter team, "What is return fraud", June 26, 2021URL: *https://www.forter.com/blog/what-is-return-fraud/, (дата звернення: 13.10.2022)*
5. Steve Kaufman, "Return fraud: How to manage retail's most miserable holiday tradition", Jan 27, 2022 URL: *https://www.signifyd.com/blog/return-fraud-bleak-holiday-task/, (дата звернення: 13.10.2022)*
6. Forter team, "5 Types of eCommerce Fraud You Need to Know About", June 26, 2021URL:*https://www.forter.com/blog/5-types-of-e-commerce-fraud-you-need-to-know-about/, (дата звернення: 13.10.2022)*
7. Security.org Team, "Account Takeover 2021 Annual Report: Prevalence, Awareness and Prevention", Feb 18, 2021URL: *https://www.security.org/digital-safety/account-takeover-annual-report/, (дата звернення: 13.10.2022)*
8. Forter team, "Ecommerce Fraud Prevention Strategies", Sep 21, 2021URL: *https://www.forter.com/blog/ecommerce-fraud-prevention-strategies/, (дата звернення: 13.10.2022)*
9. Rafael Lourenco, "Ecommerce Fraud Protection for Online Merchants: The Ultimate Guide", URL: *https://www.bigcommerce.com/blog/ecommerce-fraud/#six-types-of-ecommerce-fraud (дата звернення: 13.10.2022)*
10. Gilit Saporta, "Practical Fraud Prevention" 1st Edition, Kindle Edition, ISBN-13: 978-14920933292022, Pages 10-11
11. Gilit Saporta, "Practical Fraud Prevention" 1st Edition, Kindle Edition, ISBN-13: 978-14920933292022, Pages 10-11
12. "Managing fraudulent transactions", URL: *https://stripe.com/pt-br-us/guides/managing-fraudulent-transactions, (дата звернення: 13.10.2022)*
13. Adyen.com: "Standard Risk Rules", URL: *https://docs.adyen.com/risk-management/configure-manual-risk/standard-risk-rules,(дата звернення: 13.10.2022)*
14. squareapp.com: "Protect yourself from scams and fraud", URL: *https://squareup.com/help/us/en/article/6159-protect-yourself-from-scams-and-fraud, (дата звернення: 13.10.2022)*
15. Adyen.com: "Standard risk rules", URL: *https://docs.adyen.com/risk-management/configure-manual-risk/standard-risk-rules, (дата звернення: 13.10.2022)*
16. Adyen.com: "Dispute flow and process", URL: *https://docs.adyen.com/risk-management/understanding-disputes/dispute-process-and-flow, (дата звернення: 13.10.2022)*
17. Stripe.com: "Getting started with Stripe: fraud and disputes", Video file, *URL: https://support.stripe.com/questions/getting-started-with-stripe-fraud-and-disputes#:~:text=Early%20fraud%20warnings%20are%20notices,occurs%20before%20an%20official%20chargeback,(дата звернення: 13.10.2022)*

М. Пирх. Методи запобігання шахрайству для мерчантів онлайн комерції, з використанням показників ризику транзакцій. – Стаття.

Анотація. *У статті аналізується типи шахрайства в онлайн коммерції та методи їх запобігання шляом використання показників ризику, що надані платіжними провайдерами.*

Ключові слова: *шахрайство, SaaS, управління ризиками, запобігання шахрайству, електронна комерція, оцінка ризику, TC-40, SAFE, постачальники платіжних послуг, дружнє шахрайство.*

УДК 339.138
DOI https://doi.org/10.32782/2663-5682/2022/37/06

К. Г. Прокопенко
аспірант
Сумський національний аграрний університет
м. Суми, Україна

ПОСИЛЕННЯ БРЕНДУ АГРОКОМПАНІЙ ШЛЯХОМ ВИКОРИСТАННЯ ІНТЕРНЕТ-МАРКЕТИНГУ

Анотація. *Метою статті є аналіз сучасного стану управління інтернет-маркетингом серед аграних підприємств. У статті проаналізований рівень використання інтернет сторінок провідних агрокомпаній України, визначені ефективні приклади використання даного інструменту та проведено аналіз впливу використання інтернет-маркетингу на рівень фінансових показників. Зроблено висновки та поєднаний аналіз рентабельності підприємства у порівнянні з рівнем ефективного застосування інтернет-маркетингу. Визначено, що для успішного просування на зовнішніх ринках з метою підвищення обсягів експорту бажано викладати інформацію стосовно агропродукції шляхом побудови різних вебресурсів з присвоєнням українського та закордонного доменів.*

Ключові слова: *брендинг, інтернет-маркетинг, агропідприємства, маркетинг, рентабельність, прибутковість.*

Через складну соціально-політичну ситуацію, яка склалася в країні, агропідприємства зіткнулися з неймовірними економічними проблемами. Руйнування ринкових зав'язків та іноді відсутність можливості проводити налагоджену збутову політику вимагає від підприємств посилення сучасних методів впливу на ринок. З часів пандемії значний відсоток торговельних відносин перейшло до інтенер-простору, збільшилась довіра до онлайн-закупівель, що в свою чергу формує гарні умови для розвитку інтернет-маркетингу. Також, важливим буде зауважити, що підприємства які займаються посиленням свого бренду отримують безліч переваг, у порівнянні з підприємствами, які не займаються питанням бренду. Головними перевагами можна зазначити збільшення лояльності клієнтів та посилення довіри серед споживачів.

За даними журналу МінФін [4, ст 1] станом на 2020 рік понад 50% компаній не змогли оцінити свої ROMI. Під ROMI розуміють повернення від маркетингових вкладень. Іншими словами, кожна друга компанія не представляє, яка ціна клієнта, який прийшов з різних рекламних джерел. Це дуже важливий показник, адже саме він може відобразити чи можливо масштабувати діяльність підприємства. На сьогодні середній відсоток, що витрачається на маркетинг серед аграріїв коливається від 8% до 19%.

За даними засновника агенції «Ремаркетинг Україна» Юрія Островського статистика по аграрному секторі показує 450 тис. запитів на місяць, що на 29% більше, ніж у 2019 році. При цьому частка запитів, що надсилається з мобільних пристроїв, зросла до 38%. Середня вартість «кліка», тобто співвідношення затрат на банерну рекламу до кількості переходів через даний банер на сайт, становить 2 грн, а середня вартість контакту з клієнтом за контакт приймався перегляд користувачем сторінки «Контакти» на сайті приблизно 50 грн.

Комплексне використання інтернет-маркетингу повинно в першу чергу фокусувати увагу на просуванні інтернет сайту. Інтернет сторінки виконують одну із найважливіших функцій – розповсюдження інформації про компанію.

На сьогоднішній день донесення інформації до споживача займає пріоритетне місце серед ланок маркетингу.