KSE | Business Education

FraudBusters AI

AI-Powered Fraud Prevention SaaS Platform for Commercial Banks

Capstone Project

K.Vavrysh, K.Holynska | MBAI-MBA21 | April 26th, 2020

CONTENTS

DISCLAIMER

This presentation has been prepared by Khrystyna Vavrysh and Khrystyna Holynska for the FraudBusters AI (the “Company”) solely for the use as a visual support to discussions and is the responsibility of the Company for Capstone purposes at KSE (MBAI20). Neither the Company nor its directors, officers, employees, advisors and agents shall have any liability whatsoever in negligence or otherwise for any loss howsoever arising from any information or opinions presented or contained in this presentation nor shall they accept any responsibility whatsoever for, or make any representation or warranty, express or implied, as to the truth, fullness, accuracy or completeness of the information in this presentation (or whether any information has been omitted from the presentation) or any other information relating to the Company, its subsidiaries or associated companies, in any form whatsoever, howsoever transmitted or made available or for any loss howsoever arising from any use of this presentation or its contents or otherwise arising in connection therewith. The information and opinions presented or contained in this presentation speak as of the date hereof and are subject to change without notice. Neither the Company nor its affiliates nor advisers are under an obligation to correct, update or keep current the information contained in this presentation or to publicly announce the result of any revision to the statements made herein except where they would be required to do so under applicable law.

By attending the meeting where the presentation is made, or by reading the presentation slides, you agree to the following limitations and notifications and represent that you are a person who is permitted under applicable law and regulation to receive information of the kind contained in this presentation. This presentation is not intended specifically for potential investors and does not constitute or form part of and should not be construed as, an offer to sell or issue, or invitation to purchase or subscribe for or the solicitation of an offer to buy, acquire or subscribe for, any securities of the Company or any of its subsidiaries, joint ventures or affiliates in any jurisdiction or an inducement to enter into investment activity. No part of this presentation, nor the fact of its distribution, should form the basis of, or be relied on in connection with, any contract or commitment or investment decision whatsoever.

Certain statements, beliefs and opinions in this presentation are forward looking, which reflect the Company’s or, as appropriate, the Company’s officials’ current expectations and projections about future events. By their nature, forward-looking statements involve risks, uncertainties and assumptions, many of which are beyond the Company’s control, that could cause actual results or events to differ materially from those expressed or implied by the forward-looking statements in this presentation or discussed at this presentation. These forward-looking statements are subject to risks, uncertainties and assumptions which could adversely affect the outcome and financial effects of the plans and events described herein. You should not take any forward-looking statements contained in this presentation regarding past trends or activities as a representation that such trends or activities will continue in the future. No statement in this publication is intended to be a profit forecast. You should not place reliance on forward-looking statements, which speak only as of the date of this presentation. The Company expressly disclaims any obligation or undertaking to release any update of, or revisions to, any forward-looking statements, whether as a result of new information, future events or otherwise.

To the extent available, the industry, market and competitive position data contained in this presentation come from official or third party sources and that there is no guarantee of the accuracy or completeness of such data. The Company has not independently verified the data contained therein. In addition, certain of the industry, market and competitive position data contained in this presentation come from the Company’s own internal research and estimates based on the knowledge and experience of the Company’s management in the markets in which the Company operates. While the Company believes, acting in good faith, that such research and estimates are reasonable and reliable, they, and their underlying methodology and assumptions, have not been verified by any independent source for accuracy or completeness and are subject to change. Accordingly, you should not place reliance on any of the industry, market or competitive position data contained in this presentation.

Neither this presentation nor any part or copy thereof may be taken or transmitted into or distributed in or into, directly or indirectly, the United States of America (including its territories and possessions, any State of the United States and the District of Columbia). Any failure to comply with these restrictions may constitute a violation of U.S. state or federal law. The distribution of this presentation in other jurisdictions may be restricted by law, and persons into whose possession this presentation comes should inform themselves about, and observe, any such restrictions. This presentation is not directed to, or intended for distribution to or use by, any person or entity that is a citizen or resident in any jurisdiction where such distribution or use would be contrary to law or regulation or which would require any registration or licensing within such jurisdiction. Neither this presentation nor any copy thereof may be taken or transmitted into Australia, Canada or Japan.

This presentation is being supplied to you solely for your information and is not a prospectus and does not constitute or form part of, and should not be construed as, any offer for sale or subscription of, or solicitation of any offer to buy or subscribe for, any securities of the Company in the United Kingdom, the United States, Australia, Canada or Japan (or in any jurisdiction to whom or in which such offer or solicitation is unlawful), nor should it or any part of it form the basis of or be relied on in connection with, any contract or commitment whatsoever. Securities may not be offered or sold in the United States absent registration under the US Securities Act of 1933 or an exemption from, or in a transaction not subject to, the registration requirements thereunder. The Company does not intend to register or conduct a public offering of any securities in the United States.

This presentation is confidential and may not be reproduced, redistributed or passed on, directly or indirectly, to any other person or published, in whole or in part, for any purpose. This presentation is directed at the limited invitees who if, in the United Kingdom, must be (i) persons who have professional experience in matters relating to investments falling within Article 19(5) of the Financial Services and Markets Act 2000 (Financial Promotion) Order 2005 (the “Order”); or (ii) high net worth entities falling within Article 49(2)(a) to (d) of the Order or to those persons to whom it can otherwise lawfully be distributed (all such persons together in (i) and (ii) being referred to as “relevant persons”). This presentation must not be acted or relied upon by persons other than relevant persons and is to be kept confidential. By accepting this presentation the recipient confirms that he or she is a relevant person.

Any investment or investment activity to which this presentation relates is available only to (i) in the United Kingdom, relevant persons and, (ii) in any member state of the European Economic Area other than the United Kingdom, “qualified investors” within the meaning of Article 2(1)(e) of the Prospectus Directive (Directive 2003/71/EC), and will be engaged in only with such persons.

By attending this presentation you acknowledge that you will be solely responsible for your own assessment of the market and the market position of the Company and that you will conduct your own analysis and be solely responsible for forming your own view of the potential future performance of the Company’s business. You should not base any behaviour in relation to financial instruments related to the Company’s securities or any other securities and investments on information until after its made publicly available by the Company. Any dealing or encouraging others to deal on the basis of such information may amount to insider dealing under the Criminal Justice Act of 1993 and to market abuse under the Financial Services and Markets Act 2000. Neither the delivery of this presentation nor any further discussions of the Company with any of the recipients shall, under any circumstances, create any implication that there has been no change in the affairs of the Company since such date.

EXECUTIVE SUMMARY

Problem definition

According to the Global Economic Crime and Fraud Survey 2020 performed by PwC, fraud is a billion-dollar business, and is growing every year.[1] Banking industry is the most affected by the fraud and ready to spend a lot of money to protect their clients and their own image. Because of strict regulations, banks are required to monitor transactions closely and report any fraudulent ones. According to the Nilson report, card fraud will increase by about 5 USD bln per several years.[2] The NU Security by MasterCard provides a detailed analysis that shows that the attacks are becoming more and more sophisticated. The number of attacks of such type increased by 430% for 2019 in comparison to the same period of 2018. Consumer/institution loss is also directly dependent on the prompt reaction of the security system. Average loss within the first day after the fraud incident is calculated to be about $34, if the fraud is recognized within 3 to 5 months, the loss increases to $1,061.[3]

Covid-19 pandemic increased the risks of financial fraud significantly. In mid-March 2020, INTERPOL's Financial Crimes Unit issued a 'Purple Notice' alert to police in 194 countries and already blocked suspected fraudulent transactions worth USD 730,000.[4] The estimated rise in crime rates during the last financial crisis was over 10% and it is expected that this economic recession will be significantly worse. The unemployment is skyrocketing all over the world with little faith in government aid thus many may turn to desperate measures of using illicit activities to provide for themselves and their families.

This factor is especially significant if considered in combination with the increase of online transactions around the world. By introducing various levels of closures and insisting on social distancing, the governments induce the use of bank cards as opposed to cash for all transactions, including those that were rarely made in such a way (i.e senior citizens paying their utility bills). Thus, the likelihood of a skyrocketed demand for antifraud software is extremely high. And to meet this demand, the software itself should transform. The prevailing majority of existing solutions are rule-based. They have been built on long-monitored behavioral patterns that are no longer in place due to the pandemic outbreak. Even when the restrictions are lifted, it is unlikely that the behavior will change back in the nearest future. New habits are being formed that will be quite sticky but much less predictable thus the antifraud software should no longer rely on the presumably stable rules but become agile enough to evolve with the ever-changing circumstances. The speed of reaction is crucial in this case as some transactions to knowingly fraudulent accounts were blocked too late as the money had already been transferred further.[5] So an AI-powered real time solution is especially important to improve this situation.

Business Model, Operating Model

FraudBusters AI is an IT startup based on machine learning technology to provide fraud prevention and protection for Ukrainian banks. The model is based on a preliminary analysis of

[1] PWC. "PWC's Global Economic Crime and Fraud Survey 2020," 2020, 14.

[2] HSN Consultants, Inc. "The Nilson Report – Card Fraud Losses Reach $27.85 Billion," November 2019. https://nilsonreport.com/mention/407/1link/.

[3] NUData Security MasterCard. "2019: Fraud Risk at a Glance: Nudata Analysts' Interpretation of Real-Life Attacks," November 1, 2019. https://gallery.mailchimp.com/bf4a530dc0b5fbce4de4af60e/files/dc639831-4129-481b-8bc0-bc22e859f6a1/2019_Fraud_Risk_at_a_Glance_Report.pdf?_ga=2.253653833.1932551783.1576604990-419311239.1569444503.

[4] INTERPOL. "INTERPOL Warns of Financial Fraud Linked to COVID-19," March 13, 2020. https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-warns-of-financial-fraud-linked-to-COVID-19.

[5] Ibid

transactions, is learning from transactions, marked as fraudulent and not, identifying key patterns of fraud and then applying it to real-time data of transactions. As a result, potentially fraudulent behavior will be recognized immediately after happening and appropriate measures can be applied to minimize the losses by banks and banks' customers. The unique value proposition of the FraudBusters AI is a customized and tailor-made machine learning fraud prevention model that reflects specific bank's needs and evolves with the bank's growth.

Market analysis

The company has a primary customer segment - Ukrainian banks. Since the sales model will be based on the B2B approach, we will lend much effort to careful selection of the first group of customers with later expansion to all other banks of Ukraine. During the first year of operation we will work with those banks that are marked as 'risky' by the National Bank of Ukraine and are large and middle-range (with assets of more than 3 UAH bn). In a longer term perspective, the company expects to target other banks and, as a next step, also financial institutions that operate quite similarly to the banks so they will be included in the customers' pool at that time.

Current proposals of technological solutions are expensive. It may cost up to 2.2% of turnover, which is unprofitable for most banks. While it makes sense for some companies to pay per transaction, the banks' entire business is transaction-based so it would be more convenient to pay on a timely basis.

Sales

Sales model consists of two parts. The first part is a one-time payment for development and implementation of an individual model for one-time detection and prevention of fraud. The product is a one-time report marking the fraud risk, suspicious transaction patterns and model to detect and prevent fraud etc. The second one is subscription-based regular payment for technical and analytical ongoing support of the existing model. Support can be provided in two subscription packages: premium and basic. Basic model includes development and implementation of an individual model to detect and prevent fraud; real-time fraud alerts; monthly fraud prevention reports; 24/7 customer support. Premium package includes more services: daily analytical reports, regular updating of models, generation of additional variables.

Team

The company is founded by two highly motivated and technologically experienced founders. Further investment in the team will be made in two main directions. Most resources will go into creation of A level technological team, consisting of four senior data specialists and four juniors, providing 24/7 customer support. Additionally, two sales managers will be hired with the requirement of both business and technological expertise as the product will be sold to banks and financial institutions through direct sales and personal contacts. The company will invest in promotion of its expertise. Its management and technical specialists will be encouraged to publish articles and blogs in technical and business journals, participate in financial/banking and IT conferences and events, preferably as speakers.

Technology

There are two different technological approaches to anti-fraud protection: rule based and machine learning approaches. The rules can only be effective under stable conditions and require full reconsideration with every change. They are formed by anti-fraud experts and humans have limited ability to process data, especially big data, and rules are difficult to implement for real time processing of data. FraudBusters AI uses the second approach, based on machine learning technology. It involves development of fraud prediction models in 7 stages: from data processing and preparation to model development, assessment (the choice of models will be individual in each case as we understand that the capabilities and needs of banks are different) and tuning. We are able to correctly identify 90-95% of fraudulent transactions, using a minimum of resources in terms of time and cost of use.

Financials

Since the team will be actively working on sales, it is expected that the company will receive one on-demand model purchase and 14 months of basic subscription model purchase already in Year 1, resulting in forecasted net profit of UAH 4,000,000. The number of customers will increase during the Year 2 and we expect to gain net profit of UAH 11,700,000. Our expected gross profit margin will be quite close to the average profit margin for the industry (Software (System & Application) - 71,37%) - 68% in Years 1, 4, 5 and all the following years. Year 2 and 3 will have a slightly lower gross profit margin of 48% and 57% respectively due to two-stage expansion of the team because of growing number of customers on subscription model. However, the company will quickly recover from the gap in Year 2, demonstrating growth already in Year 3 and returning to 68% margin after that. Projected net profit margin is close to the average by industry (19,54%) in the Year 2 (20%) and Year 3 (22%) and growing significantly to over 30 and then over 40%.

Financing Required

The initial financing of UAH 750,000 will be provided by two founders of the company. In addition, the startup will apply to various funds, startup competitions etc to seek additional UAH 750,000. This money will be used to start the operations, including capital expenditures (laptops for administrative personnel and technical specialists), rent of office and salaries for the team (with the exception of the CEO and CTO) for Year 0.

The dividends of 25% will be paid out, starting from Year 2. Since the profit will increase, no additional financing from the investors will be required within the 5-year period. We expect to pay UAH 5.5 mln in dividends to the investors during the four-year period (Year 2 - Year 5) and we offer the following exit strategy: after Year 5 of operations the founders will buy the investors' share of the company.

MAIN TERMS AND DEFINITIONS

Fraud - an act of deceiving or misrepresenting.[6]

Banking fraud - an attempt to "to take funds or other assets from a financial institution".[7]

Transaction - "an event which involves money or payment, such as the act of depositing money into a bank account, borrowing money from a lender, or buying or selling goods or property".[8]

Fraud prevention - is a set of activities with the purpose "to prevent, to stop or keep from doing or happening, to hinder a person from acting".[9]

Machine learning - is "the concept that a computer program can learn and adapt to new data without human interference".[10]

[6] Merriam-Webster. 2020. "Definition of FRAUD." 2020. https://www.merriam-webster.com/dictionary/fraud.

[7] Investopedia. 2017. "Banking Fraud." Investopedia. March 26, 2017. https://www.investopedia.com/banking-fraud-4689709.

[8] Business Dictionary. 2011. "What Is Financial Transaction? Definition and Meaning." BusinessDictionary.Com. January 28, 2011. http://www.businessdictionary.com/definition/financial-transaction.html.

[9] Exactech. 2010. "Fraud Prevention." May 17, 2010. https://www.exactech.co/fraud-prevention/.

[10] Frankenfield, Jake. 2018. "Machine Learning." Investopedia. March 6, 2018. https://www.investopedia.com/terms/m/machine-learning.asp.

IMPLEMENTATION ROADMAP

The team will work on three tracks in parallel during Year 0, when the company will start its operations. First of all, the product itself will be further developed and enhanced. The model will be further tuned to provide the best performance. At the same time, the team will undergo the process of official legal registration of the company under the FraudBusters AI name and work through all needed formalities (registration at the tax agency, opening of the bank account etc.).

At the same time, the marketing track will also be gradually launched with the first phase - development of the marketing products, such as a range of product slide decks for various purposes and creation of the brochures to be used during meetings with potential customers. The team will prepare presentations for a major financial/banking forum and work with the organizers to present our product to the participants. This will boost the awareness and allow moving from cold to hot contacts faster.

Thirdly, the company will invest in the development of the customer support service. An efficient and effective customer success team will consist of technical specialists that will not simply serve as an intermediary, passing the information back and forth but be able to solve the problem immediately. They will provide 24/7 support to all clients, regardless of the subscription model. This will be developed during Year 1.

COMPANY DESCRIPTION

FraudBusters AI is an IT startup based on machine learning technology to provide fraud prevention and protection for Ukrainian banks. The model is based on a preliminary analysis of transactions, is learning from fraud transactions, identifying key patterns of fraud and then applying it to real-time data of transactions. As a result, potentially fraudulent behavior will be recognized immediately after happening and appropriate measures can be applied to minimize the losses by banks and banks’ customers. The unique value proposition of the FraudBusters AI is a customized and tailor-made machine learning fraud prevention model that reflects specific bank's needs and evolves with the bank's growth.

Description of company’s business and project’s current status

FraudBusters AI is an IT startup based on machine learning technology to provide fraud prevention and protection for Ukrainian banks. The model is based on a preliminary analysis of transactions, is learning from fraud transactions, identifying key patterns of fraud and then applying it to real-time data of transactions. As a result, potentially fraudulent behavior will be recognized immediately after happening and appropriate measures can be applied to minimize the losses. Moreover, the transactions will be further analyzed to identify potentially suspicious trends and prevent possible frauds by monitoring such cases closely. The benefit of this product is in its ability to process extremely large volumes of real time data without involving humans for preliminary analysis but rather at the stage of validating potentially fraudulent transactions. Additional robotic process automation can be applied to automate actions even further if any transaction is marked as fraud. The model and processes will be fully compliant with the client company’s policies and external regulations. As a result, financial institutions will be able not only to decrease their losses from different types of fraud but also save money on security personnel and improve customer experience significantly.

Unique value proposition: customized and tailor-made machine learning fraud prevention model that reflects specific bank’s needs and evolves with bank’s growth.

Customers' Problem

Fraud has become a hot topic for many companies in the world and Ukraine in particular. According to a Global Economic Crime and Fraud Survey 2020[11] performed by PwC, fraud is a billion-dollar business and growing every year. For instance, 48% of respondents in Ukraine said that their organizations had suffered from fraud in the last two years, compared to 43% in 2016. The conventional way of identifying fraud is resource-consuming and has low accuracy because it involves manual work. The increasing amount of data and penetration of digital technologies in business have caused a new wave of fraud that requires new methods of retaliation against that threat. There is a need for a cost-effective and fast way of fraud-detection for large-volume data sets. According to the market experts, if 2% of transactions were screened, it would result in reducing fraud losses accounting for 1% of the total.

Moreover, the Covid-19 pandemic has already created a new surge in the risk of financial fraud. In mid-March 2020, INTERPOL's Financial Crimes Unit issued a 'Purple Notice' alert to police in 194 countries and already blocked suspected fraudulent transactions worth USD 730,000. The estimated rise in crime rates during the last financial crisis was over 10% and it is expected that this economic recession will be significantly worse. The unemployment is skyrocketing all over the world with little faith in government aid thus many may turn to desperate measures of using illicit activities to provide for themselves and their families.

This factor is especially significant if considered in combination with the increase of online transactions around the world. By introducing various levels of closures and insisting on social distancing, the governments induce the use of bank cards as opposed to cash for all transactions, including those that were rarely made in such a way (i.e senior citizens paying their utility bills). Thus, the likelihood of a skyrocketed demand for antifraud software is extremely high. And to meet this demand, the software itself should transform. The prevailing majority of existing solutions are rule-based. They have been built on long-monitored behavioral patterns that are no longer in place due to the pandemic outbreak. Even when the restrictions are lifted, it is unlikely that the behavior will change back in the nearest future. New habits are being formed that will be quite sticky but much less predictable thus the antifraud software should no longer rely on the presumably stable rules but become agile enough to evolve with the ever-changing circumstances. The speed of reaction is crucial in this case as some transactions to knowingly fraudulent accounts were blocked too late as the money had already been transferred further.[12] So an AI-powered real time solution is especially important to improve this situation.

Banking industry has been the most affected by fraud even in pre-Covid-19 times and ready to spend a lot of money to protect the money of their clients and their own image. Because of strict regulations, banks are required to monitor transactions and report any fraudulent ones. In addition to that, the banking products are quite similar in terms of risks, so it opens the potential for cross sell. Because all banks are interested in fighting fraud and the machine learning models become more precise with time and amount of data they learn from, the network effect is applicable here as well. Banks would be more inclined to buy a product from the company that works with growing amounts of banking data and improves their model based on it.

Banks are playing an increasingly large role in the everyday life of the Ukrainian population. With the overall growth of income and the decline of the unemployment rate prior to the Covid-19 pandemic, the people had more money and increasingly turned to storing it in their bank accounts, at least for some time after they receive the payment (salary or social benefit).

[11] PWC. 2020. "PwC's Global Economic Crime and Fraud Survey 2020," 14.

[12] INTERPOL. "INTERPOL Warns of Financial Fraud Linked to COVID-19," March 13, 2020. https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-warns-of-financial-fraud-linked-to-COVID-19.

Moreover, with the start of the pandemic, the tendency to switch to card and contactless payments is increasing significantly. Digital payments allow one to stay away from money bills that change hands quite often and are not easy to clean with disinfectants. According to Bloomberg, the governments treat this very positively as a cashless economy increases tax revenue and helps fight corruption. The governments are seeking ways to minimize exposure to the virus through banknotes (i.e. using ultraviolet light or reissuing the notes) but going cashless is the most feasible solution.[13]

This is true for Ukrainian banks as well. According to the CEO of Privatbank Petr Krumphanzl, in the first two weeks of the quarantine in Ukraine, the average number of electronic transactions increased by 29%, payments in POS-terminal by 40%, downloads of bank's own mobile app doubled.[14]

While the overall number of customers in Ukraine, willing to use the banks for the prevailing majority of their money operations, is very volatile, the banks' assets remain stable and even showed a gradual growth in 2019. Moreover, despite the overall negative prognosis for Ukrainian economy, the Ministry for Development of Economy, Trade and Agriculture of Ukraine, the banking system is considered stable and the forecast for banks' development remains positive.[15] Their return on assets turned from negative in 2016 to positive and is slightly increasing.

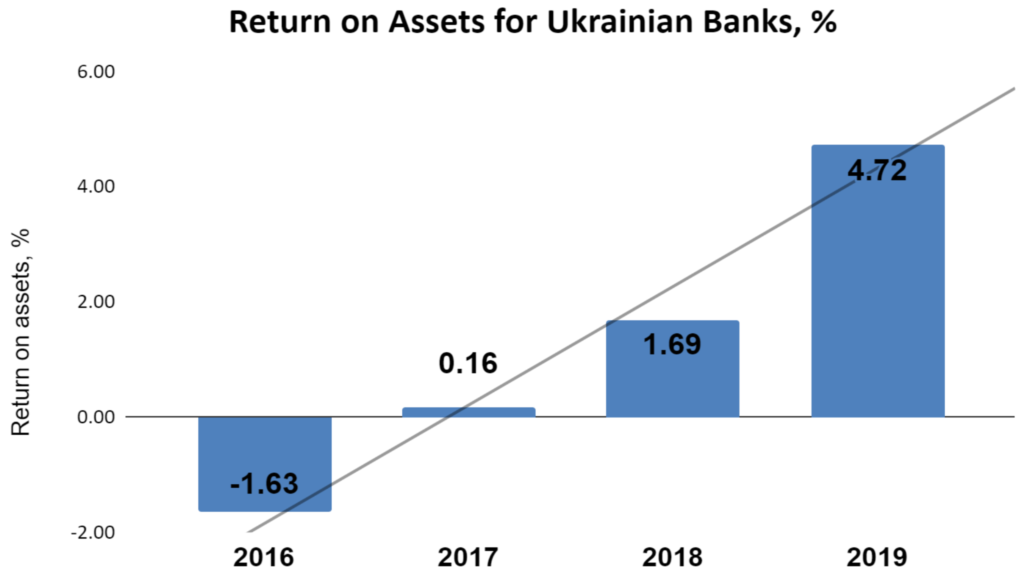


Figure 1. Return on Assets for Ukrainian Banks, % (bank.gov.ua)

At the same time, the trust in banks is very low according to various polls.[16] The people are using their cards more intensively, take more loans and make more deposits[17], but remain alert and ready to withdraw cash immediately if needed. Such cautious behavior has two root causes. The

[13] Surane, Jennifer, Olivia Rockeman, and Robert Schmidt. "Fear of Virus-Tainted Dollars Opens New Front in War on Cash." *Bloomberg.Com*, March 11, 2020. https://www.bloomberg.com/news/articles/2020-03-11/fear-of-virus-tainted-dollars-opens-new-front-in-war-on-cash.

[14] Шевчук, Сергей. "ПриватБанк: работа на Карантине, суды с Коломойским и кредитные каникулы. Интервью," 30 березня 2020. https://finance.liga.net/bank/interview/privatbank-rabota-na-karantine-sudy-s-kolomoyskim-i-kreditnye-kanikuly-intervyu.

[15] Прес-служба Мінекономіки. "Міністерство розвитку економіки, торгівлі та сільського господарства України -> Новини -> Уряд уточнив макропрогноз на 2020 рік," 30 березня 2020. https://www.me.gov.ua/News/Detail?lang=uk-UA&id=671cbaf4-7b1c-4ec5-a4af-10a852bc5a3e&title=UriadUtochnivMakroprognozNa2020-Rik.

[16] Бублик, Євген, and Юлія Шаповал. "Відновлення довіри до банків — завдання НБУ." *DT.Ua*, 2019. https://dt.ua/finances/vidnovlennya-doviri-do-bankiv-zavdannya-nbu-302948_.html.

[17] Національний банк України. "Огляд банківського сектору," 2020.

first one is the instability of the banking and political systems in Ukraine. This issue is more systemic and difficult to solve while the second one - the fear of the fraud resulting in irreversible money loss - is feasible and can potentially be dealt with. While the banks tend to invest ever-growing amounts of money into building their security and identification systems, the fraudsters are quick to break and/or hack them.

Increased use of electronic money and bank accounts as well as rapid development of technology has opened new opportunities for fraudulent activities globally. According to the Nilson report, card fraud will increase by about 5 USD bn per several years. Moreover, the loss per each 100 USD will be increasing then drop only slightly as the banks may invest even more in their security systems but will still remain high.[18]

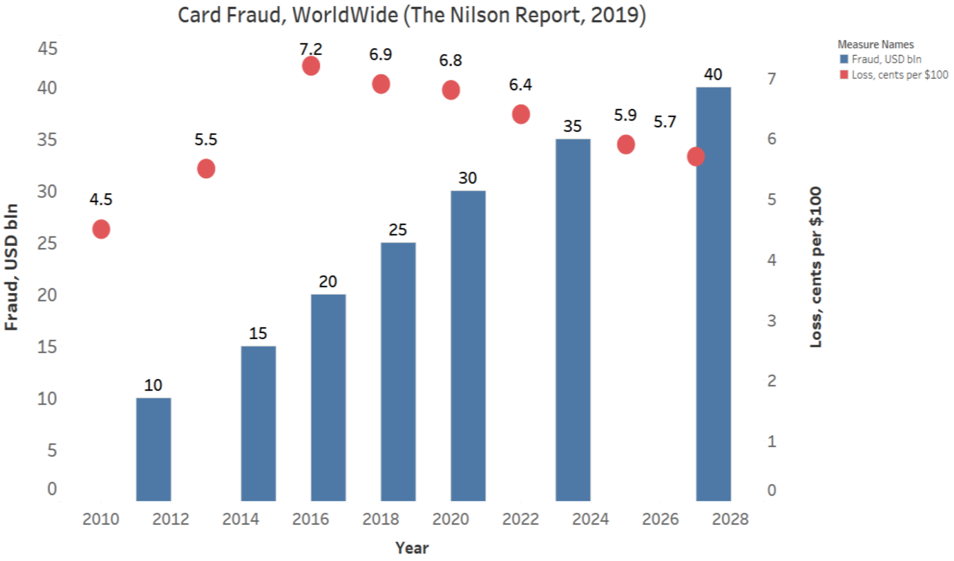


Figure 2. Card Fraud WorldWide (The Nilson Report, 2019)

In addition, the NU Security by MasterCard provides a detailed analysis that shows that the attacks are becoming more and more sophisticated. The number of attacks of such type increased by 430% for 2019 in comparison to the same period of 2018. They also indicate that it is becoming possible to track some patterns already. For instance, their data shows that February is the most likely month for attacks in retail, digital goods and travel while financial institutions should be much more cautious in September and the following few months. Consumer/institution loss is also directly dependent on the prompt reaction of the security system. Average loss within the first day after the fraud incident is calculated to be about $34, if the fraud is recognized within 3 to 5 months, the loss increases to $1,061.[19]

[18] HSN Consultants, Inc. 2019. "The Nilson Report – Card Fraud Losses Reach $27.85 Billion." https://nilsonreport.com/mention/407/1link/.

[19] NUData Security MasterCard. 2019. "2019: Fraud Risk at a Glance: Nudata Analysts' Interpretation of Real-Life Attacks." https://gallery.mailchimp.com/bf4a530dc0b5fbce4de4af60e/files/dc639831-4129-481b-8bc0-bc22e859f6a1/2019_Fraud_Risk_at_a_Glance_Report.pdf?_ga=2.253653833.1932551783.1576604990-419311239.1569444503.

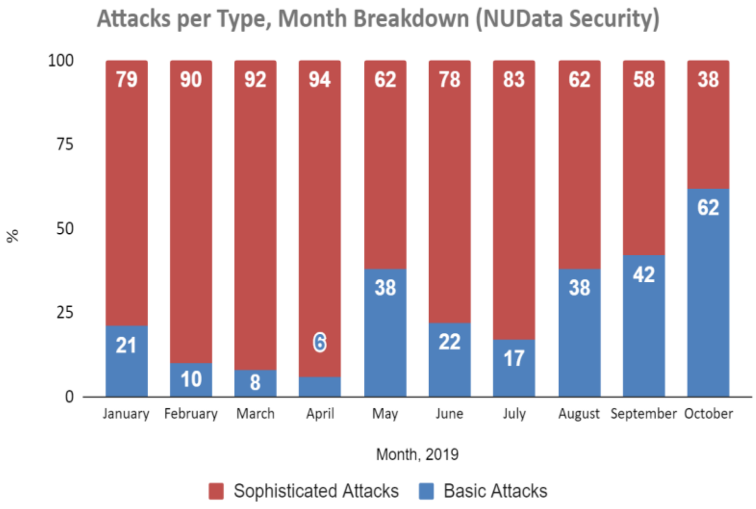


Figure 3. Attacks per type, breakdown by month (numbers are approximate)

The same tendency is true for Ukraine. Financial fraud here is becoming more sophisticated. According to EMA, in 2017-2018, over 60% of fraud was based on social engineering. This is especially difficult to prevent as frequently the clients are tricked into providing confidential information. While the clients and banks have a well-defined protocol for dealing with stolen cards, this requires a more multifaceted approach, that is offered by the AI technology.

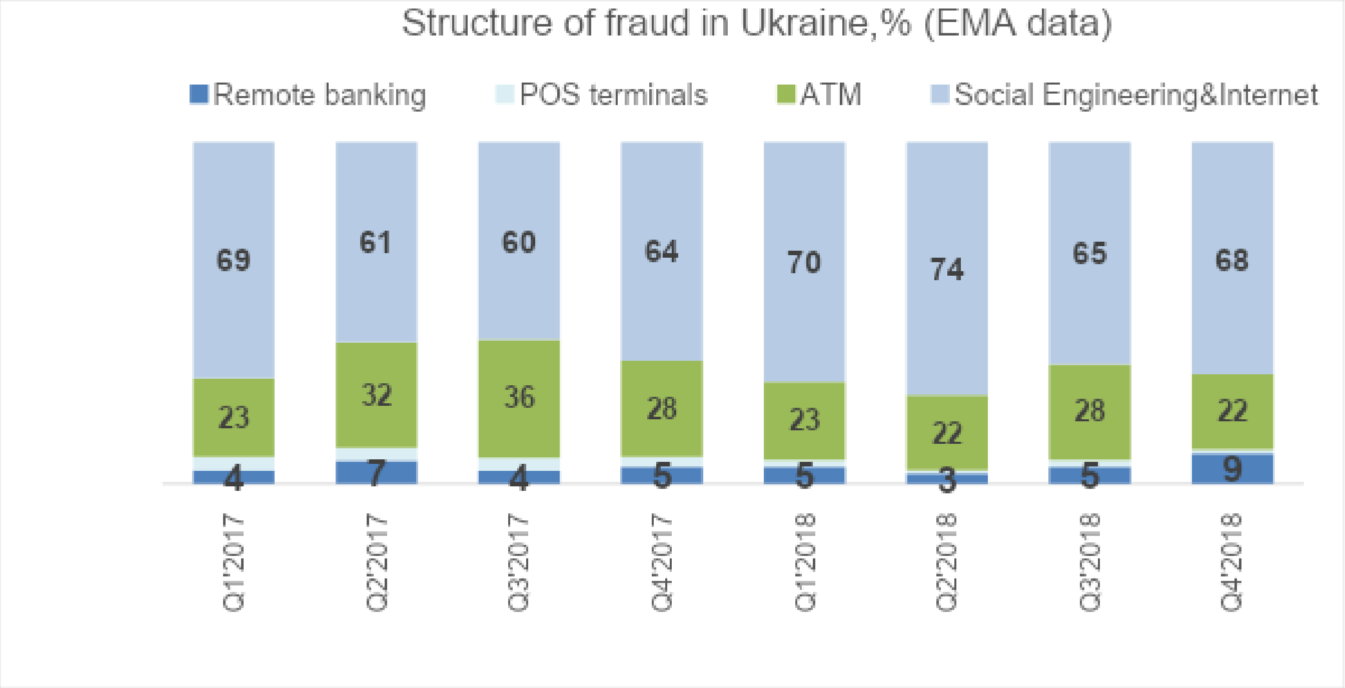


Figure 4. Types of financial fraud in Ukraine

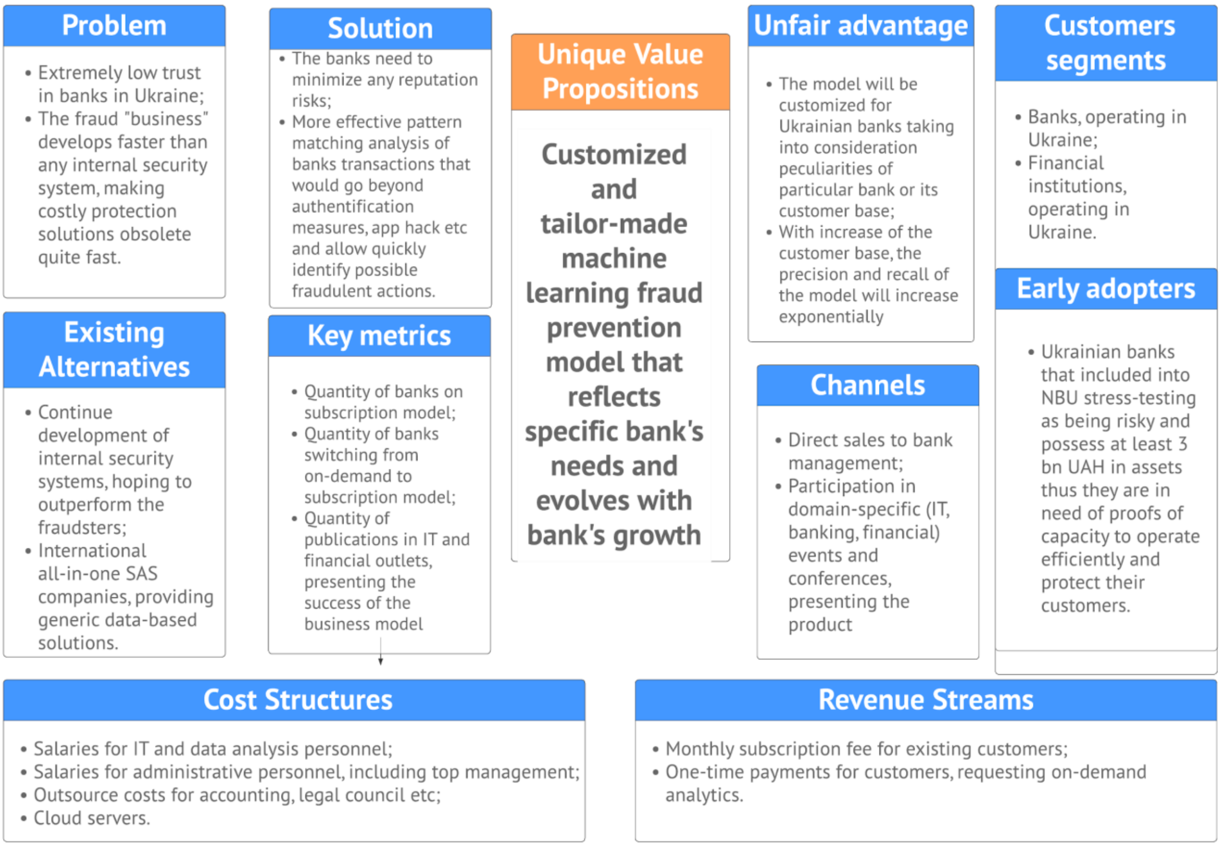
One more reason for banks to move towards a more rapid implementation of AI-based antifraud technologies is that use of AI may potentially decrease the banks' operation costs by 22% which can result in about USD 1 trillion worldwide. At the same time, the banks lack in-house specialists that would develop and install such models for them thus they are likely to utilize outsourcing and order such services from specialized companies such as FraudBusters AI.[20]

[20] Gilbert, Nestor. “10 Fintech Trends for 2020: Top Predictions According to Experts,” October 16, 2019. https://financesonline.com/fintech-trends/#AI.

Strategic plan

Our goal is to make the FraudBusters AI's model a standard for fraud prevention. For the banks, use of our product will mean significant decrease in losses because of fraud and increase in customers' trust. We offer a customized model that will be individually developed for each bank with the consideration of specific requirements, data available and demands. We will offer a low price for those banks that are willing to test our model by creating a possibility to order one-time analysis of banks' transactions and implementation of the model. However, our main profit will come from the customers using the monthly subscription model. They will receive a better accuracy of prediction due to regular updates of the model on the basis of incoming real-time data as well as more frequent and customized reports and alerts.

Analysis of business model



Problem

- Extremely low trust in banks in Ukraine;
- The fraud "business" develops faster than any internal security system, making costly protection solutions obsolete quite fast.

Existing Alternatives

- Continue development of internal security systems, hoping to outperform the fraudsters;
- International all-in-one SAS companies, providing generic data-based solutions.

Solution

- The banks need to minimize any reputation risks;
- More effective pattern matching analysis of banks transactions that would go beyond authentification measures, app hack etc and allow quickly identify possible fraudulent actions.

Key metrics

- Quantity of banks on subscription model;
- Quantity of banks switching from on-demand to subscription model;
- Quantity of publications in IT and financial outlets, presenting the success of the business model

Unique Value Propositions

Customized and tailor-made machine learning fraud prevention model that reflects specific bank's needs and evolves with bank's growth

Unfair advantage

- The model will be customized for Ukrainian banks taking into consideration peculiarities of particular bank or its customer base;
- With increase of the customer base, the precision and recall of the model will increase exponentially

Channels

- Direct sales to bank management;
- Participation in domain-specific (IT, banking, financial) events and conferences, presenting the product

Customers segments

- Banks, operating in Ukraine;
- Financial institutions, operating in Ukraine.

Early adopters

- Ukrainian banks that included into NBU stress-testing as being risky and possess at least 3 bn UAH in assets thus they are in need of proofs of capacity to operate efficiently and protect their customers.

Cost Structures

- Salaries for IT and data analysis personnel;
- Salaries for administrative personnel, including top management;
- Outsource costs for accounting, legal council etc;
- Cloud servers.

Revenue Streams

- Monthly subscription fee for existing customers;
- One-time payments for customers, requesting on-demand analytics.

Figure 5. FraudBusters AI Business Model

The product is dealing with the problem of extremely low trust for banks in Ukraine. It is mostly caused by the instability of the banks' system and fear that the bank may fall any minute as the precedents are quite frequent in Ukraine's recent past. At the same time, the fear of losing money is so ubiquitous that the customers are very alert and ready to withdraw money immediately once the first sign of the problem appears. As a result, every fraud case, negatively influencing the bank anyway, adds up to already low trust.

FraudBusters AI offers the solution by using machine learning techniques for pattern matching analysis of banks transactions. Practically all banks presumably have some type of security system in place. They invest in various authentication measures, protecting the consumers from the basic phishing, but the fraudsters are acting much faster and each new solution is quite quickly hacked. Thus, protection of transactions and security of bank client's money should take a step further and move beyond authentication frauds only.

Thus, the unique value proposition of the FraudBusters AI is a customized and tailor-made machine learning fraud prevention model that reflects specific bank's needs and evolves with the bank's growth. Compared to the competitors, this model has two main advantages. First of all, it will be customized for each client and the analysis will take into consideration some trends and patterns that are peculiar for Ukraine. Secondly, contrary to the main competitors, the company uses an entirely different pricing model - while they charge a percentage from transaction (which might turn into an insurmountable amount for the banks, whose business is transaction-based), we offer flat-fees for both the one-time use and monthly subscription. The latter comes in two versions: basic (including all features but less frequent updates) and premium (all features of the basic model and, additionally, more frequent reporting and updates etc.). Our unfair advantage is that, once the product is launched and the first banks purchase its services, the amount of data to train and improve the model will grow significantly, making the entry harder for the competitors.

The company has a primary customer segment - Ukrainian banks. The product is more likely to be purchased by the large and medium banks (with relatively significant assets of over 3 UAH bn) that experience some (frequently latent) problems thus were selected by the National Bank of Ukraine for the stress testing. This announcement is done publicly by the National Bank each year and the list is available on their website, therefore, these banks are already being closely monitored thus in need of measures to increase their reliability. In a longer term perspective the company will also include other Ukrainian banks and, as a next step, expects to target financial institutions that operate quite similarly to the banks so they will be included in the customers' pool at that time.

State-owned banks and banks belonging to foreign banking groups have longer decision-making chains thus it would take more time to negotiate the deal while it is important for the company to get its first clients. Small banks will also be considered during the first years of operations but they might be less capable of getting the premium models which is the ultimate goal of our marketing. We are not planning an expansion beyond the territory to Ukraine within the first five years of operations but this will be carefully analyzed when the scaling strategy will be created.

The product will be promoted predominantly through direct marketing. Since this is a B2B service and the number of customers is limited, it is more efficient to specifically target selected banks, gradually increasing the clients base. Additionally, the company will invest in promotion of its expertise. Its management and technical specialists will be encouraged to publish articles and blogs in technical and business journals, participate in financial/banking and IT conferences and events, preferably as speakers.

The success of the company in promoting and selling the product will be measured by the number of banks, testing the product (choosing one-time run of the fraud detection model); number of banks on subscription model; number of banks switching from on-demand to subscription model; number of publications in IT and financial outlets, presenting the success of the business model. This will allow the company to compare its performance to existing alternatives. Currently, there are two main groups of these. The first alternative way is to continue development of the banks' internal security systems. This would mean increasing investment into existing security measures with the hope to find a remedy for both current and future threats. This is not a feasible strategy as in most cases it will presumably be connected to increasing the 'physical' security while the fraudsters are leaning more and more towards behavioral methods that FraudBusters AI's product is also based on. The second alternative strategy would be to contract existing large international companies that provide similar SaaS solutions. However, most of these companies offer a generic solution for any type of company that has transactions thus they typically charge a percentage from each such transaction. While being more appropriate for, for instance, retail, this model will not work for the banks, whose business is transaction-based.

The costs will consist of capital expenditures on laptops for the company management and technical specialists and operational expenses: cloud service, salaries for the administrative personnel, including the company management, salaries for the IT team, salaries for the sales department. Most of the support functions (legal services, accounting) will be outsourced. Company's revenues will be, first of all, generated from the subscription model with lower price of one-time on-demand check as this type of service will be used primarily to introduce the client to the product, demonstrate its benefits and build trust.

This product will be sold to Ukrainian banks. Currently, there are 75 active banks functioning in Ukraine. They will be segmented on the basis of the following criteria:

1) ***Vulnerability and risk potential.*** National Bank of Ukraine conducts an annual stress-testing of the banks.[21] Sixteen banks that are included in the list for 2020 assessment will be considered the potential target for the first marketing campaign and for the first contracts.

2) ***Ownership***. The state-owned banks remain the most trusted and experience the largest growth of assets.[22] However, they will be excluded from the target audience as they already have relatively well-functioning security departments and specific requirements for working with vendors. This limits the list to 14 (two banks - Ukreximbank and Oschadbank are excluded).

3) ***Belonging to the foreign banking group.*** Four banks from the list belong to some foreign banking group which means that they must follow the rules and policies not only of the country they function in but also of these groups. Since this might potentially create additional difficulties and prolong the negotiations, these banks have been excluded from the target audience at least for the first two years of operations. This limits the list to 10 banks that will be contacted initially.

Ten banks selected for the target audience for the product launch have been further segmented on the basis of owned assets into large, medium and small. We will start from the first two groups being most likely to purchase our product.

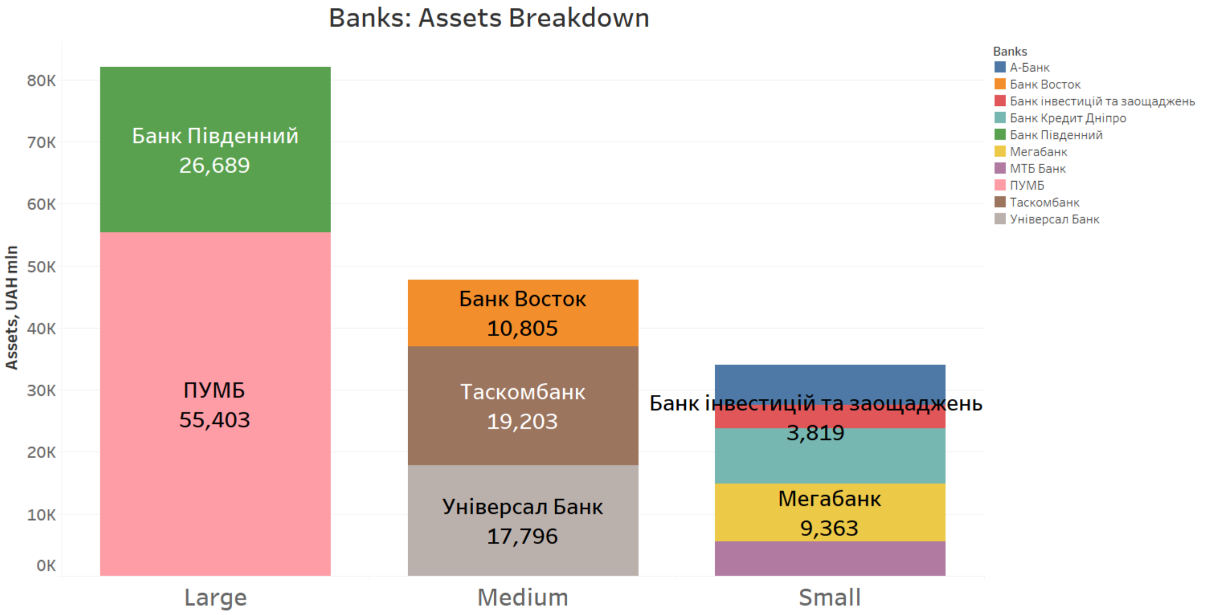
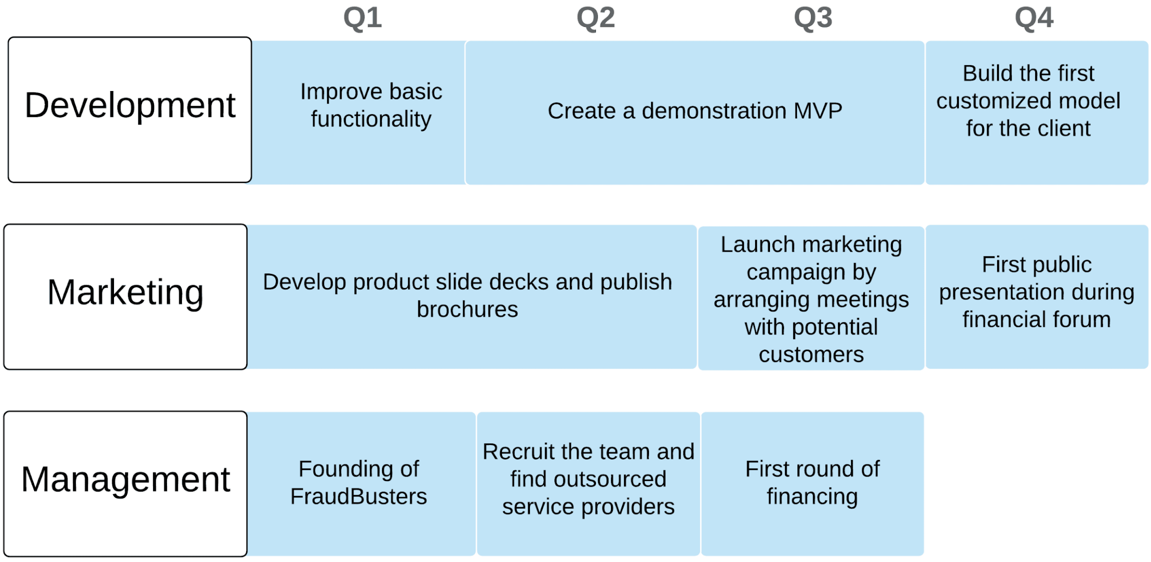


Figure 6. Banks' grouping by assets

[21] Національний банк України. "У 2020 році стрес-тестування проходитимуть 16 банків," 2020. https://bank.gov.ua/news/all/u-2020-rotsi-stres-testuvannya-prohoditimut-16-bankiv.

[22] Національний банк України. "Огляд банківського сектору," 2020.

Implementation plan



	Q1	Q2	Q3	Q4
Development	Improve basic functionality	Create a demonstration MVP		Build the first customized model for the client
Marketing	Develop product slide decks and publish brochures		Launch marketing campaign by arranging meetings with potential customers	First public presentation during financial forum
Management	Founding of FraudBusters	Recruit the team and find outsourced service providers	First round of financing	

Figure 7. Company's implementation plan

Description of company's implementation plan

The team will work on three tracks in parallel. First of all, the product itself will be further developed and enhanced. The model will be tuned to provide the best performance. At the same time, the team will undergo the process of official legal registration of the company under the FraudBusters AI name and work through all needed formalities (registration at the tax agency, opening of the bank account etc.). These two sets of activities will take place during Quarter 1 of the Year 0 of operations.

The marketing track will also be gradually launched, although its first phase - development of the marketing products, such as a range of product slide decks for various purposes and creation of the brochures to be used during meetings with potential customers - will go beyond Quarter 1 and last till the beginning of the Quarter 3.

During the Quarter 2, the team will expand to include a data scientist and a data engineer. This expanded team will develop a minimum viable product - a working model that would be used for demonstration purposes. Once the model is prepared, a sales manager will be additionally hired and trained and a more aggressive marketing campaign will be launched with the team members arranging the meetings with representatives from the selected banks (Quarter 3). In addition, during the Quarter 2, all other formalities will be resolved, i.e. all vendors for providing outsourced services will be selected. The team is expecting to receive it's first round of financing during Quarter 3.

Quarter 4 will be focused on further marketing activities. The team will prepare a presentation for a major financial/banking forum and work with the organizers to present the solution to the participants. This will boost the awareness and allow moving from cold to hot contacts faster. During Quarter 4 the team should also start working on the model for the first customer (at least 1 bank).

Possible risks and project risk mitigation techniques

Description/Detail	Probability/	Impact	Total	Priority	Mitigation	Risk owner

	Likelihood		Ranking			
Lack of data or data will be of poor quality	4	5	20	Very high	Analyze and provide guidance on data collection and storage	CTO
High churn rate and low level of conversion to subscription model	4	5	20	Very high	The sales team will work with each customer constantly monitoring the happiness level. In case when some problems emerge, the customer will be offered discounts or free months of subscription service	CEO
Absence of specialists with sufficient expertise in the bank	3	5	15	High	Develop clear instructions for model implementation and integration into Customer's systems	CEO/CTO
Banks decide to develop their own AI&ML expertise	3	5	15	High	Develop client retention strategy	CEO/CTO
Regulations of banks' operations will unable transfer of data to outsourced companies	3	5	15	High	In this case, we will consider a possibility of cooperation with the largest bank becoming an internal department	CEO
Loss of volume in sales	3	5	15	High	The sales and customer satisfaction team will be improved	CEO
Currency exchange rate fluctuations	5	3	15	High	Provide service price changes in the contract if the rate increase by >10%	CEO
The model accuracy will fall below promised threshold of agreed level	2	5	10	Average	The company will promise to pay a 10% fine to the bank, suffering from losses because of high inaccuracy. We will monitor the model performance and even the smallest drop in accuracy will result in hiring of additional technical specialists	CTO
Shortage of data science staff	2	4	8	Below average	Liaise with profiled IT courses and universities	CEO/CTO

Table 1. Risk mitigation matrix

TECHNOLOGY

There are two different technological approaches to anti-fraud protection: rule-based and machine learning approaches. The rules can only be effective under stable conditions and require full reconsideration with every change. They are formed by anti-fraud experts and humans have limited ability to process data, especially big data and are difficult to implement for real time processing of data. FraudBusters AI uses the second approach, based on machine learning technology. Our approach involves development of models in 7 stages: from data processing and preparation to model development, assessment (the choice of models will be individual in each case as we understand that the capabilities and needs of banks are different) and tuning. We are able to correctly identify 90-95% of fraudulent transactions with the use of minimum resources in terms of time and cost of use.

Overview of technological process

Today, there are two different technological approaches to anti-fraud protection: rule-based and machine learning approaches. Most anti-fraud systems use a rule-based approach. But nowadays these systems can be considered obsolete because they do not produce the desired results. First, the rules can only be effective under stable conditions. They work if the circumstances remain stable and require full reconsideration with every change. Second, the rules are formed by anti-fraud experts and humans have limited ability to process data, especially big data. Third, they are difficult to implement for real time processing of data. FraudBusters AI uses the second approach and is based on machine learning technology. Our approach involves development of models in 7 stages: from data processing and preparation to model development, assessment and tuning. We are able to correctly identify 90-95% of fraudulent transactions.

The main advantages of our approach are the ability to process big data in real time, constant self-improvement and improvement of model results, minimization of the impact of the human factors. The limitations of the model are possible lack or poor quality of the data, incorrect determination of fraud in the data that we will use to build the model. But for all such cases, we can provide guidance to customers on improving the quality of the data or devote more time to preparing the data for further analysis.

The approach of FraudBusters AI is explained in detail below

First step. Get access to the bank’s transactions’ database and evaluate it. The quantity and quality of the data determine how accurate our models will be. If the bank does not collect sufficient data, the implementation process may take 6 to 24 months.

Second step. Data preparation is one of the most resource-consuming and long-lasting steps:

- Clean and transform data. We store data on our servers unless otherwise agreed with the client, randomly reorder data that erases the effects of the particular order in which data was collected, remove duplicates, correct errors, deal with missing values, normalize data, etc.
- Explore and visualize data to identify patterns and factors that can help identify fraud and their importance for fraud detection. Also, we create new variables based on available data that will help improve model results (feature engineering). For example, this could be the distribution of purchases by night and day.
- The data will be divided into three different segments: training, testing, and cross-validation. The algorithm will be trained in a partial set of data and adjusted parameters in a test set. The performance of the model is measured by using the cross-validation set.

Third step. Model creation: to find an optimal and best performing model, different models will be designed and implemented during this step and their outcomes will be closely scrutinized and compared. For this purpose, we will use various machine learning algorithms to build a model. The following generally accepted criteria are important for selecting a particular model:

- Accuracy: The algorithm must have high accuracy in detecting fraudulent actions when processing large amounts of data.
- Coverage: The algorithm should cover as many possible fraud scenarios as possible.
- Cost: The algorithm should use minimum resources in terms of time and cost of use.

Below is an evaluation table for these parameters.[23]

Algorithm	**Type of algorithm**	**Frequency of implementation**	**Accuracy**	**Coverage**	**Cost**	**Total score**
Artificial Neural Network (ANN)	Supervised	40%	2	2	3	7
Decision Tree (DT)	**Supervised**	**38%**	**2**	**2**	**3**	**7**
Support Vector Machine (SVM)	Supervised	34%	3	3	3	9
Genetic Algorithm (GA)	Unsupervised	26%	2	2	1	5
K-Nearest Neighbor (KNN)	Unsupervised	20%	2	2	3	7
Bayesian Network (BN)	Supervised	16%	3	2	3	8
Hidden Markov Model (HMM)	Unsupervised	16%	1	1	3	5
Logistic Regression (LR)	**Supervised**	**16%**	**3**	**2**	**2**	**7**
Random Forest (RF)	**Supervised**	**16%**	**3**	**2**	**2**	**7**
Fuzzy Logic Based System (FL)	Supervised	8%	3	2	3	8

Table 2. Comparison of ML Algorithms for Fraud Protection Model

The choice of models will be individual in each case as we understand that the capabilities and needs of banks are different.

Fourth step. We do several iterations of model training so that the model provides the correct prediction as often as possible. It is worth noting that there is no such solution that can correctly predict 100% fraud. We will treat it as a good result if the accuracy of prediction is above 90%.

Fifth step. We test the model and evaluate the results. We use different metrics to measure objective performance (i.e. confusion matrix, precision-recall, test validation data, overfitting etc.)

[23] Minastireanu, Elena-Adriana, and Gabriela Mesnita. “An Analysis of the Most Used Machine Learning Algorithms for Online Fraud Detection.” *Informatica Economica* 23, no. 1/2019 (March 30, 2019): 5–16. https://doi.org/10.12948/issn14531305/23.1.2019.01.

Sixth step. We adjust the hyperparameters for better performance. For example, we set a number of training steps and learning rate.

Seventh step. Deployment: we embed the model into the processes of verification of transactions in the bank system.

During the analysis, we will receive new data and, if necessary, modify the models accordingly for better results.

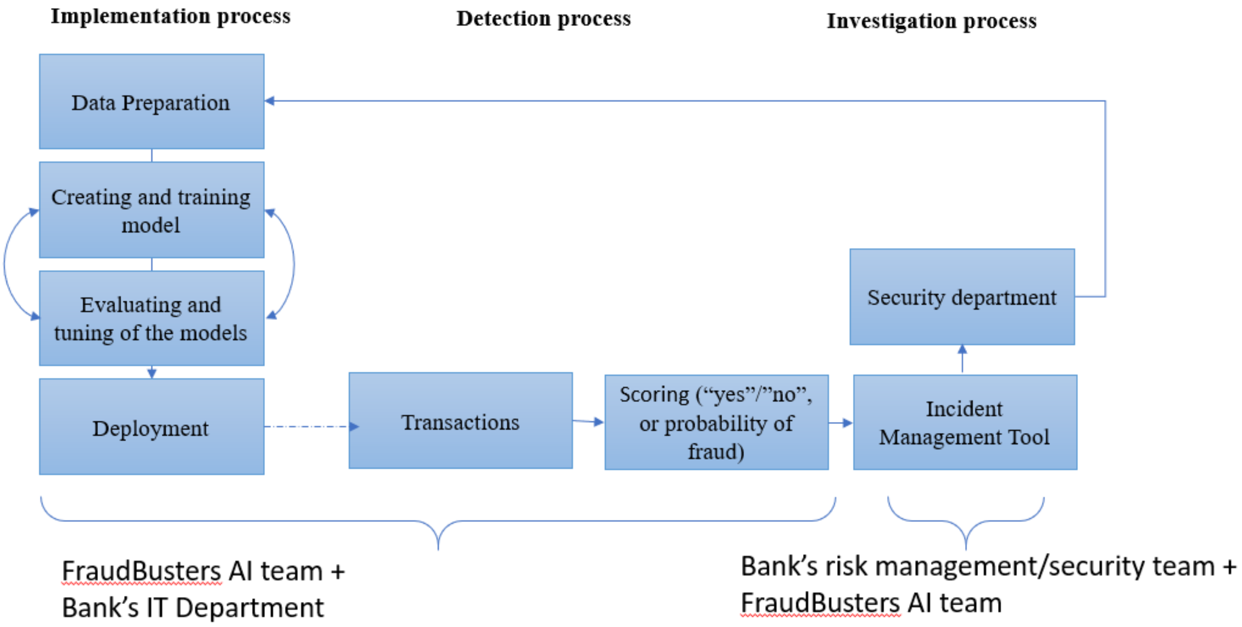

Implementation process
Detection process
Investigation process
Data Preparation
Creating and training model
Evaluating and tuning of the models
Deployment
Transactions
Scoring ("yes"/"no", or probability of fraud)
Incident Management Tool
Security department
FraudBusters AI team + Bank's IT Department
Bank's risk management/security team + FraudBusters AI team

Figure 8. Machine Learning antifraud systems (proposed approach).

MARKET ANALYSIS

Two main approaches to fraud protection are rule-based and machine-learning approaches. Both are currently present on the market with the first one still dominating but the second one quickly developing and proving its potential to overcome existing drawbacks of the rule-based approach. It is also more powerful in working with large-volumes data in real time. Future trends of the fraud protection industry are three-fold. First of all, the “physical” means to increase the transaction security are being developed further (a typical example is a multi-factor authentication, i.e a password and a code sent additionally). The second innovative technological domain that can either support or disrupt our business is the blockchain. Some banks are already using it to share information on their customers among themselves without breaching the data privacy. The third innovation in the industry will be closely followed by the FraudBusters AI as any new developments in this field may help improve our performance further. As an alternative usage of the product, the FraudBusters AI’s model can be further developed for the purposes of the upselling of the additional banking services to the bank customers.

EMA Association estimated that Ukrainians lost about UAH 1 billion due to illegal actions of fraudsters in 2017-2018.[24] Banks are forced to invest more and more resources into anti-fraud activities and admit that this has become their top priority. We expect the amount of fraud to grow, so the demand for AI antifraud solutions will increase. The following factors will contribute to this:

1) The crime rate will rise. The pandemic will deepen the economic recession, and many people will lose their jobs. The statistics from the previous crises indicates that the crime rate typically increased by at least 10%[25] and this time the situation is predictably much worse.

2) Fear of contracting a new virus will accelerate the growth of online payments. Authorities are now pushing to pay for purchases with a card rather than cash. Many people who have used cash for various reasons (fear of being deceived, have never done it before as they do not know how, to and so on), switch to payment cards and are more likely to use cards for various payments in the future.

3) Quarantine and rather strict lockdowns change people's behavior and lifestyle in a drastic way. People buy differently (changing their shopping style, places to buy, grocery carts etc.), spend time differently, etc.

4) Because of these changes, the ‘old’ rules no longer apply. The current most commonly used rule-based approach will result in more and more errors. The analysts who develop and set these rules cannot predict fast and precisely enough what comes next to effectively develop new rules. In contrast, machine learning algorithms are capable of processing large data sets and updating fraud tracking models with greater velocity and accuracy.

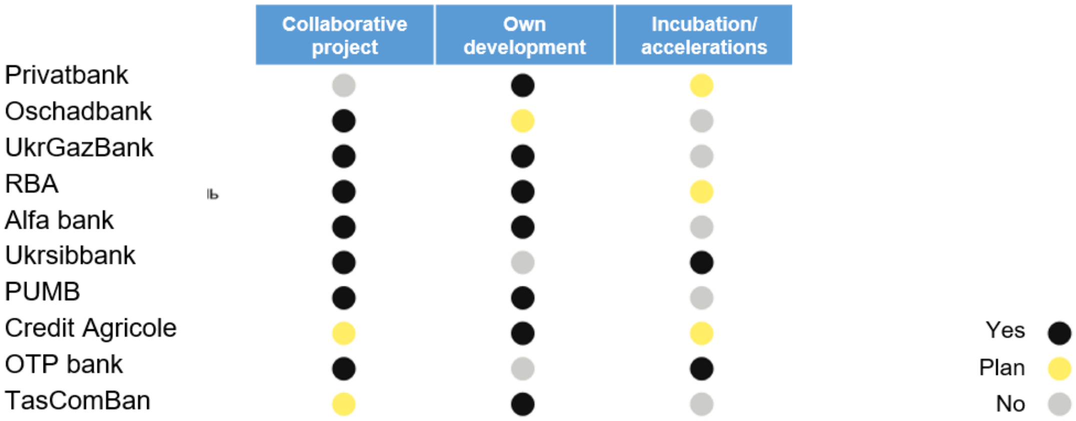
McKinsey states that nowadays only 15% of bank risk control measures are based on analytics, but the percentage will very likely rise to 40% by 2025.[26] According to the research by Denovo, the leading Ukrainian banks start to develop and use new technological solutions[27]. In this regard, they use both possible ways of implementing this - develop own products independently as well as involve external contractors.

[24] Руденко, Виктория. “Мошенники лишают денег доверчивых украинцев - Финансовый клуб,” 2019. https://finclub.net/analytics/moshenniki-lishayut-deneg-doverchivykh-ukraintsev.html.

[25] Bugriy, Maksym. “The Difficult Path to the Security Reform.” *The Ukrainian Week*, June 2, 2012. https://ukrainianweek.com/Security/51920.

[26] Microsoft Corporation. “Banking on AI,” 2018. http://info.microsoft.com/rs/157-GQE-382/images/EN-CNTNT-eBook-BankingonAI.pdf.

[27]Denovo. “Digital Transformation of Ukraine Vision 2025,” 2019. https://businessviews.com.ua/ru/digital-transformation-2019/.



	Collaborative project	Own development	Incubation/ accelerations
Privatbank	○	●	🟡
Oschadbank	●	🟡	○
UkrGazBank	●	●	○
RBA	●	●	🟡
Alfa bank	●	●	○
Ukrsibbank	●	○	●
PUMB	●	●	○
Credit Agricole	🟡	●	🟡
OTP bank	●	○	●
TasComBan	🟡	●	○

Yes	●
Plan	🟡
No	○

Figure 9. Cooperation of the top banks and fintech

The most advanced banks in Ukraine have already achieved some results. For example, PrivatBank's anti-fraud system helped save 23.4 million UAH of customers' money already in 2017,[28] Alfa Bank launches its own machine learning antifraud system in 2020.[29]

As a result, according to our estimation, the anti-fraud market may experience at least a twofold growth within the next two years.

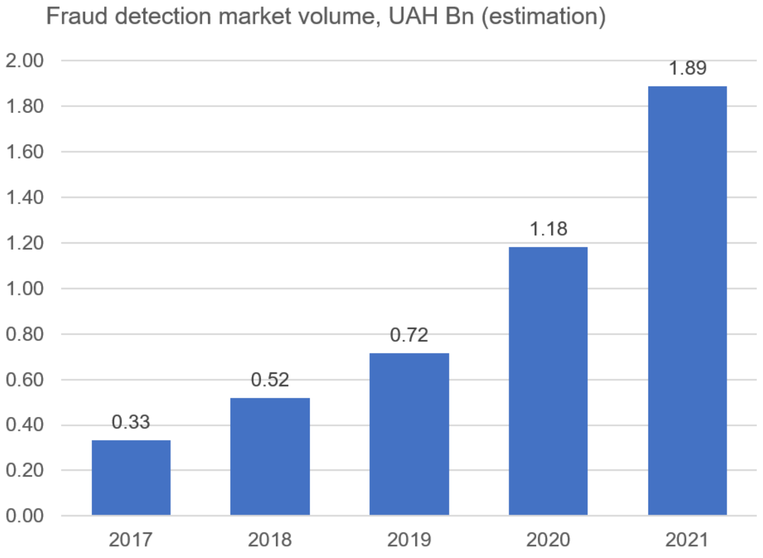


Figure 10. Estimated volume of fraud detection market

Overview of best practice approaches in the market/segment

Technologies for fraud detection and monitoring to prevent any fraudulent activities may be grouped into the following broader types of fraud detection:

[28] Кулеш, Сергей. “Интеллектуальная Антифрод-Система ПриватБанка Предотвратила 99% Мошеннических Операций в Электронных Сервисах Банка в Прошлом Году.” ITC.ua, 3 жовтня 2017. https://itc.ua/nes/intellektualnaya-antifrod-sistema-privatbanka-predotvratila-99-moshennicheskih-operatsiy-v-elektronnyih-servisah-banka-v-proshlom-godu/.

[29] Дыдышко, Виталий. “Как Искусственный Интеллект Меняет Работу Крупного Украинского Банка. Интервью - Новости Технологий Украины и Мира.” LIGA.net, 13 грудня 2019. https://tech.liga.net/technology/interview/iskusstvennyy-intellekt-v-alfa-bank-ukraina-kak-mashiny-i-lyudi-razdelyat-obyazannosti.

- Proactive and Reactive;
- Manual and Automated.

The main approaches to fraud prevention include:

- Rule based approach. It is based on business rules and experience of the company. The analysts formulate a set of principles and create a program to filter data and identify potential fraudulent behavior on the basis of these principles (rules).
- Descriptive analytics (unsupervised learning). The data is analyzed to detect deviations from normal behavior and novel fraud patterns using clustering that allows identifying outliers. The techniques of doing this include statistical outlier detection method (Z-scores, Break-Point Analysis, Peer-Group Analysis, Recency, Frequency, Monetary scoring, Association Rule Analysis), Clustering algorithms (Hierarchical Clustering, Partitioning Clustering, Self-Organizing Maps), and ONE-CLASS SVM.
- Predictive analytics (supervised learning techniques) allows to find fraud by using regression to predict a continuous target variable such as the “amount of fraud”, classification to score “probability” with binary category target variable “fraud” vs “no-fraud” or multiclass category “severe fraud”, “medium fraud”, ”no fraud”. Main algorithms: Logistic Regression, Decision Tree, Neural Networks, SVM, and Ensembles methods (bagging, boosting).
- Cluster Migration Analysis investigates changes of cluster membership throughout time, which are caused by changes in data provoked by events, such as new offers, promotions, etc. Analyzing these changes over a period of time helps to understand the usage patterns better, produce fraud signals such as abrupt clustering changes and analyze which attributes changed most significantly and trigger clustering migration.

Today most banks use the rule-based approach for antifraud systems. It entails finding a fraud by looking at on-surface and evident signals. If the system recognizes a suspicious transaction (for example, a large amount of money spent or transferred, atypical purchases, etc.), an additional verification is performed. These signals and rules are developed by anti-fraud experts manually based on previous experience. Usually, such legacy systems apply on average about 300 different rules to approve or block a transaction.

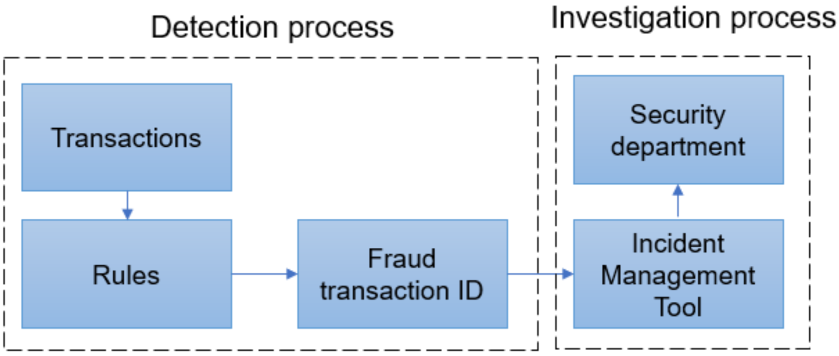


Figure 11. Rule based anti fraud systems (most used approach)

FraudBusters AI uses a machine-learning based approach. Machine learning is a set of methods and techniques that let computers recognize patterns and trends and generate predictions based on those. Today, ML approach shows better results for big companies because it has many benefits over the rule-based approach, and overcomes the limitations of it.

Advantages of using machine learning for anti fraud systems are following:

- Machine learning can process large amounts of data and identify specific trends and patterns that would not be obvious to humans.

- Real time processing.
- Fast data processing and minimum manual work. Thus, the likelihood of human factors' impact is close to zero.
- The algorithms constantly enhance accuracy and efficiency. This allows them to make better and faster decisions. In other words, there is a constant process of self-improvement.

Limitations of our approach:

- Lack of required data from the customer or the data will be of poor quality. In this case, we will have to analyze and provide guidance on data collection and storage, or spend a lot of time preparing it.
- Low quality of classification of the data that will be used to build models. For example, a large number of the fraud transactions will be labeled as "normal" or vice versa (the quantity of false positives or false negatives will exceed the acceptable rate). Human factors will be minimized but still have some influence during the initial model development and their decisions can lead to erroneous definitions. Therefore, we will need to perform several iterations of model development, which is already foreseen in the project implementation timeline.

Overview of trends

Fraud protection industry is developing in three main directions. First of all, the “physical” means to increase the transaction security are being developed further. The banks as well as other services are already using two-factor authentication to ensure that the transaction is being made by the account owner. Currently, the two-way authentication is being gradually replaced by the multi-factor authentication and the third, fourth and all other ways are based on providing biometric information. For instance, a person might be asked to confirm her identity by typing a password (a classic method), a code from email or text message (two-factor), and a fingerprint or undergo voice or facial recognition.[30] More and more devices have software necessary for such authentication methods in a secure way. Thus, biometric information recognition might potentially take a certain share of the market, although the fraudsters are already quite prepared to meet this challenge. Moreover, the techniques that can help successfully trick the system are quite primitive. The fingerprints can be made with liquid silicon or rubber cement, the eye or face recognition can be fooled with a high resolution photo, and voice can be easily modified with the readily available software.[31] Nevertheless, the technological development in this stream is also happening thus should be closely monitored as potential competitors may come from this field.

The second innovative technological domain that can either support or disrupt our business is the blockchain. The banks are using the blockchain mostly to verify the identity of their customers in order to meet tightening regulations about prevention of money laundering or financing of terrorist attacks. Thus, they are forced to invest in “know your customer” policy and this burden can be shared by several banks who form and maintain this database jointly through the blockchain.[32] In the pseudonym based blockchain network, the operations (transactions) are performed using a signature (“Proof of Work”), ensuring the validity of the transaction by the UTXO (“Unspent Transaction Output”) method in Bitcoin or similar approaches in other digital currencies may provide an innovative way for the banks to validate the transactions through this distributed ledger system.

Finally, the third innovation in the industry will be closely followed by the FraudBusters AI as any new developments in this field may help improve our performance further. The model, applied by our company to identify fraud, will already be performing half-automatically. Human analysts will be involved only to check the transactions marked by the model as potentially suspicious. However, this process can be further automated with the use of robotics with the algorithms that can go through marked transactions and perform necessary routine operations before involving a human being, minimizing the time spent on these and increasing speed and efficiency of fraud identification.[33]

[30] KPMG. “Global Banking Fraud Survey,” May 2019, 24.

[31] Wilder, Mason. “Brave New World: Can Biometric Security Help Fight Fraud?,” April 22, 2019. https://www.acfe.com/fraud-examiner.aspx?id=4295005744.

[32] Deloitte Legal. “Blockchain WP March 2018_.Pdf,” March 2018. https://www2.deloitte.com/content/dam/Deloitte/sv/Documents/legal/Blockchain%20WP%20March%202018_.pdf.

[33] JPMorgan Chase. “Redefining the Financial Services Industry: JPMorgan Chase 2016 Annual Report,” 2016. https://www.jpmorganchase.com/corporate/investor-relations/document/ar2016-lettertoshareholders.pdf.

Overview of alternative uses of company's product on the market

One potential use of the FraudBusters AI's product is for the upsale of additional banking services to the bank customers. The transactions will be already analyzed to recognize patterns thus the model could be retrained for new purposes - to identify the customers that might agree to take a loan, put money on a deposit, upgrade their service package etc. JPMorgan Chase has already tested such platform, titled "Emerging Opportunities Engine"[34] that was mostly used for stock trading but can be expanded to include other products.

In addition, the model can be used to recognize fraud for the retailers. For instance, it can help identify fraudulent behavior with regard to loyalty programs. As an example, fraud is considered as earning points for purchases that were made by someone else. The most common case is when a person asks other buyers to use their loyalty card. On one hand, this behavior is not a violation of the law, but, on the other hand, they do not make purchases which is a core purpose of the loyalty program. Instead, they accumulate points that are equivalent to tens of thousands of hryvnias and later use them. So our fraud prevention program can be helpful in this regard as well.

[34] JPMorgan Chase. "Redefining the Financial Services Industry: JPMorgan Chase 2016 Annual Report," 2016. https://www.jpmorganchase.com/corporate/investor-relations/document/ar2016-lettertoshareholders.pdf.

SALES AND MARKETING

This product will be sold to Ukrainian banks. Currently, there are 75 active banks functioning in Ukraine. They will be segmented on the basis of the following criteria:

- Vulnerability and risk potential. National Bank of Ukraine conducts an annual stress-testing of the banks. Banks that are included in the list will be considered.
- Ownership. The state-owned banks remain the most trusted and experience the largest growth of assets. However, they will be excluded from the target audience as they already have relatively well-functioning security departments and specific requirements for working with vendors.
- Belonging to the foreign banking group. Banks belonging to some foreign banking group must follow the rules and policies not only of the country they function in but also of these groups which might create additional difficulties and prolong the negotiations.

Positioning statement: For top Ukrainian banks that want to decrease losses from costs of fraud and improve customer experience connected with that, Fraudbusters AI delivers more accurate and faster predictions applying customized machine learning models.

Key message: The most accurate fraud prediction

Competitive environment

We group our competitors into two large types:

- Small, highly specialized fintech companies such as WayForPay Antifraud, Signifyd, and NoFraud. These companies provide one-size-fits-all solutions for all clients and use fee payment model (1-2% of the amount of each transaction), which are not appropriate for big finance companies. They are less bound by internal procedures and processes compared to the second group but their pricing model may work for retail but is too expensive for the banks whose entire business is transaction based. Therefore, they mainly work with ecommerce and small banks and lending institutions. Their market share is about 75-80%.
- Large-scale IT companies providing similar software as a service can offer tailor-made ML solutions (Softserve, Eleks, etc.). While some banks may turn to them, considering them as more reliable and reputable, their products are more standardized and they lack velocity in adjusting them to the needs of every specific customer. Since they are not specializing on the antifraud, their solutions are more expensive in comparison to the first group (high labor costs, more time to develop models, etc.). Their share is 20-25%.

Payment systems such as Visa and Mastercard, while having some research and activities on antifraud, are pursuing the zero liability policy, putting the responsibility on card issuers. In practice, it means that the customers are not held accountable for any fraud occurring to their cards. All expenses are to be covered by banks and if banks are delaying the repayment, are not effectively investigating the case etc, they are fined by Visa and Mastercard.[35] Antifraud service does not compise the basic earnings for Visa and Mastercard and they do not promote this service in our country.

Our main competitive advantage can be clearly identified through the use of VRIN/VRIO framework. The capabilities that make our business stand out include, first of all, a machine learning approach. While this is extremely valuable as it allows for a better prediction in

[35] Mastercard. “Card Issuers Safety & Security,” May 27, 2015. https://www.mastercard.us/en-us/issuers/safety-security.html; Visa. “Visa’s Zero Liability Policy,” March 7, 2020. https://usa.visa.com/pay-with-visa/visa-chip-technology-consumers/zero-liability-policy.html.

comparison with the rule-based approach as well as rare as most solutions on the market use the latter. We believe that this is the future of the industry and will be used by most companies soon. The same applies to AI and data science technologies that our transaction reports will be based upon. We will bring together top-notch approaches both to development of the model and to interpretation of its results. Another valuable and rare resource that our business possesses is flexible pricing. While the other approaches may bring higher profits faster, we find it more important to build long-term relationships with the customers and move them up the pricing models gradually. 24/7 customer support and happiness management will facilitate this process and ensure high quality of the service being a valuable, rare and non-substitutable resource.

Finally, our main competitive advantage that is valuable, rare, inimitable and non-substitutable is the individual and tailor-made models of fraud detection. We are convinced that each bank has its own unique set of customers, using its services for specific purposes. Thus, no matter how wide a range of rules for fraud identification purpose, it would not be able to cover all possible cases. Our model will be based on real transaction data from each bank and be regularly updated - the service not currently offered by any of existing competitors.

Advantage	**Valuable**	**Rare**	**Inimitable**	**Non-Substitutable**
Machine learning approach	✓	✓		
Individual models of fraud detection	✓	✓	✓	✓
24/7 support	✓	✓		
AI&Data science analytics	✓	✓		
Flexible pricing (different packages)	✓	✓		

Table 3. VRIN framework analysis

Also, below is a comparison of our company and its main competitors in terms of key service criteria:

- Time: how quickly a model can be designed and implemented. The small companies that specialize in fraud are able to implement the model faster, while larger companies need more time;
- Cost of model development and implementation. Current proposals from small companies are expensive - it may cost up to 2.2% of turnover. Larger companies have more flexible pricing and that is their advantage;
- Accuracy: how accurately the company's product can predict fraud. Individual models are able to provide a more accurate prediction of fraud as they take into account the particularities of banks and their data.

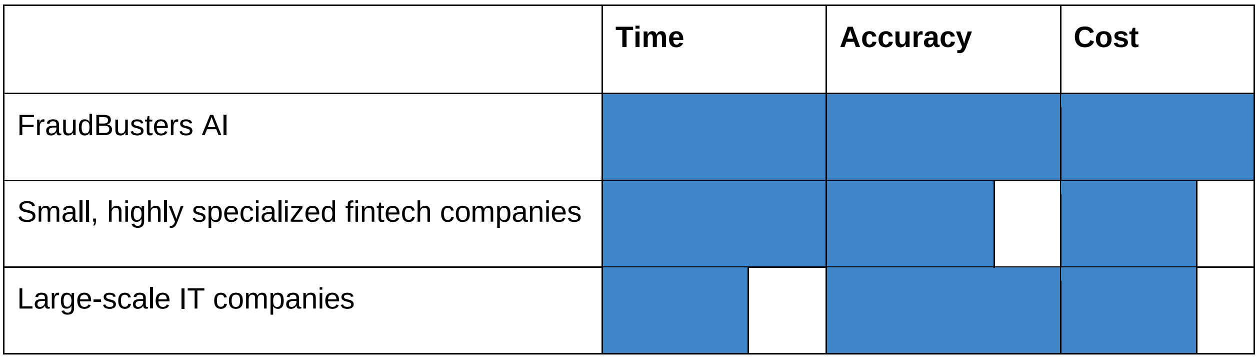


Table 4. FraudBusters AI's competitive advantage based on customer needs

FraudBuster AI is better than small companies in terms of cost and accuracy, and better than large companies in terms of time.

Description of marketing mix

The product will be focused on the banking industry and include 30 Ukrainian banks that are vulnerable to risk (marked as such by the National Bank of Ukraine by including for the stress-testing or in any other way) and have large or medium-size assets of at least 3 billion UAH. Accordingly, for the very first contracts we will start with 10 banks that have been selected by the National Bank of Ukraine for 2020 stress testing, have large or medium-size assets and do not belong to any foreign banking groups. This list will be gradually expanded to abovementioned 30 Ukrainian banks that correspond to the same criteria and even further. The platform provides individualized solutions to improve accuracy of predictions and speed of prediction based on the customers' IT infrastructure. Thus, it makes it scalable beyond the banking industry but also to include different financial institutions can benefit from it.

The target audience for the product promotion can be described as top executives and bank managers who make or can initiate decisions on the implementation of fintech products.

Key characteristics of a representative of the target audience:

- ***Key demographic:*** male 95%, female 5%, 35-55 y.o;
- ***Key psychographics:*** is proud of the bank/working in the bank and reluctant to trust any third-party, needs very brief and precise memos but with enough data and numbers to prove the point, adversive buyer-seller relations;
- ***Preferred channels:*** personal contacts (through recommendations of a trusted party), meetings at conferences, special events, in expensive/fancy restaurants.

Marketing mix

Product

The product is a platform integrated into the bank's IT system that will monitor the transactional data and identify potentially fraudulent transactions. When a suspicious transaction occurs, the system will send a message and supporting data according to the bank's policies. In addition to that, a potentially fraudulent transaction will be blocked and an additional transaction verification step will be initiated.

The product includes:

- Customized tailor-made machine learning model that is adjusted for each bank and conducts analysis of the bank's transactions to identify untypical behavior of each individual customer to recognize and prevent fraud;
- Real-time fraud alerts, allowing the banks to save money;
- Regular reports, systemizing the risks for the bank (as a made-up example: "the most frauds happen at 10-11.30 pm in the mostly empty by then office centers thus such transactions require increased attention");
- Intuitive interactive dashboards, allowing the bank's management to check the main statistics for bank's transactions and download "quick" fraud reports.

Price:

We use a market skimming objective price strategy – high initial price for a new product to benefit from those who are ready to pay a high price. The price will consist of two models:

1) low 'entry' price for those, who would like to test whether the model fits their purposes which would ease the decision to try;

2) long-term support subscription-based model for providing analytics and reports.

The subscription has two types:

- Basic plan
- Premium (more frequent updates and reports).

Transparent and predictable price is our competitive advantage as, while the competitors charge percentage from each transaction, we offer an all-inclusive monthly-based subscription price. The closest competitors use a per-transaction fee payment model - from 0.4% up to 3% of each transaction. On the one hand, our price will be much higher at the start, but then with the increase in the number of transactions our model will be more profitable for banks. So, we expect customers to be interested in this kind of collaboration model.

Place:

Due to the fact that banking data is very sensitive and should be unpersonalized when algorithms are learning from it, the platform will be integrated with the bank's IT system and the transactions' data will be proceeded on the bank's own servers (on premise). But a cloud option will be also available. All information that will be used for machine learning and building a model will be encrypted.

Promotion (promotional mix):

The following nuances are taken into account when forming a promotional mix: the ability to demonstrate or tell potential customers about the benefits of a product, product's safety and the protection of sensitive information (see Product and Place elements), to demonstrate a strong team (People). Also, we have to make great efforts for customers' retention, because we are more interested in long-term subscription cooperation (see Price element). It's also worth noting that we will have limited marketing budgets at launch, so we will need to invest wisely. So key elements of the Promotional Mix are following (according to priority):

- Web site: demonstration of the features and benefits of the product, team, the opportunity to use the application;
- The product will be promoted through speaking slots and sponsorship at exhibitions, conferences, forums for bankers, finance experts, direct mailing, using social networks (.i.e LinkedIn), networking events etc.;
- The product will be presented in a brochure that will be distributed during the above mentioned events and in-person meetings;
- PR - key specialists will speak at profile events, write articles and comment on specialized technical and banking publications
- A 10-slide pitch deck with more details will be created and sent as a follow-up after the first meeting and upon request;
- Targeted digital ads to promote special or limited offers.

People:

Our approach is to build an A-players team. This means that the company will devote a great attention to development and support of the employees to make sure that we hire and develop the best talents.

Top management of the company will be involved in the selling process. The sales managers will have both technical and business experience. On the one hand, it is important that communication will be conducted in a familiar style for the client, but it is also equally important for the employees to be able to answer any questions, including technical, and provide all the clarifications:

- During the first year, the product will be promoted by two business owners that created the product and know it perfectly both from technical and financial point of view;

- After the business grows, two sales representatives will be hired and trained very carefully to convey the essence of the product diligently. They must possess at least basic technical skills to understand how the model can be customized for each bank.

Process:

Considering that the company is a startup, the processes are in its formation stage. Therefore, to build appropriate processes, the feedback from customers will be collected regularly and diligently analyzed.

- The model will be regularly updated (quarterly for the basic and monthly for the premium customers);
- The customers will receive automatic fraud alerts and regular fraud reports delivered to their email and by post to the bank management upon request);
- All subscribed customers will receive 24/7 technical support.

Physical evidence:

- Office will be located in one of Kyiv's largest IT hubs - Unit City;
- The representatives will offer meetings in the places (i.e restaurants) which the bank management typically attends;
- All employees will be encouraged to participate in conferences, forums etc (both financial/banking and technical), write blogs, articles to increase credibility and prove expertise.

Sales strategy

Our sales strategy is to “land and expand”. In the beginning, we attempt to lock the deal and convince the customers to open the account and start business with us, even if it entails the smallest possible model of cooperation. It would allow us to demonstrate the value of our product and its benefits for each customer. As a next step, we will focus on deepening and widening the cooperation through expansion of the services and converting the customers to a more permanent subscription model. We also expect that in times of crisis, the banks will not be ready to spend a lot at once, so such small starting deals will serve as a good anchor for future cooperation. Furthermore, once the economy recovers again, we will already have experience of successful projects thus it will be much easier for banks to agree for a larger package of services.

Since the service is relevant to many functions within the bank (IT, security, finance and risk management, etc.), we anticipate a large number of individuals who may have an impact on the decisions and with whom we will need to communicate to strike a deal. The following groups of banks’ employees can be identified, depending on the needs that may be of interest:

- C-level. They are directly responsible for the financial performance of the company. Typical Job Titles: CEO (Chief Executive Officer), COO (Chief Operating Officer), CFO (Chief Financial Officer), CRO (Chief Risk Officer);
- Risk management leaders. They are directly involved in fraud investigations and who need to improve results (reduce fraud losses). Typical Job Titles: VP/Director/Manager of Credit Risk,
- Payments, Banking Operations, or other functional department, Chief Risk Officer;
- IT leaders. They are responsible for the technological processes in the bank, for which the platform can become another element of process optimization. Typical Job Titles: CIO (Chief
- Information Officer) or CTO (Chief Technology Officer), VP/Director/Manager of Software Engineering or IT Architecture/Infrastructure;
- Innovations leaders. They drive innovations in the company and may be interested in gaining additional competitive advantage for bank customers (usually, it is marketing).

Typical Job Titles: CDO (Chief Digital Officer) or CTO (Chief Transformation Officer), CIO (Chief Innovation Officer)

- Legal, finance, contracts(tender) departments and other

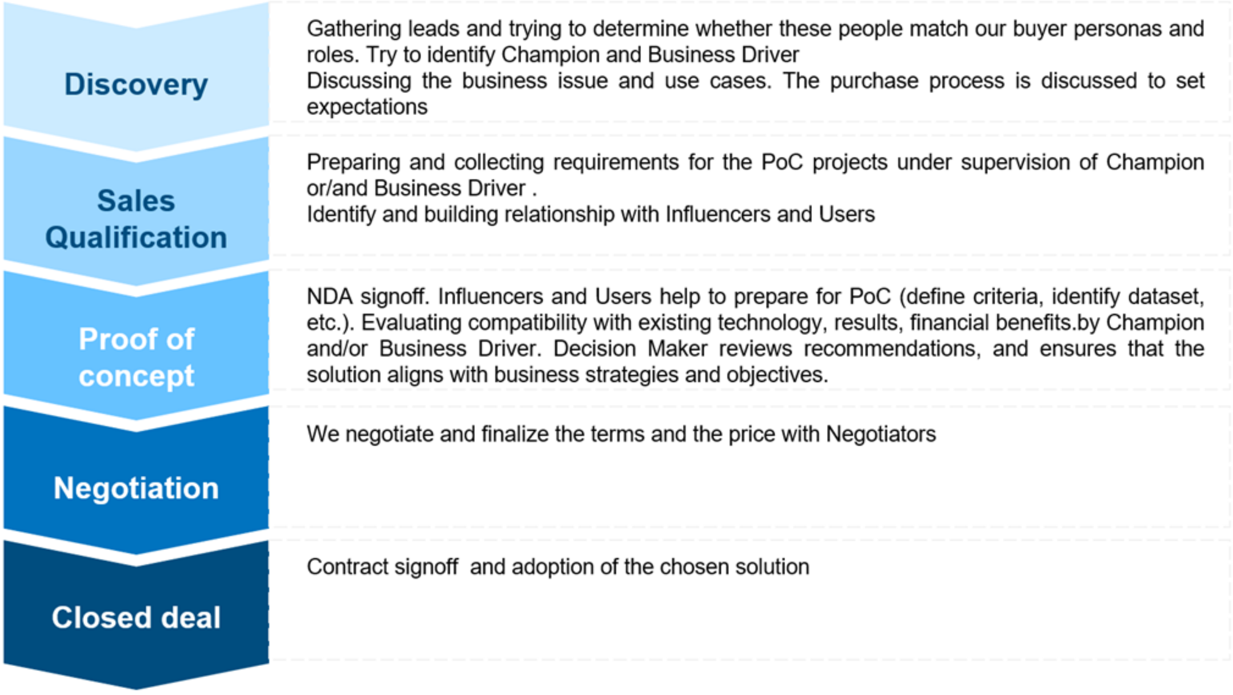
All these positions have different levels of influence upon internal decision making in banks. The same applies even to positions on one level. Therefore, it is important to determine ‘buying’ roles in each case. We define the following roles:

- The Business Driver has the ultimate credibility, organizational power, and necessary resources (budget and people) to ensure that the organization commits to change.
- The Champion is the key advocate for the purchase of the offering who identifies the internal stakeholders whose agreement is necessary to move forward.
- Decision Maker. They may or may not be the sole deciders
- Influencer is a person whose job or perspective may have an impact on the decision to purchase. IT managers are evident influencers.
- Users are individuals or groups whose daily activities are affected by the purchase and subsequent usage of the product. Powerful users can bless or kill an impending deal no matter how much the champion pushes.
- Negotiators - procurement leaders, and legal teams. They can drive prices down, negotiate different terms.

Our sales cycle consists of 5 steps: Discovery, Sales qualification, Proof of concept, Negotiation and Closed deal.

During the first stage of the sales process, it is important to identify people, their roles and needs to make sure that the company has money to purchase our service. Our goal is to find a champion and convince her of the benefits of our solution. This person will be a supporter who will be passionate about the product and facilitate the selling process within the company by identifying detractors and helping to address them, providing information on internal processes, people and persons responsible for certain stages of the deal (we are particularly interested in The Business Driver). Usually, 3-4 meetings are needed to identify the champion.

An important step is the Proof of concept (POC). At this stage, we implement a pilot project on real bank’s data. It will allow us to demonstrate our product and demonstrate business value. Considering that not all banks have sufficient data or good quality of the data, we may face a situation where the model will not perform well due to poor data quality. Banks have billions in turnover, the antifraud process involves the internal resources of the bank, the quality of the prediction depends on data quality, so we cannot be 100% financially responsible for the result. This step will allow us and the Bank to assess whether we can solve the problem and whether the Bank will get expected ROI. If we sell a full package and the bank does not get value, we will not be able to further expand the range of services for this bank. We will just waste time.



Discovery	Gathering leads and trying to determine whether these people match our buyer personas and roles. Try to identify Champion and Business Driver Discussing the business issue and use cases. The purchase process is discussed to set expectations
Sales Qualification	Preparing and collecting requirements for the PoC projects under supervision of Champion or/and Business Driver . Identify and building relationship with Influencers and Users
Proof of concept	NDA signoff. Influencers and Users help to prepare for PoC (define criteria, identify dataset, etc.). Evaluating compatibility with existing technology, results, financial benefits.by Champion and/or Business Driver. Decision Maker reviews recommendations, and ensures that the solution aligns with business strategies and objectives.
Negotiation	We negotiate and finalize the terms and the price with Negotiators
Closed deal	Contract signoff and adoption of the chosen solution

Figure 12. Sales cycle

Sales plan

In the first year, we will work on the quality of our service, so we plan to have only one order for the one-time transaction analysis and fraud prevention report. We expect that this (in addition to an active marketing campaign) will lead to 14 month of subscription purchase for the first year. In the coming years, we will increase the number of the clients. We plan to get 3 clients' accounts each year for a one-time analysis of banks' risks and vulnerabilities per year and get 2-4 new clients for both subscription models. We will focus on selling the subscription packages both as a first-time purchase and through converting the one-time customers to this model, as we plan to generate more revenue from this type of service. We expect that signing an agreement with one customer can take from 3 to 6 months. In particularly difficult cases, the process of obtaining a client can take up to 2 years.

Below is a projection of our sales. Some of the projects in the support will start from the 2-3rd quarter of the year.

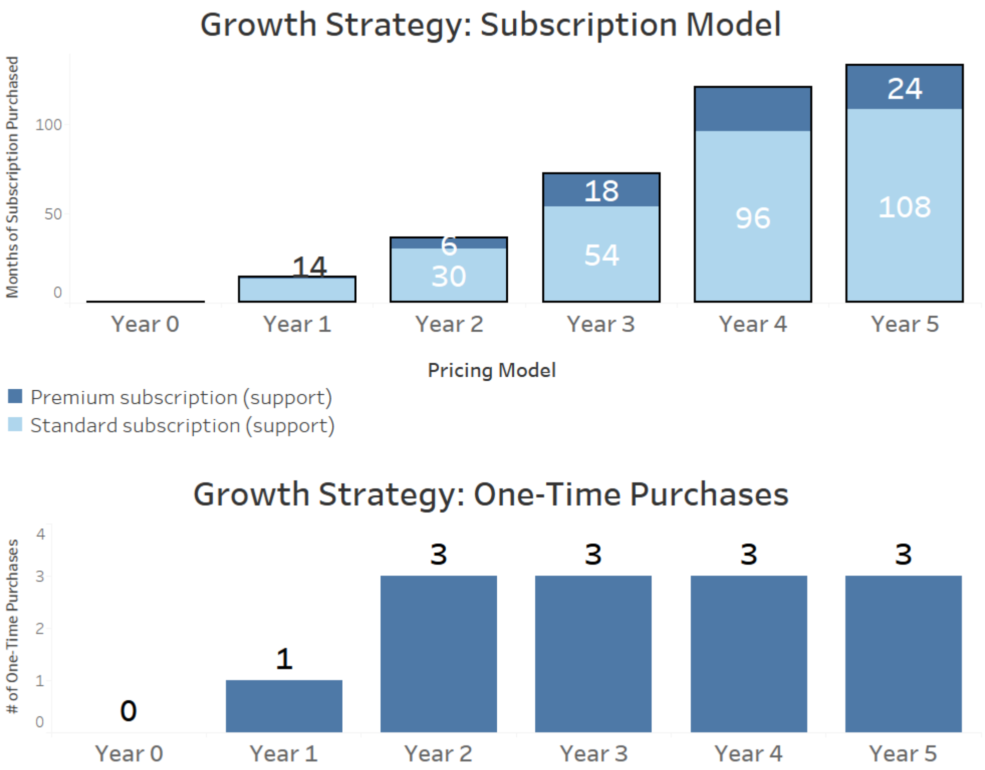


Figure 13. Sales plan for 5 years

Pricing analysis

Current proposals of technological solutions are expensive. For example, it may cost up to 2.2% of turnover, which is unprofitable for most banks. While it makes sense for some companies to pay per transaction, the banks' entire business is transaction-based so it would be more convenient to pay on a timely basis.

Pricing benchmarking with competitors

To estimate the cost for our project model of work, we conducted research that allowed us to identify the range of pricing. The exact price for each customer is formed individually and depends on Customer's requirements, data and needs. Moreover, our business model, in contrast to main competitors, is not a turnkey project. We offer both the product and the support and the latter is the main added value that we provide. Thus, for comparison purposes, we have summed up the cost of developing an analytical report and three months of subscription, which generally equals the cost of 3-5 months of work for this type of projects and used the lower benchmark price for that.

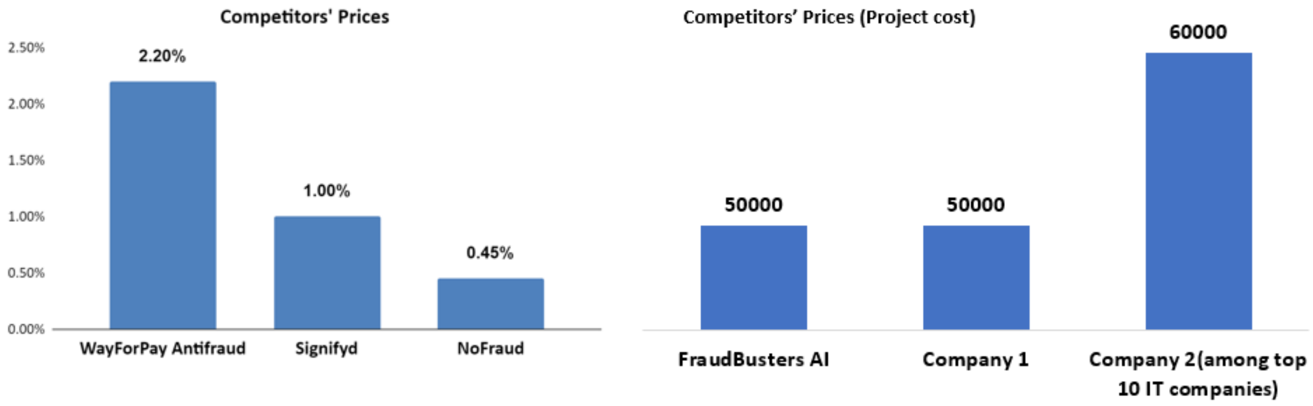


Figure 14. Competitors' Prices

Sales approach

Sales model consists of two components. The first approach is a one-time payment for creation and implementation of an individual model for a single detection and prevention of fraud. The product in this case is a report of analysis of all provided bank's transactions marking the fraud potential, suspicious transaction patterns and model to detect and prevent fraud etc.

The second pricing model is subscription-based. It includes a regular (monthly) payment for technical and analytical ongoing support of the existing model. The model is developed as in the first version, but the analysis is conducted in real time for the entire duration of the purchase. The product is not a one-time report but several, depending on the type of subscription:

Basic:

- Creation and implementation of an individual model to detect and prevent fraud on the basis of bank's transaction data;
- Real-time fraud alerts;
- Monthly fraud prevention reports;
- 24/7 customer support.

Premium

- Basic model +
- Daily analytical reports;
- Quarterly updates of the model (on the basis of additional variables, generated by the model).

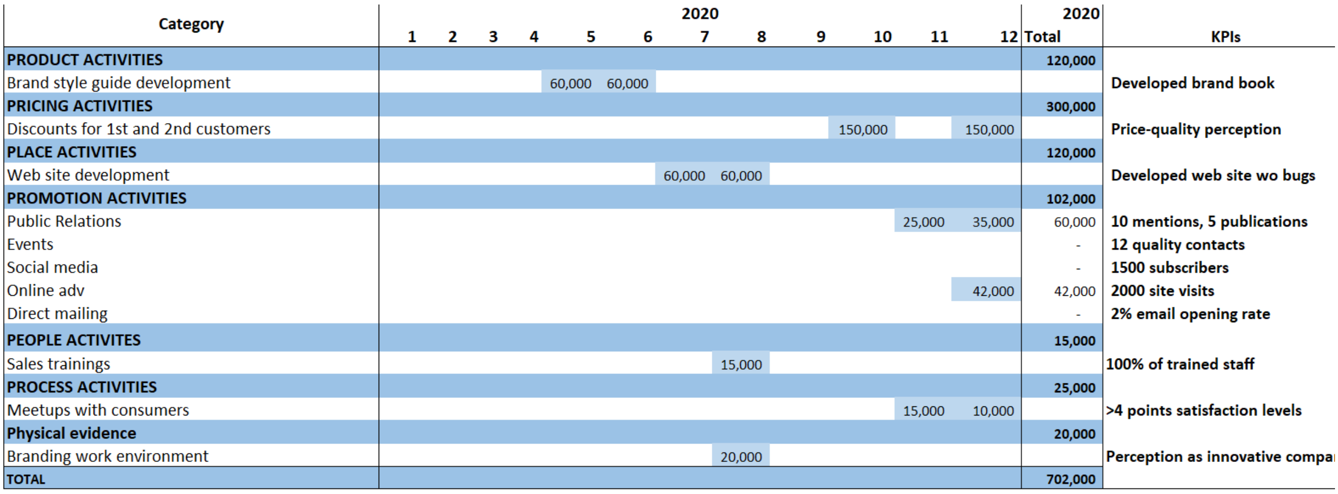
The difference between two subscription models is that the premium package includes more services: daily analytical reports, quarterly updates of the model, generation of additional variables.

The cost of the product is based on two different pricing strategies: market penetration objective for one-time fraud analysis and market skimming for ongoing support. The company will offer low prices for creation and one-time analysis of the bank’s transaction with the purpose to its customer base while the prices for ongoing support will be higher. This diversification is needed to get fast market penetration and receive revenue at the same time. Such a model is viable since the service itself will initially demonstrate the financial benefits of purchase and in the future the customers will be more likely to be willing to pay more for ongoing support.

Cost formation is based on consideration of the required number of hours for the service and the average hourly cost of the specialists involved in the work.

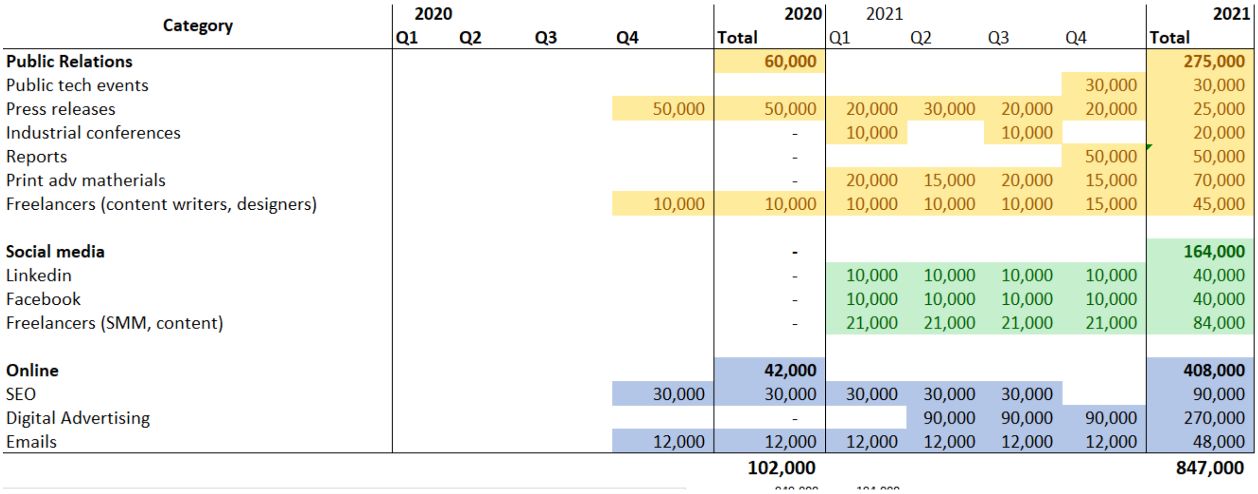
Marketing budget

Since both the company and the product are new, the marketing costs will take a large share of the company’s expenses, but it is needed and a customary practice for new IT companies. In the beginning of the year of launch a relatively small amount will be spent only on logo and brand book development. However, starting from Quarter 4 of the Year 0, the marketing efforts will become more aggressive. We spend most of our budget on discounts for first time Clients in Y0. First contracts are very important to us, we need to get successful cases that can be shown to others. Even though the focus will be made on direct sales, the selling process will be based on a large variety of online materials thus their production and support is expected to be costly. Such products include website, emails, digital advertising, publication on social media (i.e. LinkedIn, Facebook). Additionally, the company will work on building up its reputation of expertise through participation in various specialized events. Marketing budget in this case will be spent on press releases and printed advertising materials (i.e. high-quality brochures, presenting the product). Also, the company will produce regular industry reports (overview of frauds in banking, technologies etc) that will be printed and sent to the banks and financial institutions.



Category							2020						2020	KPIs
	1	2	3	4	5	6	7	8	9	10	11	12	Total	
PRODUCT ACTIVITIES													**120,000**	
Brand style guide development					60,000	60,000								**Developed brand book**
PRICING ACTIVITIES													**300,000**	
Discounts for 1st and 2nd customers										150,000		150,000		**Price-quality perception**
PLACE ACTIVITIES													**120,000**	
Web site development							60,000	60,000						**Developed web site wo bugs**
PROMOTION ACTIVITIES													**102,000**	
Public Relations											25,000	35,000	60,000	**10 mentions, 5 publications**
Events													-	**12 quality contacts**
Social media													-	**1500 subscribers**
Online adv												42,000	42,000	**2000 site visits**
Direct mailing													-	**2% email opening rate**
PEOPLE ACTIVITES													**15,000**	
Sales trainings								15,000						**100% of trained staff**
PROCESS ACTIVITIES													**25,000**	
Meetups with consumers											15,000	10,000		**>4 points satisfaction levels**
Physical evidence													**20,000**	
Branding work environment								20,000						**Perception as innovative compa**
TOTAL													**702,000**	

Figure 15. Marketing plan



Category	2020				2020	2021				2021
	Q1	Q2	Q3	Q4	Total	Q1	Q2	Q3	Q4	Total
Public Relations					**60,000**					**275,000**
Public tech events									30,000	30,000
Press releases				50,000	50,000	20,000	30,000	20,000	20,000	25,000
Industrial conferences					-	10,000		10,000		20,000
Reports					-				50,000	50,000
Print adv matherials					-	20,000	15,000	20,000	15,000	70,000
Freelancers (content writers, designers)				10,000	10,000	10,000	10,000	10,000	15,000	45,000
Social media					**-**					**164,000**
Linkedin					-	10,000	10,000	10,000	10,000	40,000
Facebook					-	10,000	10,000	10,000	10,000	40,000
Freelancers (SMM, content)					-	21,000	21,000	21,000	21,000	84,000
Online					**42,000**					**408,000**
SEO				30,000	30,000	30,000	30,000	30,000		90,000
Digital Advertising					-		90,000	90,000	90,000	270,000
Emails				12,000	12,000	12,000	12,000	12,000	12,000	48,000
					102,000					**847,000**

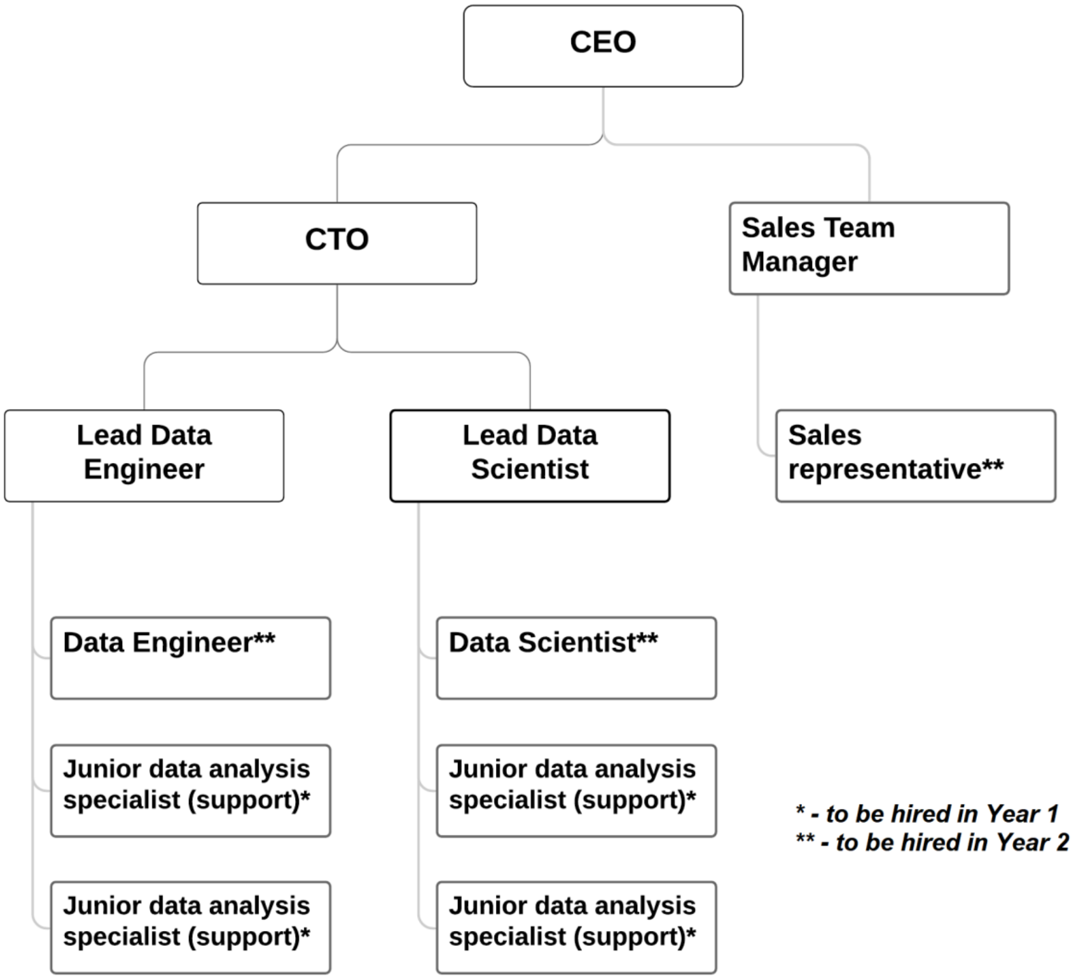
Figure 16. Promo budget projections

ORGANIZATIONAL PLANNING

Corporate management

The company is founded by two highly motivated and technologically experienced founders. Further investment in the team will be made in two main directions. Most resources will go into creation of A level technological team, consisting of four senior data specialists and four juniors, providing 24/7 customer support. Additionally, two sales managers will be hired with the requirement of both business and technological expertise as the product will be sold to banks and financial institutions through direct sales and personal contacts. The company will invest in promotion of its expertise. Its management and technical specialists will be encouraged to publish articles and blogs in technical and business journals, participate in financial/banking and IT conferences and events, preferably as speakers.

Organizational structure (diagram + description)



CEO
CTO
Sales Team Manager
Lead Data Engineer
Lead Data Scientist
Sales representative**
Data Engineer**
Data Scientist**
Junior data analysis specialist (support)*
Junior data analysis specialist (support)*
Junior data analysis specialist (support)*
Junior data analysis specialist (support)*

- to be hired in Year 1
***** - to be hired in Year 2***

Figure 17. FraudBusters AI Organizational Structure

The team of the project currently consists of two people who developed the idea from scratch. The person who created the technology and the prototype for the model will occupy the Chief Technology Officer position and further lead the development of the model. During the operations of the Year 0, two additional technical specialists will be hired - lead data engineer and lead data scientist. The former will be responsible for development of the algorithms of the model, improvement of existing features and creation of new ones etc. Lead data scientist will focus on the analysis part of the pipeline. She will look at the precision and recall scores of the model and seek ways to improve it as well as develop the business reports for the clients, alerts and other products.

Once the company gets its first clients, the technical team will be further expanded during Year 1. Four junior data analysis specialists will be added. They will have support functions, addressing customers' requests and answering questions. The support team will be fixing all minor issues under supervision of the more senior technical specialists.

The next round of expansion of the technical team will take place during Year 2. Two more specialists will be added - data engineer and data scientist. They will work under supervision of respective leads and further develop and enhance the product.

Additionally, from the start of business operations, the team will also hire a sales team manager. The sales manager will work under supervision of the second founder who will become the Chief Executive Officer, responsible for overall strategic management of the company. While the sales will be conducted by two owners at the very beginning, further client management will be done by the sales team. The team will be responsible not only for sales but also for constant communication with clients and building long-term relationships (customer satisfaction, control of project implementation, solving non-technical issues such as document management, etc.). Data analysts are very expensive, so all non-technical parts of the project implementation will be spent by sales managers. We expect them to spend 20-30% of their time on current clients' projects and 70-80% - on sales and new projects. During the Year 2, when the number of clients is expected to increase, an additional sales manager will be hired. Since the company is working on a B2B model, no further expansion of the team is expected within the five years of operations.

FINANCIALS

Since the team will be actively working on sales, it is expected that the company will receive one on-demand model purchase and 14 months of basic subscription model purchase already in Year 1, resulting in forecasted net profit of UAH 4,000,000. The number of customers will increase during the Year 2 and we expect to gain net profit of UAH 11,700,000. Our expected gross profit margin will be quite close to the average profit margin for the industry (Software (System & Application) - 71,37%) - 68% in Years 1, 4, 5 and all the following years. Year 2 and 3 will have a slightly lower gross profit margin of 48% and 57% respectively due to two-stage expansion of the team because of growing number of customers on subscription model. However, the company will quickly recover from the gap in Year 2, demonstrating growth already in Year 3 and returning to 68% margin after that. Projected net profit margin is close to the average by industry (19,54%) in the Year 2 (20%) and Year 3 (22%) and growing significantly to over 30 and then over 40%.

The initial financing of UAH 750,000 will be provided by two founders of the company. In addition, the startup will apply to various funds, startup competitions etc to seek additional UAH 750,000. This money will be used to start the operations, including capital expenditures (laptops for administrative personnel and technical specialists), rent of office and salaries for the team (with the exception of the CEO and CTO) for Year 0. The dividends of 25% will be paid out, starting from Year 2. Since the profit will increase, no additional financing from the investors will be required within the 5-year period. We expect to pay UAH 5.5 mln in dividends to the investors during the four-year period (Year 2 - Year 5) and we offer the following exit strategy: after Year 5 of operations the founders will buy the investors' share of the company.

Purposes of financing

The initial financing of UAH 750,000 will be provided by two founders of the company. In addition, the startup will apply to various funds, startup competitions etc to seek additional UAH 750,000. This money will be used to start the operations, including capital expenditures (laptops for administrative personnel and technical specialists), rent of office and salaries for the team (with the exception of the CEO and CTO) for Year 0.

Since the team will be actively working on sales, it is expected that the company will receive one client that will make the on-demand model purchase to test the effectiveness of the model. Additionally, we expect 14 months of purchase of the basic subscription model by - forecasting 10 months of purchase by one bank and 4 months by another bank closer to the end of the year. As a result, we forecast net profit of UAH 4,000,000 after Year 1. The number of customers will increase during the Year 2 and we expect to gain net profit of UAH 11,700,000.

The dividends of 25% will be paid out, starting from Year 2. Since the profit will increase, no additional financing from the investors will be required within the 5-year period. We expect to pay UAH 5.5 mln in dividends to the investors during the four-year period (Year 2 - Year 5) and we offer the following exit strategy: after Year 5 of operations the founders will buy the investors' share of the company. Another possible strategy of business development would be to accept the offers of purchase of the business by large IT companies that have an antifraud stream. Since the analysis of financials shows that, since the company is quite small, each expansion of operations leads to some decrease in profit margins. While it is followed by recovery, having our business incorporated into a larger entity may smooth such transitions.

Overview of forecasted Capital Expenditures

FraudBusters AI is an IT company thus the only capital expenditures needed are the laptops for the administration purposes and for the technology development. They will be purchased in several stages. During the Year 0 the team will consist of the CEO, CTO, the sales manager and two technical specialists so 3 administrative laptops and 2 PCs for data analysis need to be purchased in the beginning of operations. In the Year 1 we expect to actively work with the first clients thus new hires will be made - 4 junior data analysis specialists that will be both assisting with model improvement and performing support functions. As a result, additional 4 PCs for data analysis have to be purchased. In Year 2 the sales team will be expanded to include an additional sales manager to support existing clients (i.e promote the switch to subscription or from basic to premium plan). The technical team will also be increased to include two more technical specialists, requiring the purchase of one laptop for administrative purposes and 2 PCs for data analysis.

It is expected that the laptops will last for three years until they need to be replaced with the newer and more powerful ones. Thus, in Year 4 five laptops purchased at the start of operations will be replaced, and in Year 5 the laptops bought for hired support specialists will also be replaced.

Capital investment model (CapEx)

	Units	Year 0	Year 1	Year 2	Year 3	Year 4	Year 5
Category 1							
Laptops for administrative personnel	UAH	90,000	0	30,000	0	90,000	0
PC for data analysis	UAH	120,000	240,000	120,000	0	120,000	240,000
Total CapEx	UAH	210,000	240,000	150,000	0	210,000	240,000

Table 5. Capital Expenditures of the FraudBusters AI

Overview of Operating Expenses forecast

Operating expenses will include office rent, marketing activities, sales and performance bonuses for the team, maintenance of the security system, services that will be outsourced (accounting, legal), payments for cloud storage and use for data analysis, stationery and other incidental expenses. It is expected that the total operating expenses for the five years of operations will equal UAH 13,233,800. The most costly item (about 51%) is the marketing however it is not unusual for an IT service company to invest a significant amount of money into raising brand awareness and promoting the product. Another major expense will be the office rent (18%) and sales and performance bonuses (17%). Both are needed to promote the product and are described in detail in the marketing mix. The rest of expenses will comprise 5% of expenses or less.

Operating Expenses (forecast)

Item	**Units**	**OpEX**
Stationery	UAH	73,000
Office rent	UAH	2,430,000
Security system maintenance	UAH	62,500
Marketing	UAH	6,761,500
Accounting outsourced services	UAH	450,000
Legal outsourced services	UAH	753,800
Cloud system	UAH	150,000
Sales & Performance Bonuses	UAH	2,433,000
Other	UAH	120,000
Total	**UAH**	**13,233,800**

Table 6. Operating Expenses of the FraudBusters AI

Overview of Profit and Loss Statement

FraudBusters AI is expected to receive net profit, starting from the Year 1 of operations. Year 0 will involve spending on setup of the business so the only costs will be operational (office rent, salaries of already hired personnel etc).

The profit will be received starting from the Year 1 and net profit margin will be 20% and gradually growing. According to Dr. Damodaran[36], an average profit margin for Software (System & Application) is 71.37%. Our expected gross profit margin will be over quite close to this - 68% in Years 1, 4, 5 and all the following years. Year 2 and 3 will have a slightly lower gross profit margin of 48% and 57% respectively due to two-stage expansion of the team because of growing number of customers on subscription model. However, the company will quickly recover from the gap in Year 2, demonstrating growth already in Year 3 and returning to 68% margin after that. Projected net profit margin is close to the average by industry (19,54%) in the Year 2 (20%) and Year 3 (22%) and growing significantly to over 30 and then over 40%.

PROFIT AND LOSS STATEMENT

All figures are in UAH th

	Year 0	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**
Sales	0	4,000	11,700	23,100	36,300	39,300
Cost of goods sold or service	0	1,269	6,437	9,901	11,712	12,751
Gross profit	**0**	**2,731**	**5,263**	**13,199**	**24,588**	**26,549**
Selling, general and administrative expenses	463	1,653	1,899	2,683	3,298	3,701
Operating profit	**-463**	**1,078**	**3,364**	**10,516**	**21,291**	**22,848**
Operating profit margin	*0%*	*27%*	*29%*	*46%*	*59%*	*58%*
Depreciation	**0**	**70**	**150**	**200**	**130**	**120**
EBIT	**-463**	**1,008**	**3,214**	**10,316**	**21,161**	**22,728**
EBIT margin		*25%*	*27%*	*45%*	*58%*	*58%*
Interest rate	0	0	0	0	0	0
EBT	**-463**	**1,008**	**3,214**	**10,316**	**21,161**	**22,728**
EBT margin		25%	27%	45%	58%	58%
	20%	*20%*	20%	20%	20%	20%
Taxes	0	202	643	2,063	4,232	4,546
Net income	**-463**	**807**	**2,571**	**8,253**	**16,929**	**18,182**
Net Income margin		*20%*	*22%*	*36%*	*47%*	*46%*

Table 7. Profit and Loss Statement for the FraudBusters AI

Overview of forecasted Balance Sheet

The company will finance its activities by UAH 750,000 of equity provided by two founders equally. The same amount of money will be obtained through venture funds, business angels, startup

[36] Damodaran, Aswath. 2020. "Margins by Sector (US)." Damodaran Online. January 2020. http://pages.stern.nyu.edu/~adamodar/New_Home_Page/datafile/margin.html.

competition etc (the founders will seek financing actively throughout year 0). Since the business will bring profit starting from Year 1, no additional funding is required.

Since it is difficult to obtain a loan from the bank and the loans are expensive, the decision was made not to use this form of financing the business activities. Thus, the company will not have any short-term liabilities.

The dividends will be paid out starting from the Year 2. Estimated amount of dividends paid per year is 25% of net income. Half of the dividends will be paid to the founders that contributed the capital and half of the sum will go to the investors (approximately 5.5 UAH mln).

BALANCE SHEET						
All figures are in UAH th						
	Year 0	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**
ASSETS						
Current assets						
Cash & Cash Equivalents	828	1,464	3,393	9,782	22,399	35,916
Accounts Receivable	0	0	0	0	0	0
Inventory	0	0	0	0	0	0
Prepaid expenses	0	0	0	0	0	0
Total current assets	**828**	**1,464**	**3,393**	**9,782**	**22,399**	**35,916**
Fixed assets (non-current assets)						
Gross PPE	210	450	600	600	600	600
- cumulative depreciation	0	70	220	420	340	220
Net Fixed Assets	**210**	**380**	**380**	**180**	**260**	**380**
TOTAL ASSETS	**1,038**	**1,844**	**3,773**	**9,962**	**22,659**	**36,296**
LIABILITIES						
Accounts payable	0	0	0	0	0	0
Short-term-liabilities	0	0	0	0	0	0
Credit	0	0	0	0	0	0
TOTAL LIABILITIES	**0**	**0**	**0**	**0**	**0**	**0**
SHAREHOLDER'S EQUITY						
Contributed capital	1,500	1,500	1,500	1,500	1,500	1,500
Retained Earnings	-463	344	2,273	8,462	21,159	34,796
TOTAL SHAREHOLDER'S EQUITY	**1,038**	**1,844**	**3,773**	**9,962**	**22,659**	**36,296**
TOTAL LIABILITIES AND SHAREHOLDERS' EQUITY	**1,038**	**1,844**	**3,773**	**9,962**	**22,659**	**36,296**

Table 8. FraudBusters AI Balance Sheet

Overview of forecasted Cashflow Statement

The company will have cash inflow from financing activities only in the Year 0 when the contributed capital is acquired. Starting from Year 2 the financing activities will have cash outflow as the dividends will be paid to the investors and founders of the company. It signifies that the company will generate enough cash from operating activities to finance its own activities without the need to attract additional contributed capital or make long or short-term liabilities.

Since the capital investments will be made in the laptops which depreciate quite rapidly due to constant technological innovations, the investing activities will form some cash outflow but it will be spread rather evenly over the first five years of operations.

CASHFLOW STATEMENT

All figures are in UAH th

	Year 0	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**
Net Income	-463	807	2,571	8,253	16,929	18,182
Depreciation	0	70	150	200	130	120
=+ or - changes in AR	0	0	0	0	0	0
=+ or - changes in AP	0	0	0	0	0	0
Cashflow from Operating Activities	**-463**	**877**	**2,721**	**8,453**	**17,059**	**18,302**
Capital Investments (CapEx)	210	240	150	0	210	240
Return (dividends) from investments made	0	0	0	0	0	0
Cashflow from Investing activities	**210**	**240**	**150**	**0**	**210**	**240**
Credits from commercial banks	0	0	0	0	0	0
Repayment of credits to commercial banks	0	0	0	0	0	0
Proceeds from IPO	0	0	0	0	0	0
Equity financing from the founders/investors	1,500	0	0	0	0	0
Dividends to the shareholders	0	0	643	2,063	4,232	4,564
Cashflow from Financing Activities	1,500	0	-643	-2,063	-4,232	-4,564
Total Cashflow	**828**	**637**	**1,929**	**6,390**	**12,616**	**13,517**
Cash at the beginning of the period	0	828	1,464	3,393	9,782	22,399
Cash at the end of the period	**828**	**1,464**	**3,393**	**9,782**	**22,399**	**35,916**

Table 9. FraudBusters AI Cashflow Statement

SUPPLEMENTS

List Of Tables

List Of Images

References

Bugriy, Maksym. “The Difficult Path to the Security Reform.” *The Ukrainian Week*, June 2, 2012. https://ukrainianweek.com/Security/51920.

Business Dictionary. 2011. “What Is Financial Transaction? Definition and Meaning.” BusinessDictionary.Com. January 28, 2011. http://www.businessdictionary.com/definition/financial-transaction.html.

Damodaran, Aswath. 2020. “Margins by Sector (US).” Damodaran Online. January 2020. http://pages.stern.nyu.edu/~adamodar/New_Home_Page/datafile/margin.html.

Deloitte Legal. “Blockchain WP March 2018_.Pdf,” March 2018. https://www2.deloitte.com/content/dam/Deloitte/sv/Documents/legal/Blockchain%20WP%20March%202018_.pdf.

Denovo. “Digital Transformation of Ukraine Vision 2025,” 2019. https://businessviews.com.ua/ru/digital-transformation-2019/.

Exactech. 2010. “Fraud Prevention.” May 17, 2010. https://www.exactech.co/fraud-prevention/.

Frankenfield, Jake. 2018. “Machine Learning.” Investopedia. March 6, 2018. https://www.investopedia.com/terms/m/machine-learning.asp.

Gilbert, Nestor. “10 Fintech Trends for 2020: Top Predictions According to Experts,” October 16, 2019. https://financesonline.com/fintech-trends/#AI.

HSN Consultants, Inc. “The Nilson Report – Card Fraud Losses Reach $27.85 Billion,” November 2019. https://nilsonreport.com/mention/407/1link/.

INTERPOL. “INTERPOL Warns of Financial Fraud Linked to COVID-19,” March 13, 2020. https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-warns-of-financial-fraud-linked-to-COVID-19.

Investopedia. 2017. “Banking Fraud.” Investopedia. March 26, 2017. https://www.investopedia.com/banking-fraud-4689709.

JPMorgan Chase. “Redefining the Financial Services Industry: JPMorgan Chase 2016 Annual Report,” 2016. https://www.jpmorganchase.com/corporate/investor-relations/document/ar2016-lettertoshareholders.pdf.

KPMG. “Global Banking Fraud Survey,” May 2019, 24.

Mastercard. “Card Issuers Safety & Security,” May 27, 2015. https://www.mastercard.us/en-us/issuers/safety-security.html; Visa. “Visa’s Zero Liability Policy,” March 7, 2020. https://usa.visa.com/pay-with-visa/visa-chip-technology-consumers/zero-liability-policy.html.

Merriam-Webster. 2020. “Definition of FRAUD.” 2020. https://www.merriam-webster.com/dictionary/fraud.

Microsoft Corporation. “Banking on AI,” 2018. http://info.microsoft.com/rs/157-GQE-382/images/EN-CNTNT-eBook-BankingonAI.pdf.

Minastireanu, Elena-Adriana, and Gabriela Mesnita. “An Analysis of the Most Used Machine Learning Algorithms for Online Fraud Detection.” *Informatica Economica* 23, no. 1/2019 (March 30, 2019): 5–16. https://doi.org/10.12948/issn14531305/23.1.2019.01.

NUData Security MasterCard. “2019: Fraud Risk at a Glance: Nudata Analysts’ Interpretation of Real-Life Attacks,” November 1, 2019. https://gallery.mailchimp.com/bf4a530dc0b5fbce4de4af60e/files/dc639831-4129-481b-8bc0-bc22e859f6a1/2019_Fraud_Risk_at_a_Glance_Report.pdf?_ga=2.253653833.1932551783.1576604990-419311239.1569444503.

PWC. “PWC’s Global Economic Crime and Fraud Survey 2020,” 2020, 14.

Surane, Jennifer, Olivia Rockeman, and Robert Schmidt. “Fear of Virus-Tainted Dollars Opens New Front in War on Cash.” *Bloomberg.Com*, March 11, 2020. https://www.bloomberg.com/news/articles/2020-03-11/fear-of-virus-tainted-dollars-opens-new-front-in-war-on-cash.

Wilder, Mason. “Brave New World: Can Biometric Security Help Fight Fraud?,” April 22, 2019. https://www.acfe.com/fraud-examiner.aspx?id=4295005744.

Бублик, Євген, and Юлія Шаповал. “Відновлення довіри до банків — завдання НБУ.” *DT.Ua*, 2019. https://dt.ua/finances/vidnovlennya-doviri-do-bankiv-zavdannya-nbu-302948_.html.

Дыдышко, Виталий. “Как Искусственный Интеллект Меняет Работу Крупного Украинского Банка. Интервью - Новости Технологий Украины и Мира.” LIGA.net, 13 грудня 2019. https://tech.liga.net/technology/interview/iskusstvennyy-intellekt-v-alfa-bank-ukraina-kak-mashiny-i-lyudi-razdelyat-obyazannosti.

Кулеш, Сергей. “Интеллектуальная Антифрод-Система ПриватБанка Предотвратила 99% Мошеннических Операций в Электронных Сервисах Банка в Прошлом Году.” ITC.ua, 3 жовтня 2017. https://itc.ua/nes/intellektualnaya-antifrod-sistema-privatbanka-predotvratila-99-moshennicheskih-operatsiy-v-elektronnyih-servisah-banka-v-proshlom-godu/.

Національний банк України. “Огляд банківського сектору,” 2020.

Національний банк України. “У 2020 році стрес-тестування проходитимуть 16 банків,” 2020. https://bank.gov.ua/news/all/u-2020-rotsi-stres-testuvannya-prohoditimut-16-bankiv.

Прес-служба Мінекономіки. “Міністерство розвитку економіки, торгівлі та сільського господарства України -> Новини -> Уряд уточнив макропрогноз на 2020 рік,” 30 березня 2020. https://www.me.gov.ua/News/Detail?lang=uk-UA&id=671cbaf4-7b1c-4ec5-a4af-10a852bc5a3e&title=UriadUtochnivMakroprognozNa2020-Rik.

Руденко, Виктория. “Мошенники лишают денег доверчивых украинцев - Финансовый клуб,” 2019. https://finclub.net/analytics/moshenniki-lishayut-deneg-doverchivykh-ukraintsev.html.

Шевчук, Сергей. “ПриватБанк: работа на Карантине, суды с Коломойским и кредитные каникулы. Интервью,” 30 березня 2020. https://finance.liga.net/bank/interview/privatbank-rabota-na-karantine-sudy-s-kolomoyskim-i-kreditnye-kanikuly-intervyu.