Title Page

**A Business Plan for Health Insurers: How to Tackle Fraud & Insurance Claims with Technology**

by

**Deborah Wokpetah**

BME, City University of New York, 2017

Submitted to the Graduate Faculty of the

Department of Health Policy and Management

Graduate School of Public Health in partial fulfillment

of the requirements for the degree of

Master of Health Administration

University of Pittsburgh

2020

Committee Page

UNIVERSITY OF PITTSBURGH

Graduate School of Public Health

This essay is submitted

by

**Deborah Wokpetah**

on

April 20, 2020

and approved by

**Essay Advisor:** Kevin Broom, PhD/MBA, Associate Professor, Health Policy and Management Graduate School of Public Health, University of Pittsburgh

Tom Davis, MBA, Clinical Assistant Professor, Joseph M. Katz Graduate School of Business, University of Pittsburgh

Copyright © by **Deborah Wokpetah**

2020

**Abstract**

Kevin Broom, PhD/MBA

**A Business Plan for Health Insurers: How to Tackle Fraud & Insurance Claims with Technology**

Deborah Wokpetah, MHA

University of Pittsburgh, 2020

**Abstract**

Health insurance fraud has presented itself to be a challenge in the healthcare industry. The reality is that health insurance fraud can take different forms - from billing for services that were not rendered to patients, to kickbacks, bribery and overutilization of services. On average, there are at least $68-$300 billion in annual damages due to fraudulent health insurance claims in the United States. This accounts for nearly 10% of the income of the national health care industry – money that can be redirected towards creating public health programs to address issues of healthcare. The fundamental problem for health insurers dealing with fraud is their inability to design an effective and efficient mechanism with their current systems at a low cost.

The goal of this paper is to outline a plan for health insurers to conduct in depth analyses of possible fraud and to create warning systems to alert to potential abuses in billing and claims systems. Current solutions on the market are complex, expensive and require long term contracts – limiting such solutions to mainly large health care organizations that seek to make drastic changes in their bottom line. This business plan outlines health insurance fraud prediction and detection methods using big data and artificial intelligence technologies to help insurers from losing money to fraudulent claims and to drive business performance.

Table of Contents

[Preface viii](#_Toc49334579)

[1.0 Executive Summary 1](#_Toc49334580)

[1.1 Business Objectives 1](#_Toc49334581)

[1.2 Mission Statement 2](#_Toc49334582)

[1.3 Guiding Principles and Keys to Success 2](#_Toc49334583)

[2.0 Products and Services 3](#_Toc49334584)

[2.1 Key Features 3](#_Toc49334585)

[2.2 Specific Services Descriptions 4](#_Toc49334586)

[3.0 Market Analysis 7](#_Toc49334587)

[3.1 Industry Analysis 7](#_Toc49334588)

[3.2 Market Size, Trends, Needs and Growth 8](#_Toc49334589)

[3.3 Main Competitors 9](#_Toc49334590)

[4.0 Marketing Strategy and Implementation 11](#_Toc49334591)

[4.1 SWOT Analysis 11](#_Toc49334592)

[Strengths 11](#_Toc49334593)

[Weaknesses 12](#_Toc49334594)

[Opportunities 12](#_Toc49334595)

[Threats 13](#_Toc49334596)

[4.2 Marketing Strategy and Positioning 13](#_Toc49334597)

[4.3 Sales Strategy 14](#_Toc49334598)

[5.0 Financial Plan 16](#_Toc49334599)

[5.1 Essential Assumptions 16](#_Toc49334600)

[5.2 Client Pricing Plans and Pricing Structure 17](#_Toc49334601)

[5.3 Client Benefits 18](#_Toc49334602)

[5.4 Pro Forma 19](#_Toc49334603)

[6.0 Implementation 23](#_Toc49334604)

[6.1 Implementation Strategy 23](#_Toc49334605)

[7.0 Summary 25](#_Toc49334606)

[8.0 Conclusion 26](#_Toc49334607)

[Appendix A Satellite Map of Business Location in Nova Place, Pittsburgh, PA 27](#_Toc49334608)

[Appendix B Organizational Structure of the Business 28](#_Toc49334609)

[Bibliography 29](#_Toc49334610)

List of Tables

**Table 1:Summary of Hiring Costs……………………………………………………………. 17**

**Table 2: Sample Cost savings for Prime Healthcare Services Inc…..……………………… 18**

**Table 3: Income Statement…………………………………………………………………… 20**

**Table 4: Statement of Cash Flows……...…………………………………………………….. 21**

**Table 5: Balance Sheet………………………………………………………………………… 22**

**Table 6: Implementation Timeline…………………………………………………………… 24**

# Preface

I would like to thank my essay advisor, Dr. Kevin Broom, PhD/MBA, and my essay reader, Tom Davis, MBA/Clinical Assistant Professor for their time. Without their expertise, direction and patience, this essay would not exist. I would also like to thank my residency preceptor, Patrick Tracy (Director of UPMC CHIP program) and my internship manager Judy Johnson (Vice President of Aspirant), for the knowledge you instilled in me was phenomenal.

Lastly, I would be remiss if I did not acknowledge the Almighty God, the support of my family and my boyfriend for whom I am always grateful for. Thank you all.

# Executive Summary

## Business Objectives

This business plan aims to discuss the creation of a private company dedicated to implementing proprietary and existing technology-based insurance fraud detection and prevention technologies, while offering advanced consulting services to health insurers. Currently, in the United States alone, insurance fraud costs insurers as much as $300 billion per year in false and fraudulent claims, stemming not only from individual cases of fraud but also from organized crime specialized in this type of activity (NHCAA, 2018).

This proposal offers customized solutions for insurers based on powerful proprietary software modeling, which is used in tandem with existing tools in fraud prevention to conduct in-depth analyses of any health insurance company’s claims system and user profiles. This permits health insurers to not only detect cases of possible fraud by individuals or non-provider organizations, but also sets up warning systems that alert to the possibilities of potential abuses in billing and claims systems by health care providers that may be using illegal billing procedures to their benefits. Through Big Data algorithms and databases, fast and accurate alerts regarding suspicious or unusual behavior can be developed. Third party security risk assessment, in conjunction with data encryption will prevent sensitive insurer and client data from being stolen and used for illegal and fraudulent purposes.

## Mission Statement

The primary mission of this business plan is to save health insurers money that stems from fraudulent claims and provider activities while keeping costs down. This will be done by ethically and efficiently conducting anti-fraud consultancy for health insurers, following all pertinent legal parameters regarding user privacy, data collection, and information use. This business proposal is inextricably tied to the principles of fairness and integrity in the realm of health care. The business will be based in North Shore Pittsburgh, in the Nova Place business building as shown in Appendix A.

## Guiding Principles and Keys to Success

In addition to ethical principles that involve a fair and legal use of user and insurer data, this business will employ the latest security measures to protect the information of insurers. Furthermore, it is guided by the idea of fairness, integrity, and a commitment to continual research and development to ensure the use of effective and comprehensive technologies in the pursuit of preventing insurance fraud.  The keys to success for this business proposal are as follows:

* Commitment to both integrity and efficiency
* An untiring pursuit of the best methods and technologies for fraud detection, always seeking for cutting-edge approach
* Developing proprietary processes that give firms an advantage when doing data analysis
* A comprehensive strategy in fraud prevention that incorporates security as an important tenet

# Products and Services

## Key Features

The core services of this business proposal are advanced analytics applications to specific health insurer data environments. An on-site initial comprehensive assessment is recommended to consider the size of the insurer. This initial comprehensive assessment will include the following key features:

1. An assessment of known fraud impact: Past cases of fraud, if it exists within the organization, will be collected and analyzed in order to build a profile of known instances of fraud.
2. Data size and security assessment: At this stage, an analysis of the insurer’s data – from personal profiles and data to information on payments, third parties, claims and other pertinent data – will be conducted to draw conclusions on the specific needs of the insurer.
3. Design of fraud data monitoring alert system: An individualized plan to monitor the insurer’s data and claims structure will be designed to score and prioritize fraud alerts before being reviewed by internal analysts.
4. Implementation of advanced monitoring: Once a specific application has been designed to meet the needs of the insurer, specific cases, clients or providers will be flagged for manual anti-fraud revision. This monitoring will permit certain accounts or transactions to be profiled for future algorithm building and will feature a color-coded risk status for different individuals, organizations, or accounts. This will permit analysts of insurers to keep track of the riskiest accounts and quickly assess potential cases of abuse or fraudulent claims in the future.
5. Comprehensive security risk assessment: According to Accenture (2017), at least 25% of US consumers have had their health insurance data stolen by hackers and interested parties. Among other things, this information will be used to create a fraudulent claims case management to analyze the relationship between third parties and stolen individual policy holder information. A security risk assessment will allow insurers to take note of current risks and undergo immediate steps to reduce them to the highest possible degree.
6. Additional consulting services: In addition to individualized proprietary software, established data analysis techniques, combined with the latest research and technology related to fraud detection, will be utilized in order to advise insurers on best practices in security and prevention.

## Specific Services Descriptions

1. **Risk Analysis Profiles**: This specific service entails the creation of user profiles for individual and group policy holders of insurers. The user profiles are built upon machine-learning algorithms that collect, organize, and evaluate data on individual and group policy holders in order to create different profile types. Subsequent policy holders from those related to claims to simple elements such as updating or changing policy holder information will be given specific weights and values with the end goal of creating a profile score for the policy holders. Industry and company data of known fraudulent cases will also be tabulated and profiled for machine learning purposes; known cases from the past will be used to program the algorithms to recognize old patterns and update them when new ones are identified. This system will be used to create scores and alert to when policy holder profiles need attention from fraud prevention analysts.
2. **Transaction Risk Profiling**: Transaction risk profiling of insurers is just as critical. This allows careful tracking of income and outflow of cash, especially with respect to payouts and filed claims. Following the money is an important element of detecting fraud, and as such, transaction profiling, informed by algorithms will be used for further machine learning and can give another element of protection to insurers. Even if an individual policy holder is not profiled, a transaction that meets specific criteria can be flagged by the risk profiling algorithm, can be examined carefully by fraud prevention analyst experts.
3. **Insurance Fraud Algorithms and Machine Learning**: In both above cases, proprietary fraud detection algorithms will be based on known information related to health insurance fraud. This information will be transformed into predictive learning technology that will additionally be able to detect and define possible new patterns that indicate fraudulent activity. Insurers can continually test these against control simulations in order to validate its effectiveness; thereby equipping themselves the necessary knowledge to be sustainable moving forward.
4. **Leading-Edge Database Technology**: The fastest and most powerful relational and non-relational database technologies will give the broadest scope and most potential to conduct analysis over extremely complex and vast amounts of data. One example is using MongoDB - a non-relational database structure with the data science integration platform Apache Spark to provide parallelized queries across data fields. Currently, some companies, such as FICO (Holzhauer, 2018), utilize MongoDB in a fraud prevention framework related to protecting credit score fraud.
5. **Harnessing the Power of the Blockchain**: Blockchain technology will be utilized for two primary datasets, that of policy holder information and that of transactions conducted within the scope of claims and payouts. The former will provide an accurate and bulletproof methodology of making it difficult for fraud perpetrators to appropriate or compromise information. Such technology is currently being used by numerous companies in similar fraud prevention applications, such as IBM (Mauri, 2017).
6. **Customized, Bespoke Front-End:** While the technology is proven and effective, a customized front-end will make all complex operations understandable. Graphs, charts, and a usable and intuitive interface will be implemented so that the fraud prevention framework can produce meaningful formats for analysts who will depend on it in the future.

# Market Analysis

## Industry Analysis

According to the National Health Care Anti-Fraud Association (NHCAA, 2018), there are at least $68-$300 billion in annual damages due to fraudulent health insurance claims in the United States alone, which totals to almost 10% of the income of the national health care industry. Some estimates are even higher, and they are not limited to private insurance companies, but also impact public health systems. The United States General Accounting Office (GAO, 2018), the Congressionally chartered accountability office for the monitoring of public spending, estimates that in FY 2017, there was at least $52 billion in fraudulent claims made only to Medicare, the state-supported health insurance system.

These costs represent an enormous burden to both private and public health insurers. These fraudulent claims are not only costly to insurers, but also eventually harm consumers, as insurers are forced to raise premiums to cover unnecessary and ultimately false insurance claims. As a result, the fraud prevention industry is working diligently to find effective solutions to save immense amounts of time, money, and effort in the hopes of making insurers’ operational costs lower and eventually passing savings on to consumers and institutional partners. The rapid growth of Big Data technology is fueling the growth of companies and products dedicated to stopping the proliferation of health care and insurance fraud.

Currently, several technologies are being implemented by fraud prevention companies and consultants to this end. Some examples include (Culp, 2014):

* **Predictive modeling**. This process entails the use of analytics that study historically documented fraud instances, captures and expresses their patterns in algorithmic language, and then applies them to current operations in order to flag possible fraud cases.
* **Business rules.** This strategy entails the knowledgeable definition of certain scenarios or rules that could indicate possible fraudulent behaviors globally during various stages of claims processing.
* **Network Analysis.** This method examines the multitude of relations amongst stakeholders and parties that can indicate unusual or suspicious links. When shared across different industry data, this becomes a valuable tool for identifying associations with potentially fraudulent intentions or tendencies. Such measures are being implemented by the companies themselves, as well as public institutions such as CMS (Centers for Medicare and Medicaid Services), though as of now, there are few singular products that stand out in terms of giving such organizations the necessary tools for fraud prevention. According to the GAO (2018), the case of Medicare shows that the organization still relies on relatively simple data analysis and traditional law enforcement investigation to detect and prosecute fraud instances.

## Market Size, Trends, Needs and Growth

The United States health insurance market currently represents an industry worth over $1 trillion, with some 2.3% annualized market growth between 2015 and 2020 and a projected growth rate of 1% for FY 2020 (IbisWorld, 2020). According to IbisWorld (2020), this market is constituted by over 6300 health insurance companies that employ over 600,000 people in this continually growing segment. According to the US Census Bureau (2018), over 91.2% of Americans have health insurance, as such the market in the US alone is considerably immense.

While the current growth rate of the market has been analyzed at 2.3% and projected at 1% for 2020 (IbisWorld, 2020), the matter of the global health insurance market presents additional opportunities. According to Allied Market Research (2019), the global health insurance industry is valued at over $3.153 trillion and will reach $4.475 trillion by 2026, which constitutes a remarkable 4.4% compound annual growth rate (CAGR) in the next six years. This expansion of the global health market will possibly result in a growth in certain services and needs for the industry, not only in terms of direct client-provider services, but also in fraud assessment, recovery, and prevention services. The increasing digitalization of the industry, in general, presents an excellent opportunity to adapt global software products for use in diverse markets and locations.

## Main Competitors

Some companies are actively pursuing data analysis and related applications to curtail medical fraud. One example is the data analysis company SAS, who offers a comprehensive data analysis solution for the purposes of fraud detection and prevention (SAS, 2020). Among other features, their offer includes cross-analysis of insurer data with that of user network information, including social media activity. In addition to fraud data management, they offer detection and alerts, social network analysis, manual search features, case management, and deployment options that include both full hosting options as well as partial hosting (SAS, 2020). SAS has a variable pricing structure and as such does not publish prices on their web pages; however, they do provide a general idea of pricing. They stipulate specific requirements, such as a minimum of 10 employees, 2-3 years in business (minimum), an agreement of at least $10,000 in total spending, and credit approval.

Other companies focus on health care insurance fraud prevention from a security standpoint. One example is Alpine Security, an SAS competitor that focuses on advanced analytics in detecting possible security risks and finding adequate solutions to minimize them. Their focus in marketing their services has been in highlighting several significant breaches in the last 6 years in which over 109 million Americans have had their sensitive data stolen from health insurance computers due to malicious activity (Espinosa, 2018). While Alpine Security pitches directly to health insurance providers, their service is not necessarily specific to the industry, nor does it incorporate global anti-fraud measures. In addition, their main avenue of business is cyber security assessment and risk reduction in general.

A third example involves a consulting company, Accenture, using a variety of techniques, including partnerships, to offer global health insurance fraud prevention and detection services. Currently, Accenture offers its own risk analytics suite, proprietary data, risk, and insights models, claims fraud analytics, and enterprise-wide fraud detection and management as services to health insurance companies and related industries. Their services claim to screen all claims procedures, product purchase procedures, transaction risk scoring, and logic-driven alerts for specific behaviors and activities in real time. Accenture also offers cross-comparisons and screening using their proprietary Social Analytics Screening, which purportedly will use publicly available social media information and profiles as sources for information to contrast with claimant-provided information.

# Marketing Strategy and Implementation

## SWOT Analysis

A SWOT (Strengths, Weakness, Opportunities & Threats) Analysis allows for a realistic overview of the various facets in favor of and against the business model in order to make planning more solid. The main threats and risks involve factors outside of the control of the business proposal, including regulatory issues and general external factors. On the other hand, there are numerous advantages to the positioning and design of this business including the relative nascence of this particular sector, which provides numerous opportunities to create a market niche and consolidate clients within the larger panorama of the insurance fraud prevention area.

### Strengths

One of the key strengths of this business plan is the fact that transparent pricing will be offered to smaller and medium tier insurers, which will make great inroads with companies seeking to try the service, enticed by minimal risk, low to no-commitment requirements, and the promise of saving money. This latter aspect, economic benefits, is another key strength of this business plan, which will offer immediate and measurable savings and subsequent value. A planned emphasis on research and development will be another key strength, as will implementing models and methods that are constantly renovated and improved.

### Weaknesses

Among the primary weaknesses of the business model is related to the quickly changing nature of fraud implementation; with fraud being a problem as old as business itself, it constantly evolves and adapts to security measures. This presents specific challenges to the business model. Client retention is another possible weakness; if clients do not see tangible, measurable results, they could discontinue the service. For this reason, it will be important to create visible reporting so that clients are aware of the savings of time, money, and reputation.

### Opportunities

One of the primary opportunities of this business model is the fact that the market for the specific product offering is relatively new and the competition so far is relatively undeveloped. This translates to the fact that the services offered stand out more easily and cater to a market need that is underserved. Furthermore, as the population ages, insurance claims might become a major source of fraud prevention efforts. As the market analysis has demonstrated, the industry is projected to continue to grow significantly in coming years. There is also a significant opportunity to branch into other types of insurance fraud prevention services, for example homeowners insurance, car insurance, life insurance, and other big-ticket insurance types where this business plan can be applied. Considering that the same algorithms will be valid across insurance industries with only minor modifications to structure and interface, this represents a massive opportunity of growth.

### Threats

One of the major threats to the business is hacking and other types of black hat activities that could compromise the security of the algorithms used, as well as sensitive customer data. The current state of computer security has demonstrated that even the latest security systems can be breached, and these breaches can produce great negative impacts to a company’s image and revenue. Third party risk management when it comes to data security will be performed continuously. First, data encryption will be performed and verified for all vendors – including data stored on laptops, hard drives, databases, servers, etc. Next, role-based access to information and information systems will be enforced on a daily basis. This means that access to client data will be provided to users who need the information to perform their job. There will also be the implementation of a disaster recovery program which will include ways to restore client data in the case of a disaster.

Another external threat is related to market regulation and legal changes to aspects that affect the business, such as consumer and data privacy. Changes in public policy regarding how data is screened and handled could produce costly effects on the business model and operations.

## Marketing Strategy and Positioning

The marketing strategy will be primarily based on a clear and well-referenced and structured website that will state the services and be directed at the target market. Digital marketing will be used to develop partnerships with advertising providers such as AdWords and Media.net in order to build viable and effective channels to build a presence and ensure strong positioning in the digital sphere. Social networking will also be a part of the strategy, using platforms such as Twitter to provide updated information related to the core services and products, as well as to communicate with clients, customers and the general public. Industry publication ads are another potential avenue for targeting marketing efforts. Due to the vertical organizational structure of the business as shown in Appendix B, marketing will be conducted by the marketing specialists while sales personnel will undertake efforts to pitch the business to clients in the pipeline.

Especially important will be to focus marketing energies on sales representatives and contact with insurance industry representatives, garnering presence at industry conventions and gatherings, where networking will generate contacts and spread the word of services to be offered. The initial positioning for this business is for various sizes of health insurance companies that are looking for solutions to reduce the costs of fraud and false claims. For all types, from the smaller health care insurance providers to the large, multinational type, this service aims to create value and savings for different tiers of service including the most basic and up to the most complex enterprise solution.

## Sales Strategy

The sales strategy will be driven not only by presence via online channels and personal representation but will also rely on sales representatives to tailor plans to the larger enterprise clients in such a way that they are aware of the savings and benefits of this service. For smaller insurers, transparent pricing plans that are accessible, understandable, and furthermore that make financial sense to the companies will be provided. For this reason, much of the overarching sales strategy will rely on highlighting the immense damage caused by fraudulent insurance claims and focus on reducing them can increase the bottom line and profitability of any enterprise.

Another important aspect of the sales strategy resides in insurers’ retention and service. By providing responsive, attentive, and accessible service, an image of providing a service that is attuned to client needs and a willingness to satisfy those needs will be created. The insurer philosophy is paramount and will be a major strategy for consolidating and maintaining clients.

Finally, the effectiveness of this service and its economic benefits are fundamental attributes that insurers will be evaluating. Due to the often-abstract nature of fraud prevention, interface and activity reporting will be a central part of the offered services. This aspect of the sales strategy involves providing insurers with clear communication that makes the benefits of this service visible and understandable to the decision-makers in their organizations. Examples of possible visualizations and reports that can be provided to insurers are: number of flags/alerts, number of flags/alerts resulting in claims denials, number of fraudulent claims detected, number of suspicious claimant profiles identified, number of prevented transactions due to claimant flags, projections of fraudulent activity economic savings averted by our measures.

# Financial Plan

## Essential Assumptions

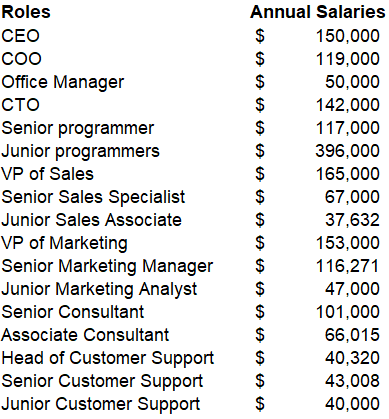
As with any new business or startup, there is an initial period in which the focus of the business activities will be to build a strong client base and find areas in which to grow the business. In this sense, some of the essential assumptions incorporated in the following projections are that payroll costs will be stable throughout the first year minimum, as well as overhead costs.

Listed below and in Table 1 are assumptions of fully loaded salaries of employees according to industry averages (Indeed, 2019). These software and technology costs are averages and based on comparable companies that have managed to successfully implement such technologies but on a larger scale.

Some of the assumptions made in this business plan include:

* 1. Amazon Web services and the technology needed to start this business will total $500,000 with an estimated $30,000 put aside for capital expenditures.
  2. All equipment will undergo a five-year straight-line depreciation.
  3. Sales and payroll taxes are estimated to be 21% as per the industry average
  4. A total of 6 junior programmers will be hired
  5. All salary estimates are based on industry averages (Indeed, 2019)
  6. An attorney will be contracted on a needs basis ($35/hour) in order to ensure 100% utilization of legal services when need be

Table 1: Summary of Hiring Costs



## Client Pricing Plans and Pricing Structure

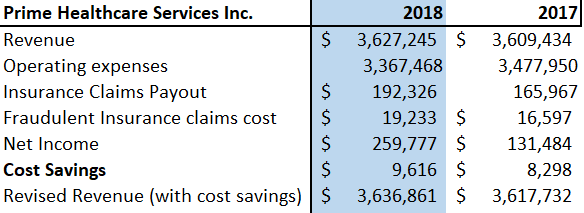
Clients will be provided with numerous pricing options depending on the size of the business, concretely, the volume of policy holders and the complexity and amount of data. The initial pricing structure will represent a variable rate that is proportional to business size, with insurers receiving discounted rates for higher volume plans. The nature of the business facilitates scaling without having to increase resources proportionally, since most of the work will be done by machine learning and software.

The pricing options available to clients come in 3 forms - basic, standard and pro. With the basic package, clients are provided with the product, but will not be provided with consulting services. In the case where issues will arise, the client will be responsible for resolving them. On the other hand, standard and pro pricing options provide clients with the product and consulting services. In the case of pro pricing, customer service representatives are available to help clients with debugging and resolving product issues. Clients have the flexibility to pay on a monthly basis or provide a one-time payment.

## Client Benefits

Specific client benefits will be provided for based on an analysis of the software’s number of fraudulent flags and interventions. A sample calculation could be based on previously cited industry numbers that conservatively estimate the amount of health care fraud as approximately 10% of all claims payouts (Insurance Information Institute, 2019). With this information, we could stipulate cost savings of avoiding 50% of fraudulent claims for insurers, with 30% of those savings as revenue for the business and 20% for the client(s). An initial assessment of prospective clients will include a projection of expected savings contrasted with the cost of the service offered so that the client has a clear picture of the benefits being provided. A sample cost savings is provided below in Table 2 using the financial information of Prime Healthcare Services Incorporation (Ernst & Young, 2019).

Table 2: Sample Cost savings for Prime Healthcare Services Inc

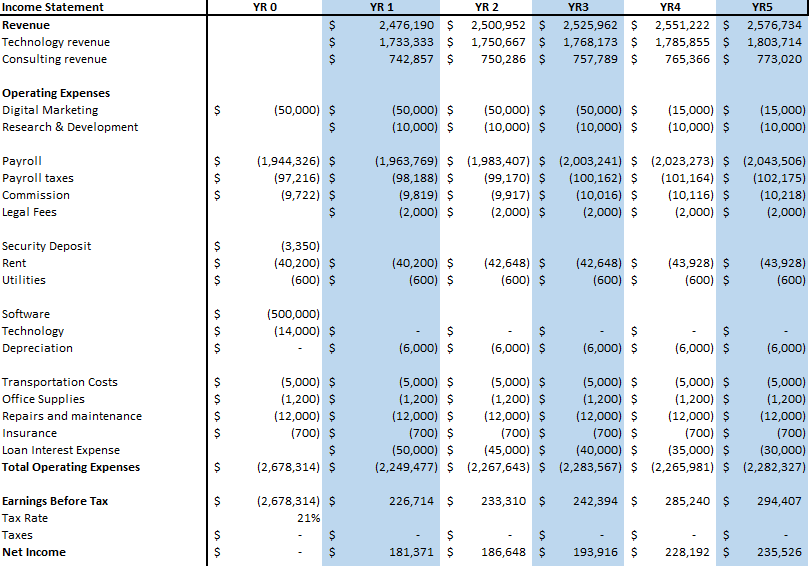


## Pro Forma

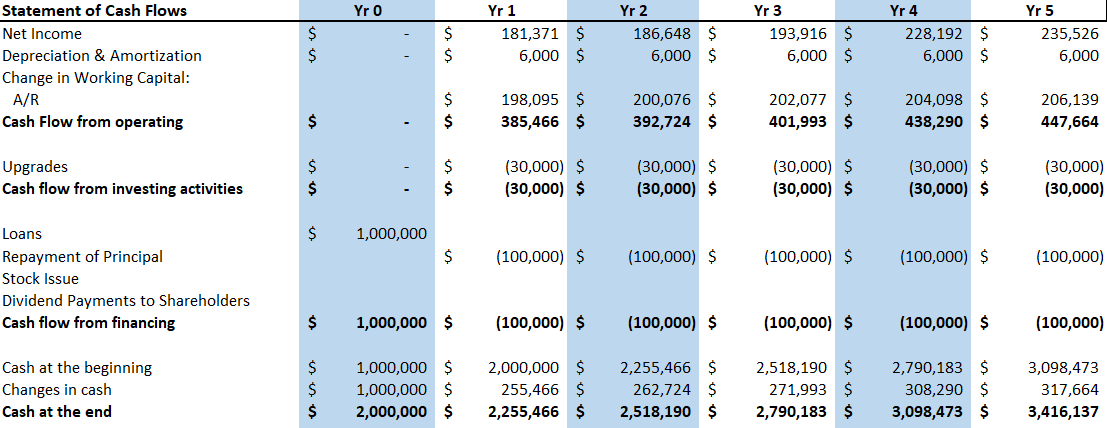
The business is seeking a million-dollar bank loan at a 5% interest rate over 10 years. The income statement below in Table 3 summarizes numerous aspects of the first year of performance of the business, specifically revenues, expenses, and costs, in order to give executives and investors a relatively accurate depiction of the first fiscal year’s financial performance. Assuming that the annual cost of fraud in the health insurance market is $52 billion, with about 6300 health insurance companies in the US, the cost acquired per insurer is approximately 8 million dollars. Assuming that this business proposal is able to save insurers 30% of those fraudulent costs, that is an estimated $2 million dollars in revenue for this business in the first year – assuming that we are able to secure one client in the first year. Furthermore, commission is estimated to be 4% of net revenues in order to incentivize sales personnel into marketing the business to prospective clients. Rental space required for this business is approximately 1000 square feet, with the average cost per square feet being $3.35 bringing annual rent expense to $40,200 in year 0.

Total revenue was increased by 1% every year, with the assumption that each year, the business will be working with one client, capturing cost savings of 20% to insurers in need of standard services where technology and consulting services will be needed. Because there isn’t enough operating income to offset the negative operating loss from Year 0, the business will not pay taxes in the first five years. However, eighty percent of the full net operating loss from Year 0 is recorded as a Deferred Tax Asset on the Balance Sheet, which is then used as an expense on the income statement to lower net income for future years as shown in Tables 3 and 5.

Table 3: Income Statement

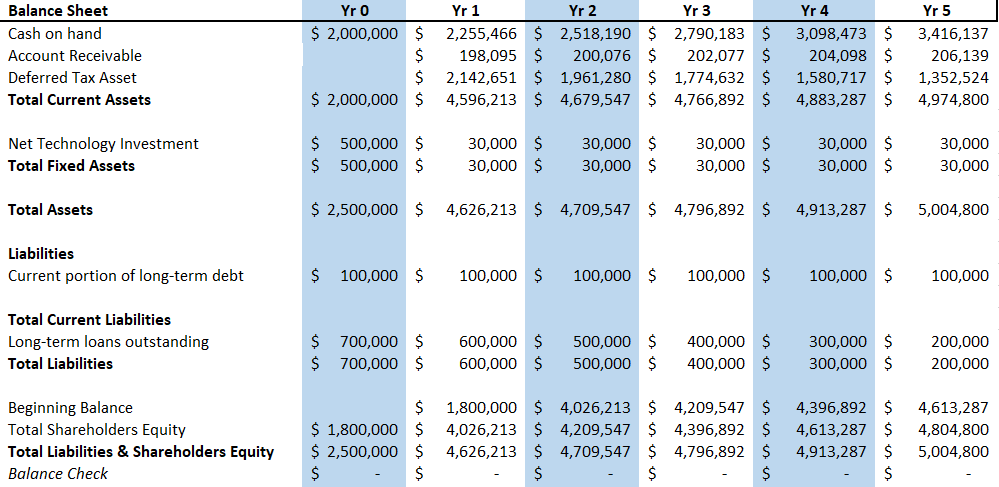


The cash flow statement below in Table 4 is a summary of the company's operating performance, focusing on the ability of the business to meet operational expenses. Since we are requesting for $1 million dollars from investors at a 5% interest rate spread over the course of 10 years, we see that principal payments will be made each year. Money that will be used for capital expenditures and software updates in the future are shown under upgrades in the statement of cash flows in the amount of $30,000 every year. The business is projecting positive cash because of the impact of taxes on the taxable income. Due to the 2.6 million dollars of operating loss from Year 0, the value of the business’ assets increases, thereby providing the business with larger net income as seen in Tables 3 and 4.

Table 4: Statement of Cash Flows

It is expected that not all clients will be able to pay a one-time fee for the cost of the services that will be provided, and as such, Accounts Receivable are estimated to be approximately 8% of the total revenue the business will incur as shown in Table 4. Net technology investment are from investments in Amazon Web Services software and the total cost of technology and equipment purchases in years 0 and 1. The loss from Year 0 on the income statement allows the business to lower its taxable income in Years 1 to 5. Eighty percent of the loss is spread over the subsequent years’ net operating net income and is recorded as a deferred tax asset on the Balance Sheet as shown in Table 5. A summary of the balance sheet statement for the business is shown below.

Table 5: Balance Sheet



# Implementation

## Implementation Strategy

The core activities of implementation will begin with a 4-month planning & financing phase - an initial hiring phase and platform building phase as shown in Table 4 below. It is in this phase that all IT hiring will be conducted in order to begin the early stages of obtaining Amazon Web Services products and predictive algorithms for fraud claims. Once the algorithms are being built, the next phase of building the interface will begin. During this phase, there will be a focus on training the algorithms to categorize different types of claims data while being able to assign risk scores based on transaction risk profiling, risk and network analysis of sample claims data.

When the training of the algorithms to assign risk scores and flag fraudulent claims are complete, the next phase will involve the testing of the interface. It is during this phase that debugging of errors will take place, in addition to designing an implementation strategy for clients. During the implementation planning phase, there will be a focus on the development of realistic timelines, including that pertaining to financing, marketing, technology development, and product testing. Furthermore, this stage will incorporate a planning of evaluation measures, which are essential in determining what aspects of the business plan are working.

A guideline that can be used in evaluating aspects is Holden & Zimmerman’s (2009) EPIC evaluational model for strategic plans (assessing contexts, gathering reconnaissance, engaging stakeholders, describing the plan, and focusing evaluation). In addition, human resources planning will define and anticipate business needs in all sectors of the project. Sales personnel will be responsible to pitch the business venture to insurers once all the above phases are complete. Prior to pitching to investors, the marketing plan will be analyzed to determine ways to market the business to insurers besides the use of networks and Allegheny County Data. Within the first year, the business must be able to secure a minimum of one client in order to go into business. Afterwards, management and programmers will work with clients to define the project scope and outline in depth the necessary steps to undertake in the successful completion of the project.

Table 6: Implementation Timeline

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Month | 0-2 months | 2-4 months | 4-6 months | 6-9 months | 9-12 months |
| Planning Phase |  |  |  |  |  |
| Hiring & Technology |  |  |  |  |  |
| Interface design |  |  |  |  |  |
| Product testing |  |  |  |  |  |
| Marketing phase |  |  |  |  |  |

# Summary

According to Allied Market Research (2019), the global health insurance industry is valued at over $3.153 trillion and will reach $4.475 trillion by 2026, which constitutes a remarkable 4.4% compound annual growth rate (CAGR) in the next six years. This expansion of the global health market will possibly result in a growth in certain services and needs for the industry, not only in terms of direct client-provider services, but also in fraud assessment, recovery, and prevention services. The increasing digitalization of the industry, in general, presents an excellent opportunity to adapt global software products for use in diverse markets and locations.

There are a few companies that see the benefits of predictive analytics and machine learning in preventing health insurance fraud. One such company is Alpine Security, an SAS competitor that focuses on advanced analytics in detecting possible security risks and finding adequate solutions to minimize them. Their focus in marketing their services has been in highlighting several significant breaches in the last 6 years in which over 109 million Americans have had their sensitive data stolen from health insurance computers due to malicious activity (Espinosa, 2018). While Alpine Security pitches directly to health insurance providers, their service is not necessarily specific to the industry.

The primary mission of this business plan is to save health insurers money that stems from fraudulent claims and provider activities while keeping costs down. Through the use of risk and transaction analysis, user profiles of individual and group policyholders can be profiled for machine learning while predictive learning technology will detect and define possible new patterns that indicate fraudulent activity for insurers; this way, they are prepared with the tools to take ownership of fraud prevention moving forward.

# Conclusion

This business proposal seeks to offer customized solutions for insurers based on powerful proprietary software modeling, which is used in conjunction with existing tools in fraud prevention to conduct in-depth analyses of any health insurance company’s claims system and user profiles. To begin, an investment of one million dollars will be sought from investors in the form of a loan in order to cater to the startup costs of the business. More importantly is the ability of the business to payback the initial investment cost within 2 years, signaling that the business will be able to meet its operational costs and expenses in the future. It is encouraging to consider that there is a global market for private and public health insurance that could represent an utterly immense potential market for the services being offered in this business plan. The centralization of the software services offered in this business proposal could facilitate a smooth adaptation to operation in other markets in the future as well.

* + - * 1. Satellite Map of Business Location in Nova Place, Pittsburgh, PA



* + - * 1. Organizational Structure of the Business

# Bibliography

Accenture. (2018). Finance & Risk Practice for Financial Services​ | Accenture. Retrieved January 17, 2020, from Accenture.com website: https://www.accenture.com/us-en/financial-services-finance-risk‌

Accenture. (2017). One in Four US Consumers Have Had Their Healthcare Data Breached, Accenture Survey Reveals | Accenture Newsroom. Retrieved January 17, 2020, from Accenture.com website: https://newsroom.accenture.com/news/one-in-four-us-consumers-have-had-their-healthcare-data-breached-accenture-survey-reveals.htm

Allied Market Research. (2019). The Global Health Insurance Market. Retrieved January 17, 2020, from Allied Market Research website: https://www.alliedmarketresearch.com/health-insurance-market

Culp, S. (2014, February 3). Insurers Help Themselves and Their Customers by Fighting Fraud More Effectively. Forbes. Retrieved from https://www.forbes.com/sites/steveculp/2014/02/03/insurers-help-themselves-and-their-customers-by-fighting-fraud-more-effectively/#8d679cd7647f

Deshpande, K. (2018, April 4). The Power of Analytics For Insurance Fraud Detection - Insurance Insights. Retrieved January 22, 2020, from Insurance Insights website: https://blogs.lexisnexis.com/insurance-insights/2018/04/the-power-of-analytics-for-insurance-fraud-detection/

Espinosa, C. (2018, March 29). Alpine Security. Retrieved January 17, 2020, from Alpine Security website: <https://www.alpinesecurity.com/blog/5-biggest-healthcare-cybersecurity-breaches>

Statements, C. F. (2019) Ernst & Young LLC. Prime Healthcare Services Inc.

GAO. (2018). Medicare: Actions Needed to Better Manage Fraud Risks. Gao.Gov, (GAO-18-660T). Retrieved from https://www.gao.gov/products/GAO-18-660T

Holden, D. J., & Zimmerman, M. A. (2009). Evaluation planning here and now. In D. J. Holden & M. A. Zimmerman (Eds.), *A practical guide to program evaluation planning: Theory and case examples*. [Sage e-book].

Holzhauer, E. (2018, September 27). Fraud Detection at FICO with MongoDB and Microservices. Retrieved January 22, 2020, from MongoDB website: https://www.mongodb.com/blog/post/fraud-detection-at-fico-with-mongodb-and-microservices

IBISWorld. (2020). IBISWorld - Industry Market Research, Reports, and Statistics. Retrieved January 17, 2020, from Ibisworld.com website: <https://www.ibisworld.com/industry-statistics/market-size/health-medical-insurance-united-states>

Indeed (2019). Retrieved from https://www.indeed.com/salaries/contract-attorney-Salaries,-Pennsylvania

Insurance Information Institute. (2019). Background on: Insurance fraud | III. Iii.Org. https://www.iii.org/article/background-on-insurance-fraud

Mauri, R. (2017, July 12). Blockchain for fraud prevention: Industry use cases - Blockchain Pulse: IBM Blockchain Blog. Retrieved January 22, 2020, from Blockchain Pulse: IBM Blockchain Blog website: https://www.ibm.com/blogs/blockchain/2017/07/blockchain-for-fraud-prevention-industry-use-cases/

NHCAA. (2018). The Challenge of Health Care Fraud - The NHCAA. Retrieved January 17, 2020, from Nhcaa.org website: https://www.nhcaa.org/resources/health-care-anti-fraud-resources/the-challenge-of-health-care-fraud.aspx

NHCAA. (2020). What Does Health Care Fraud Look Like? - The NHCAA. Retrieved January 17, 2020, from Nhcaa.org website: <https://www.nhcaa.org/news/what-does-health-care-fraud-look-like.aspx>

SAS. (2020). Health Care Fraud Detection and Investigation Software | SAS Detection and Investigation for Health Care. Retrieved January 17, 2020, from Sas.com website: https://www.sas.com/en\_us/software/detection-investigation-for-health-care.html

Schiller, K. (2018, February 25). Aetna is taking on insurance fraud with machine learning - Arcweb Technologies. Retrieved January 17, 2020, from Arcweb Technologies website: https://arcweb.co/aetna-fraud-machine-learning/

UPMC. (2019). UPMC CY 2019 First Quarter Financial Results. UPMC | Life Changing Medicine.https://www.upmc.com/media/news/050219-financial-results-first-quarter-2019

US Census Bureau. (2018, September 12). Health Insurance Coverage in the United States: 2017. Retrieved January 17, 2020, from The United States Census Bureau website: https://www.census.gov/library/publications/2018/demo/p60-264.html