ISSN Print 2786-5150
ISSN Online 2786-5169

UDC 343.53:[338.467:004.031.4]:658(73) DOI https://doi.org/10.26661/2414-0287-2023-1-57-13

AN OVERVIEW OF THE TYPES AND METHODS OF FRAUD PREVENTION FOR ONLINE SMALL AND MEDIUM-SIZED BUSINESSES

Pyrkh M.O.
Zaporizhzhia National University
Ukraine, 69600, Zaporozhzhia, Zhukovsky str., 66
michaelpyrkh@gmail.com
ORCID 0000-0002-3306-1200

Key words:
fraud prevention,
online commerce, recession,
payment cards,
payment transactions,
profit, costing,
small and medium businesses

This article aims to investigate fraud prevention practices for small and medium-sized businesses by e-commerce sellers in the United States. Small and medium-sized businesses are businesses that are often identified as having fewer than 500 employees, lower annual revenue than large businesses, and a less complex organizational structure. Small and medium-sized businesses play a vital role in the economy by creating jobs, driving innovation, and supporting local communities. Since the Internet provides a wide range of "contactless" business activities, the urgency of combating fraud in this area is very important. Currently, small and medium-sized businesses (SMBs) make up a huge segment of the U.S. economy – 44 % of GDP, about half of all employment, and half of the roughly $370 billion in total technology spending. Small and medium-sized businesses have been hit hard by the current economic difficulties and are now weighing every purchase more carefully. Recent research by consulting firm McKinsey found that 37 percent of small and medium-sized business owners cite inflation as their biggest concern – the highest percentage in 40 years. One in five expect growth to slow and talent a challenge amid the Great Attrition. Intense financial pressures during the economic crisis have led to an increase in fraud, according to a survey of fraud experts by the Association of Certified Fraud Examiners (ACFE). The ACFE report found a direct relationship between economic downturns and the increase in the intensity of fraudulent activity. Thus, based on the above, it can be concluded that the relevance of this research is very high. This article covers the following different types of scams, such as: Fraud with card testing; Account takeover fraud; Parcel interception fraud; Chargeback fraud; Refund fraud.

ОГЛЯД ТИПІВ ШАХРАЙСТВА, ЩО ЗАГРОЖУЮТЬ МАЛОМУ ТА СЕРЕДНЬОМУ БІЗНЕСУ В США, ЯКІ ПРОВАДЯТЬ ДІЯЛЬНІСТЬ ОНЛАЙН

Пирх М.О.
Запорізький національний університет
Україна, 69600, м. Запоріжжя, вул. Жуковського, 66

Ключові слова:
запобігання шахрайству,
онлайн-коммерція, рецесія,
платіжні картки,
платіжні транзакції, прибуток,
формування собівартості,
середні і малі підприємства

Ця стаття спрямована на дослідження методів запобігання шахрайству для малого та середнього бізнесу продавцями електронної комерції (e-Commerce) в Сполучених Штатах. До середнього та малого бізнесу відносять підприємства, які часто ідентифікуються менш ніж 500 співробітниками, нижчим річним доходом, ніж великі підприємства, і менш складною організаційною структурою. Малий і середній бізнес відіграє життєво важливу роль в економіці, оскільки створює робочі місця, стимулює інновації та підтримує місцеві громади. Оскільки мережа інтернет надає широкий спектр на провадження підприємницької діяльності «безконтактно», актуальність боротьби з шахрайством в цій сфері є дуже важливою. Наразі малий і середній бізнес (SMBs) становить величезний сегмент економіки США – 44 % ВВП, близько половини всієї зайнятості та половина з приблизно 370 мільярдів доларів загальних витрат на технології. Підприємства малого та середнього бізнесу сильно постраждали від нинішніх економічних труднощів і тепер ретельніше зважують кожну покупку. Недавні дослідження, проведені консалтинговою компанією «Мак Кінзі» показали, що 37 відсотків власників малого та середнього бізнесу називають інфляцію своєю найбільшою проблемою – це найвищий відсоток за останні 40 років. Кожен п'ятий

ISSN Print 2786-5150
ISSN Online 2786-5169

очікує, що зростання сповільниться, а талант є проблемою на тлі Великого виснаження. Інтенсивний фінансовий тиск під час економічної кризи призвів до зростання шахрайства, згідно з опитуванням експертів з шахрайства, проведеним Асоціацією сертифікованих експертів з шахрайства (ACFE). У звіті ACFE встановлено пряму залежність між економічними спадами та зростанням інтенсивності шахрайської діяльності. Таким чином, виходячи з вищенаведеного можна зробити висновок, що актуальність цього дослідження є дуже високою. В цій статті розглядаються такі різні типи шахрайства, такі як: шахрайство з тестуванням картки; шахрайство з захопленням облікового запису; шахрайство з перехопленням посилки; шахрайство з поверненням платежу; шахрайство з поверненням коштів.

Formulation of the problem

Let's take a look at why fraud prevention is so important to running a successful and profitable business.

The total cost of fraud to SMBs can vary significantly depending on the industry, size of the company and nature of the fraud. However, according to a 2020 study by the Association of Certified Fraud Investigators (ACFE), the average loss for small businesses with fewer than 100 employees was $150.000. This amount can be devastating for small businesses and even lead to bankruptcy in extreme cases. Additionally, the cost of fraud is not limited to actual monetary losses, but can also include legal fees, reputational damage, and the time and resources required to investigate fraud and take steps to prevent future occurrences [3].

In addition to ACFE, the results of the "True Cost of Fraud" study for e-commerce and retail are also available, and what they reveal should be of concern to these companies. This year's results show a significant increase in both the value and volume of fraud.

Figure 1 shows that every $1 of fraud now costs US retailers and e-commerce sellers $3.75, up 19.8 % from the pre-Covid 2019 study of $3.13. This also represents a 4.2 % increase from the 2021 survey, which was conducted during the pandemic [3].

Fig. 1 – Trends in anti-fraud cost growth per US dollar earned

As can be seen from the above, fraud prevention is vital for small and medium-sized businesses.

Analysis of recent research and publications

The interest of scientists is drawn to the study and systematization of online fraud prevention processes, several studies have been conducted by fraud experts conducted by the Association of Certified Fraud Examiners (ACFE). Research scientists emphasize the growing trend of online payment fraud [2]. Researchers of the Anti-Fraud Research Center, Institute of Criminal Justice Studies, and the University of Portsmouth scientists Mark Button, Chris Lewis, and Jack Tapley emphasize the growth of types and types of fraud, which are aimed at small and medium-sized enterprises operating online [6]. Researchers from one of the leading anti-fraud service providers, Sift, emphasize the importance of fraud prevention and its impact on the costs of enterprises, both direct and indirect [8], researchers from Stripe [9], PayPal [10], and "Braintree" [11], devote their research to increasing the effectiveness of fraud prevention.

Formulation of the goals of the article

The goal of the article is to investigate fraud prevention methods for small and medium-sized businesses and e-commerce sellers in the United States.

Presentation of the main research material

There are various fraud types that small and medium-sized businesses may encounter. They might deal with fraud committed by their own employees or fraud committed by so-called "dummy" companies on the outside [6].

The most frequent instances of fraud against small and medium-sized businesses which accept electronic payments and offer services or sell goods online will be covered in this article. Here are a few of the most typical methods con artists use to target online retailers and suppliers.

Card testing fraud. A fraudster illegally obtains one or more credit card numbers when participating in card testing fraud. Scammers typically get hold of these numbers by either directly stealing them or buying them from specific websites. In order to avoid drawing too much attention to themselves, card verification fraud starts with the smallest purchases. The fraudster will attempt to make smaller purchases using each card number in order to determine which ones are valid. The credit card limits for each card are also determined in part by smaller purchases. Following the initial testing, fraudsters might start making more significant purchases. Many merchants are the victim of card-testing fraud, and by the time they realize it, the fraudster has probably had time to make several large purchases.

Account takeover fraud. Fraudsters can access customer accounts using several different techniques. Fraudsters can use a variety of strategies, including buying

ISSN Print 2786-5150
ISSN Online 2786-5169

stolen passwords and security codes, gathering customer information online, and using phishing scams.

Fraudsters can change account information, make purchases, withdraw money (if that function is available), and access other user accounts once they have control of the account. Identity theft takes the form of account takeover fraud. Account takeover fraud victims may never again trust the provider, and any previous customer relationships will be damaged, if not destroyed. As a result, one of the most harmful types of e-commerce fraud is account takeover fraud.

Figure 2 shows the account capture scheme.

Parcel interception fraud. With parcel interception fraud, a fraudster uses a stolen credit card to make purchases from a victim's online store, but they get around some security measures by using real addresses for both shipping and billing. When placing an order, the objective is to stop the delivery before it gets to the requested address.

Fraudsters can accomplish this using one of three methods:

1. Stealing the package from the drop-off location if they know the victim and live nearby;
2. Contacting your company's customer service representative to change the shipping address before the product is ready to ship;
3. Contacting the shipping company independently to re-route the package to their preferred location.

Chargeback fraud. When a customer makes a purchase before getting in touch with the credit card company to cancel it, this practice is known as "chargeback fraud". Because it may result from a valid purchase that the customer is unaware of, chargeback fraud is an interesting case. This specific situation is frequently referred to as "friendly fraud". However, friendly fraud hurts e-commerce merchants just as much. Relationships with clients and customers may suffer as a result. Some con artists purposefully engage in chargeback fraud by abusing business policies to obtain items for free while knowing that the purchase will be reversed to their credit card.

Companies incur significant costs as a result of chargebacks, including

- Refund payments;
- Lost goods;
- Shipping costs;
- Fines, and administrative costs;

Refund fraud. In refund fraud, a fraudster buys a product or service using a stolen credit card and then makes a refund to their credit card. One of the most common tactics is to inform the merchant that the refund will need to be processed on a new credit card because the old one has been closed [7].

Measuring the impact of fraud on enterprise costs. Entrepreneurs must assess a wide range of factors in order to determine the overall cost of fraud to a business. The calculation of direct financial losses as a result of fraud is one method for estimating the effect of fraud on the cost of doing business. Chargeback fees lost revenue and the expense of detecting and stopping fraud are some examples of this. Businesses can evaluate the success of their fraud prevention efforts and modify their strategies by tracking the cost of fraud over time.

Customer Retention Rate: Fraud can lower customer retention rates by making customers doubt the company. Businesses can assess whether fraud prevention strategies

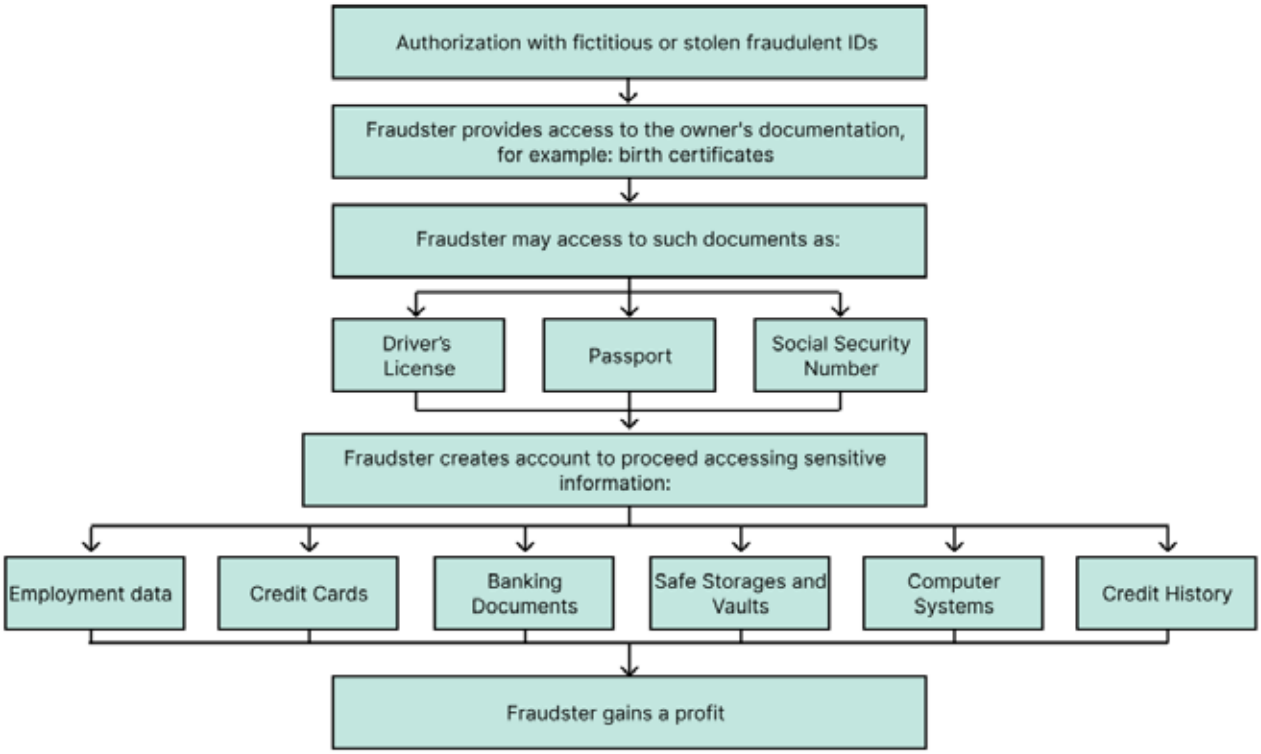

Fig. 2 – Account take-over scheme

ISSN Print 2786-5150
ISSN Online 2786-5169

are successful in preserving customer loyalty and trust by monitoring customer retention rates over time.

Employee Engagement: Employee involvement is frequently needed for fraud prevention initiatives, such as fraud awareness training and reporting suspicious activity. Businesses can evaluate the success of these steps in lowering the risk of fraud by measuring employee engagement and satisfaction. Fraud can harm a business's reputation and brand image, which can result in indirect costs like lost sales and decreased customer confidence. Businesses can assess the impact of fraud on their image and reputation and take action to mitigate any negative effects by tracking brand reputation and customer sentiment.

Businesses can identify potential fraud risks and ensure compliance with industry regulations by conducting routine audits. Companies can evaluate the success of their fraud prevention efforts and pinpoint areas for development by tracking audit results over time [8].

Analysis of services and payment systems to prevent online payment fraud. Here are some examples of companies that provide fraud prevention solutions that can integrate with small and medium-sized businesses (SMBs) and their pricing models.

Stripe offers many fraud prevention tools, including machine learning algorithms and analysis of buyer behavior. They have a calculated pricing model that charges 2.9% + $0.30 per successful transaction [9].

PayPal offers several fraud prevention tools, including fraudsters and chargeback protection. They have a billing pricing model that charges 2.9% + $0.30 per transaction [10]. Shopify: Shopify offers several fraud prevention tools, including machine learning algorithms and order risk analysis. They have a tiered pricing model with plans starting at $29/month and transaction fees ranging from 2.4% + $0.30 to 2.9% + $0.30 depending on the plan [11]. Braintree: Braintree offers a range of fraud prevention tools, including machine learning algorithms and behavioral analysis. They have a calculated pricing model that charges 2.9% + $0.30 per successful transaction [12]. It is important to note that the cost of fraud prevention solutions can vary significantly depending on the specific needs and requirements of the business. Additionally, some companies may offer pricing models based on transaction volume or other metrics. Before making a decision, SMBs are advised to evaluate several different fraud prevention companies and compare prices, features, and integration options.

Conclusion

The conducted research made it possible to reach the following conclusions. Fraud prevention is a critical issue for small and medium-sized merchants. The financial consequences of fraud can be significant, leading to increased costs and lost profits, as well as damage to a company's reputation. SMBs can use a variety of methods to prevent fraud, including self-education and staff training, fraud prevention software, advanced authentication procedures, and partnerships with third-party companies.

By implementing effective fraud prevention measures, small and medium-sized businesses can protect their business and customers from financial losses and maintain the trust of their customers. It is important for small and medium-sized businesses to constantly evaluate and update their fraud prevention strategies to stay ahead of new fraud methods and protect their business.

In addition, with the advancement of technology, small and medium-sized businesses can use the power of artificial intelligence and machine learning algorithms to prevent and predict fraud.

References

1. Winning the SMB tech market in a challenging economy (February 21, 2023). URL: https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/winning-the-smb-tech-market-in-a-challenging-economy (access date: March 19, 2023).
2. Impact of Recession on Fraud. URL: https://www.acfe.com/fraud-resources/impact-of-recession-on-fraud (access date: March 19, 2023).
3. The 2020 Report to the Nations – the ACFE's 11th study on the costs and effects of occupational fraud. URL: https://acfepublic.s3-us-west-2.amazonaws.com/2020-Report-to-the-Nations.pdf (access date: March 19, 2023).
4. Discover the True Cost of Fraud. URL: https://risk.lexisnexis.com/insights-resources/research/us-ca-true-cost-of-fraud-study (access date: March 19, 2023).
5. Measuring the Impact of Fraud. URL: https://sift.com/sift-edu/fraud-basics/impact-of-fraud (access date: March 19, 2023).
6. Fraud typologies and victims of fraud. National Fraud Authority, Literature review, Mark Button, Chris Lewis and Jacki Tapley Centre for Counter Fraud Studies, Institute of Criminal Justice Studies, University of Portsmouth. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/118469/fraud-typologies.pdf (access date: March 19, 2023).
7. 5 Types of eCommerce Fraud You Need to Know About, May 5, 2022, URL: https://www.forter.com/blog/5-types-of-e-commerce-fraud-you-need-to-know-about/ (access date: March 19, 2023).
8. Measuring the Impact of Fraud, URL: https://sift.com/sift-edu/fraud-basics/impact-of-fraud (access date: March 19, 2023).
9. Stripe: Financial infrastructure for the internet, URL: https://stripe.com/en-gb-us (access date: March 19, 2023).
10. Payments made easy with PayPal. URL: https://www.paypal.com/us/business (access date: March 19, 2023).
11. Shopify: Fraud analysis, URL: https://help.shopify.com/en/manual/orders/fraud-analysis (access date: March 19, 2023).
12. Braintree: Game-changing fraud protection, URL: https://www.braintreepayments.com/features/fraud-tools (access date: March 19, 2023).