
Megha Venugopal, Senior Technology Consultant
Aswin Natarajan, Manager
Deloitte Consulting India Pvt Ltd
Abstract

As we are steadily marching towards digitalization and virtualization with the intent to save millions of person hours and start maintaining transactions online, there is one dangerous off-shoot which every major organization both Government and Private are struggling to combat – **Cyber Threats** that results in data breach, theft of identity & personal information. World over, there has been numerous instances of fraudulent transactions be it either stolen credit cards, or stolen PHI or PII information that is **causing friction between organizations and its consumers.**

While organizations have to contend with **credit card theft, loss of personal health information** at an individual level, there are also several **data breaches** that hit the enterprise at the same time resulting in loss of reputation on top of data.

At an enterprise level, according to a Nasdaq report dated September 2015 \(^1\), there were **over 1,500 incidents of data breaches (up by over 46% from 2013)** leading to compromising over one billion data records. According to Nilson Report, October 2015 \(^2\) the **global credit and debit card frauds** accounted for **$21.84 billion in 2015** which is more than the GDP of 30% of the countries in the globe.

This paper describes an approach where organizations can use a combination of two seemingly disparate cognitive techniques such as Robotic Process Automation and Voice Recognition that can help combat and prevent fraudulent transactions.
## Contents

Global Financial Services & Healthcare Industry in 2017 – An Outlook ................................. 4

Cyber Security & Cyber Threats – A never-ending Game of ‘Cat & Mouse’ ....................... 5

Conventional Fraud Management Techniques – Typical Challenges ................................. 6

Need for Alternative Techniques for Fraud Prevention .......................................................... 7

Combating Fraud using Alternative Techniques: Cognitive RPA and Cognitive VR........ 8

Use Case 1: Financial Services – Monitoring of Credit Card Usage ............................... 8

Use Case 2: Health Plans– Monitoring for prevention of unauthorized use of PHI & PII ............................................................................................................................................. 11

How can organizations benefit ............................................................................................. 14

Looking Ahead ....................................................................................................................... 16

Cited References .................................................................................................................... 17

Other References ................................................................................................................... 17

Appendix A ............................................................................................................................. 18

Appendix B ............................................................................................................................. 19
Global Financial Services & Healthcare Industry in 2017 – An Outlook

The global financial services and healthcare industries are currently at an inflection point. If one were to look at the top challenges faced by these two seemingly diverse industries, the themes are strikingly similar. There are three critical areas of ‘disruptions’ these industries are currently facing which is shaping the outlook on how 2017 and beyond is going to look like.

Due to an ever changing and increasingly complex regulatory landscape, rising consumerism and rapid advancement of digitization and a population that is becoming increasingly aware, it has become imperative for these organizations to be more proactive as opposed to be reactive.

Due to rapid digitization and preference for online transactions, it is critical for organizations to have robust security mechanism that will enable organizations to stay ahead of online fraudsters and hackers.

![Figure 1: Top Challenges for Financial Services and Healthcare Industry in 2017](image-url)
Both healthcare and financial services organizations have had several mandates and regulations that has caused disruption of their business operations and technology stack. While the healthcare industry has just about figured out its approach to a slew of regulations (and counter regulations) such as ACA, AHCA (which is still under discussion), ICD-10 etc., the financial services industry was hit by Brexit implications in 2016.

Next comes the market disruptions where industries are facing competition and challenges from both traditional and non-traditional players. For example in the case of healthcare industry, one of the leading trend is towards Retail Care Offering (RCO) where pharmacy players such as CVS and Walgreens are moving from their traditional model to a more integrated care delivery. If one were to compare the same on financial services, 2016 saw the rise of several Financial Technology (FinTech) and Insurance Technology (InsurTech) entering the market with a unique set of products and offerings.

In addition to the above, changing consumer demographics and mindset in terms of preferring a more digital/online approach to doing things as opposed to the traditional means is providing both an increased level of challenges as well as opportunities for the organizations to handle. As consumers are adapting to newer technologies and going digital, there is always an element of risk in terms of the data falling into the wrong hands. The implications for such an event is very huge and as a result it is essential for organizations to have very robust data security or cybersecurity mechanisms to combat data breaches, fraud and theft of data.

**Cyber Security & Cyber Threats – A never-ending Game of ‘Cat & Mouse’**

While these global institutions are battling multiple waves of technology disruptions, they have to deal with another set of monsters in the form of cyber threats. Due to rapid digitization and the fact that the hackers have somehow managed to stay one-step ahead of these organizations, there are several issues they have to contend with.

**Data Breaches**

While industries of any type can be prone to data breaches, the losses for financial services institutions are two fold - damage to credibility and loss of confidential membership data that can have catastrophic consequences. For example it was noted in Gemalto’s Breach Level Index Report, March 2017 that there
were a total of 1,792 worldwide leading to almost 1.4 billion records compromised (an increase of 86% from 2015) which shows that as firms are boosting their arsenal with latest technologies, so are the disruptive forces. Of this, more than 2/3 (68%) were caused by malicious outsiders with the sole intent to damage the overall credibility.

**Credit Card Theft**

If one looks at the credit card industry, as stated in the Nilson Report from October 2015 [2], the global loss due to credit card fraud was pegged at $21.84 billion of which 72% was borne by card issuers. If one looks at these numbers in perspective, then the damage is not just financial but the overall credibility of the institution takes a beating.

**Medical Identity Theft**

Medical Identity Theft is on the rise. While 2015 might seem a distance memory, one had not seen a data breach of such magnitude until the news of the three Blue Cross & Blue Shield plans came to light where close to 92 million records were affected, according to the Forbes Report [6]. According to the Identity Theft Resource Center (2016) Report [7], healthcare and financial services accounted for around 40% of the overall hackings. In the case of healthcare industries that ramifications are much beyond financial as members’ PHI and PII are either in public domain or sold off to the dark web for disruptive elements. There are situations where fraudsters can steal medical identity of someone else to avail medical services or even worse procure drugs which would not have been given under the normal circumstances.

**Conventional Fraud Management Techniques – Typical Challenges**

All organizations have robust fraud management systems that works on a set of rules and any action not conforming to those rules will automatically trigger a series of alerts and subsequently activating a set of events. While organizations have been successful in creating a set of robust processes, there are two critical areas of concern that needs to be addressed in order to come up with an effective set of solutions - *how to prevent fraud and at the same time not to scare genuine customers.*
The number of individuals impacted by identity theft and consumer fraud has resulted in loss of $16 billion from over 15.4 million victims \(^9\). Since 2010, identity thieves have stolen over $107 billion.

Organizations in their zeal to combat fraud, are falling into the most common pitfall of scaring away consumers by placing a lot of hurdles in their online experience by placing additional requests during the authentication process of an online transaction. As a result organizations are always in a state of conflict between enabling a better consumer experience Vs improving its ability to combat fraud.

While traditional fraud management techniques have been effective in detecting fraud, there are some inherent challenges as illustrated in the figure below.

Please refer to Appendix A for additional details around challenges faced by organizations and individuals alike in using Conventional Fraud Management Systems.

**Figure 2**: Typical challenges in Conventional Fraud Management Techniques

**Need for Alternative Techniques for Fraud Prevention**

While institutions are beefing up conventional techniques and investing in their existing security processes to ensure multiple layers of protection are created, it could be worth exploring additional or alternative approaches. The intent is to not replace the existing approach to see how the alternate approach can complement and co-exist with conventional approaches.
With the rise of concepts such as Machine Learning and Deep Learning, organizations can leverage Cognitive techniques such as Robotic Process Automation and Voice Recognition to add an extra layer of sophistication to its security apparatus.

Please refer Appendix B for additional details about Robotic Process Automation and Voice Recognition.

**Combating Fraud using Alternative Techniques: Cognitive RPA and Cognitive VR**

One of the most common issues faced by end users in the digital age is identity theft. These days’ hackers are more sophisticated and coordinated by going after users’ phone and financial data thereby leaving no chance for banks or any financial institutions to perform more effective fraud prevention. As a result even when there are identities being stolen and misused there is still the possibility of the calls from the banks landing up the alley of the hackers subsequently preventing any detection whatsoever.

We will demonstrate two varied use cases, both related to impersonation and subsequent theft of data.

**Use Case 1: Financial Services – Monitoring of Credit Card Usage**

In this scenario, a combination of Cognitive Voice Recognition and application of Cognitive RPA can be applied towards any decision taken for fraudulent transactions without hindering the customer experience.

**Member Enrollment & Fulfillment**

At this very first step, the user provides personal information to process his/ her application for a credit card. In the proposed solution, for the information gathering process, we are introducing a new step where the user can be asked a series of simple questions for which the responses would be provided in his/ her own voice. Unknown to the user, this information is then captured in the application layer and fed downwards for subsequent storage and profiling. In addition, the system can then also ask the users to read though few additional piece of standard information in order to create a specific voice pattern. Given the cost involved for storage, analysis & retrieval this can be performed only after the user’s application is accepted and successfully processed.
Pattern Storage & Profiling

This voice pattern can then be **subsequently stored in a data bank** to be accessed for the purpose of performing any validations. Since there are going to be several millions user records, all of this collective information can **stored in the organization’s Enterprise Data Warehouse** that can be subsequently retrieved in case of a need. While in the past, members’ personal information gets stored in the Enterprise Data Warehouse for subsequent analysis, here we are introducing an **additional element of mapping and storing users’ voice patterns** for future retrieval.

![Diagram](image)

**Figure 3:** Application of RPA and Voice Recognition for timely detection of Credit/Debit card frauds

User Profiling & Stratification

Given the vast amount of data and spending patterns available for analysis, organizations can then **define spending patterns and habits** including any seasonal spikes. In addition with the help of business rules
defined by Cognitive techniques such as Machine Learning algorithms specific patterns can be created. If any access to other social media sites such as Facebook, Twitter, and Instagram can be enabled, it will also help in doing additional real-time analysis. This data can then be subsequently mapped to individual users which can be retrieved in case of any anomalies from the expected behavior that can range from unusual choice of card usage, increase in volume/ frequency of transactions or the overall $ value of the transactions.

Pattern Retrieval & Validation

When the bank/ credit card firm is suddenly alerted to these anomalies that seems disproportionate to the general behavior of the user, the first step could be to send a text/ SMS alert asking the user to provide or respond to a basic set of queries. In addition, a call can then be placed to validate the authenticity of the transactions performed. In order to prevent any doubts, the automated call will then ask the user to a series of questions and will process both voice & data.

Depending upon the outcome, the legitimate user will either be notified of such fraudulent transactions (as opposed to finding a few weeks later in the mail) and have those addressed immediately. In case the user appears to be impersonating someone else, the card can be put on hold or suspended and the actual user informed through normal communication channels.

How the solution works

At the core of the solution lies a series of Machine Learning algorithms. These algorithms will be constantly performing a series of checks and balances with the sole purpose of identifying patterns, determining anomalies and subsequently taking a decision on the ‘fraud’ that has occurred. This in turn would trigger the Cognitive RPA function which will then act on the ‘fraud’. An automated call/ SMS alert will be triggered to the concerned user who then has to respond accordingly. Subsequently a call will also be placed to the user, asking him/ her to validate certain key information pertaining to the concerned transaction/ account. In case the responses are not in line with the expected behavior of the user profile then the user will be flagged and intimated to the concerned team(s). Hence fraudulent transactions are detected and corrective action is triggered.
Use Case 2: Health Plans – Monitoring for prevention of unauthorized use of PHI & PII

Similar to financial services, another industry that typically gets impacted due to theft of personal identity is health plans. One of most common scenarios is when someone is impersonated and ends up getting incorrect bills for medical services, prescription drugs or for any care delivery by caregivers.

In this scenario, a combination of Cognitive Voice Recognition and application of Cognitive RPA can help prevention of Medical Identity Theft by performing a detailed validation of member information using cognitive techniques. Let’s look at a scenario related to request for pre-authorization that are typically placed for high-end and expensive medical procedures.

**Figure 4: Application of RPA and Voice Recognition for Health Plans**

**Membership Enrollment & Premium Processing**

The entire process will begin at the time of member enrollment where along with membership information pertaining to demographics & financial data, a series of simple questions will be asked and
the user response will be captured and patterns would be established. In addition, unknown to the user
we are introducing a new element of the **users providing some basic personal information in his/ her
own voice** which can be captured as part of the member enrollment process. This **information capture**
will **happen at the application layer** which will subsequently be fed to the organizations’ enterprise Data
Warehouse. Similar to Scenario 1 described above, in order to manage the overall costs and the volume
of data that will be stored, this step can be involved after the member’s application is processed and the
initial premium is also paid and reconciled.

**Voice Pattern Mapping & Storage**

This **voice pattern** can then be **subsequently stored in a data bank** to be accessed for the purpose of
performing any validations. Since there are going to be several millions user records, all of this collective
information can stored in the organization’s Enterprise Data Warehouse that can be subsequently
retrieved in case of a need. While in the past, members’ personal information gets stored in the Enterprise
Data Warehouse for subsequent analysis, here we are **introducing an additional element of mapping and
storing users’ voice patterns** for future retrieval.

**User Stratification using Care Management Techniques**

Typically healthcare organizations in addition to gathering members’ information will also be investing
heavily on **Care Management** or more recently referred to as **Population Health Management** since the
cost of prevention is always less than the cost of curing something after the fact. To this effect, healthcare
organizations typically send communications in various forms and shapes to its users about health, well-
being and will also take substantial efforts to analyze user profile including risk of any ailments. In order
to perform this, organizations can **take advantage of Machine Learning tools** and algorithms that can be
constantly on the lookout for these members including suggestion of any change to their dietary regimen
or preventive wellness checks. However the additional element is leveraging these Cognitive techniques
to **define rules that would also identify and detect any anomalies or deviations** from expected user
behavior. These tools and algorithms typically engage in real-time and 24X7 behavioral profiling of
members.

**Pattern Retrieval & Validation**

In the event that a person’s medical identity is stolen and subsequently an attempt is made to access any
services using a network or out of network provider, upon detection a sequence of steps will then be
triggered. The first and foremost would be to **perform back-end analysis of the type of medical treatment** for which the pre-authorization request was placed and compare against history of visits or ailments and overall wellness chart for that member.

In case of an anomaly, an alert will be triggered in case the type of request is in out of sync with the expected behavior of the member. This alert could be in the form of a call or an SMS asking a set of responses from the user. This can be followed by placing a call to the user using an automated caller through RPA and a set of questions can then be asked. Based on the response to questions a final decision on the ‘fraud event’ will take place.

Depending upon the outcome, the legitimate user will either be notified of such fraudulent transactions (as opposed to finding a few weeks later in the mail) and have those addressed immediately.

**How the solution works**

At the core of the solution lies a series of Machine Learning algorithms. These algorithms will be constantly performing a series of checks and balances with the sole purpose of identifying patterns, determining anomalies and subsequently taking a decision on the ‘fraud’ that has occurred. This in turn would trigger the Cognitive RPA function which will then act on the ‘fraud’. An automated call/ SMS alert will be triggered to the concerned user who then has to respond accordingly. Subsequently a call will also be placed to the user, asking him/ her to validate certain key information pertaining to the concerned transaction/ account. In case the responses are not in line with the expected behavior of the user profile then the user will be flagged and intimated to the concerned team(s). Hence fraudulent transactions are detected and corrective action is triggered.
How can organizations benefit

Organizations can have a range of benefits through effective and possibly enterprise-wide application of Cognitive Robotic Process Automation and Cognitive Voice Recognition.

Some of the key benefits include but not limited to the following.

**Improved Customer Retention**

As mentioned earlier, identity theft is one of the major concerns of individuals and end-users especially when it comes to credit cards. As stated in the Nilson Report, October 2015 [2] the credit card users bore 72% of the total financial loss (of $21.84 billion). Using the above Cognitive techniques if a significant portion of fraud can either be prevented or detected at an early stage and the members subsequently informed this would definitely lead to increased customer satisfaction and subsequently possible word of mouth publicity and improved sales.

**Enhanced Secondary Sales**

While Cognitive RPA and Cognitive VR can be primarily used for fraud prevention, the analysis of spending patterns can be used to offer alternate or better products to the customers more suited to their life-style.
**Accelerated Financial Impact**

In addition to the impact to customers, there is also a lateral impact to financial organizations. It is a well-known fact that the cost involved in maintaining an existing customer is always less compared to the cost of acquiring a new customer. In case of any frauds, the customers tend to get disillusioned and might also leave for a competitor thereby causing financial strain on the organization who would now need to tap into new customers or risk losing market share.

While the application of a full-blown Cognitive RPA and Cognitive Voice Recognition will reap plenty of benefits for organizations, the process of implementation takes time and is going to be expensive with the level of integration required.

However having said that, organizations should slowly start on the path of RPA if already not so that the required setup can be implemented over a period of time.
Looking Ahead

There are several merits for organizations especially in Financial Services and healthcare to choose the path of Cognitive RPA and Voice Recognition for combating and preventing fraud. This is by no means to supplant the existing conventional techniques but rather to enhance them wherever possible.

With the advent and **extensive usage of Machine Learning and Natural Language Processing**, there has been a splurge of big and small players on the market offering **solutions around Cognitive Thinking**. Given the fact that the world is not going to move away from digitalization and virtualization of workplace, it is imperative that more robust techniques be in place to reinforce existing processes.

However there is never only one right answer or one right approach for the unexplored. Organizations should look at their risk taking appetite, robustness and stability of existing processes before embarking on this journey to ensure that the new process complements existing ones and does not end up competing with or cannibalizing them. In the end, it is always a good (albeit radical one maybe) for enterprises to identify ways to come together, share ideas and share best practices to ensure that there are enough barriers to prevent loss of financial, PHI or PII data.
Cited References

Other References
Appendix A

Below are some of the key challenges faced by organizations in combating fraud using conventional techniques.

Robust but inflexible Systems

While the conventional fraud management systems are robust, one area where they might be lacking is in terms of flexibility to integrate with different functions of the enterprise and adaptability to read data from traditional and non-traditional medium. As a result, the alerts thrown by these systems are more siloed in nature as opposed to offering a more integrated view.

Multiple fraud management systems across the value chain

Most of the organizations have multiple fraud management systems across the value chain that could be separated for example either by the line of business or geography they are targeting. As a result, there are instances where a transaction gets flagged resulting in a harrowing experience for the customers. These systems were meant more of a ‘band aid’ fix instead of a long-term solution since the organizations did not want consumers to get impacted in the meantime. However the same set of solutions could instead be acting as ‘trouble maker in chief’ for genuine consumers.

Lack of Access to External Data

The process of purchasing an insurance or Financial Services product has moved from an elaborate experience to a more digitized process where brokers are at the forefront of using alternate distribution channels such as mobile apps or portals. As a result there is a lack of personal connect and the process of performing an end-to-end validation from available sources (Credit Bureau, Chamber of Commerce) and other non-traditional sources (Social Media websites) rarely happen. Hence the analytics functions that the organizations have setup will never reach its full potential in terms of scalability and usability.

Lack of Real-Time Behavioral Profiling & Analysis

Fraud management systems cannot afford to have a down-time since fraudsters do not. As a result, it is important for organizations to have systems that do not hinder the millions of transactions taking place during the process of profiling and analysis. While the conventional techniques will have performance parameters built in, in times like these there is a need for having a more adaptive or ‘Cognitive’ solution that has the ability to constantly learn, improve and implement its learnings without disrupting the user experience.
Appendix B

Robotic Process Automation Overview

Automation in manufacturing and production line exists for several years, where robotic hands work handle manufacturing and packaging goods. Robotic Process Automation or RPA is a methodology, to extend automation to Information technology services by deploying software bots.

RPA takes the robot out of the human. The average knowledge worker employed on a back-office process has a lot of repetitive, routine tasks that are dreary and uninteresting. RPA is a methodology of using software that mimics the activity of a human being in carrying out a task within a process. It can do repetitive stuff more quickly, accurately, and tirelessly than humans, freeing them to do other tasks requiring human strengths such as emotional intelligence, reasoning, judgment, and interaction with the customer.

However, automating Information technology services has unique challenges, it requires disparate enterprise applications to talk to each other while keeping the end-to-end implementation flexible enough to deal with changes in business requirements.

Evolution of RPA

Robotic Process Automation has evolved over the years as a result of varied research and continued usage in several areas. As a result there has been a natural progression from being used as a tactical tool to being deployed as a strategic response to some of the threats organizations are facing from insiders and outsiders.

The basic form of RPA also known as ‘Repeat & Do’ RPA is typically suited for transactional activities that requires a consistent pattern of user input in addition to zero need for any decision making. Here the RPA involves process automation where computer software drives existing applications through their standard user interface in the same way that a human does, in other words it orchestrates applications via presentation layer integration in contrast to integrating via the application back-end.

Next on the evolution chain is the Autonomous RPA which can be primarily applied for end-to-end automations and validations. The latest in the evolutionary chain is the Cognitive RPA which is suited for
situations where the user performs an action after analyzing the data and making a decision. Here RPA is achieved by applying machine learning.

![Figure 6: Evolution of RPA](image)

**Voice Recognition Overview**

The concept of voice recognition is the ability of machines to understand, interpret and decode human voices which can range from a few simple texts to complex speech and spoken commands with the main intent of creating and mapping human speech patterns.

The application of Voice Recognition can range from simple textbook commands such as ‘Open Internet Explorer’ or ‘Open Music’ to complex approaches including Natural Language Processing. Today the usage of Voice Recognition has been pushing the envelope of realism in terms of wide ranging applications such as Siri for Apple, Alexa for Amazon, Google Assistant etc.
Author Biography

Megha Venugopal

Megha Venugopal has over 9 years of experience in the field of Software and Product Development. She has worked extensively on embedded systems and Cognitive tools in Automotive Infotainment, Hi-Tech and Telecom and Media industries.

Megha is also experienced in translating complex business needs and requirements to technical features. During my tenure with Robert Bosch, Intel and AT&T she has worked on several mission critical projects and have gained expertise in managing complex projects and working with cross-location teams across India, Germany, USA and Taiwan.

During her stint with Intel Corporation and AT&T, Megha has submitted for several invention disclosures of which, two are in the patent filing process:

- Patent filed for “Coordination of connected home devices to provide Immersive Entertainment Experiences”
- Patent filed for “Method And Apparatus For Recording Advertised Media Content”

Megha has a Bachelor’s degree in Electronics & Communications Engineering from Mahatma Gandhi University, Cochin.

Megha is married to Aswin Natarajan and they welcomed their first child, Baby Ayra in 2016.
Aswin Natarajan

Aswin Natarajan is a PMP certified Healthcare Professional with over 13 years of experience in Business & IT Consulting, Project Management & Delivery of complex healthcare solutions for the US Payer market.

Since completing his engineering in 2003, Aswin has worked on various industries such as Telecom and Insurance on delivering performance engineering and enhancement solutions before eventually finding his home in Healthcare.

Aswin has done several assessments for US Health plans for their readiness in meeting various regulatory compliance initiatives such as ACA, ICD-10, since 2010.

At present Aswin is managing a multi-year engagement for a leading US Health Plan in transforming and revitalizing their core business operations by enabling cross-platform movement of critical member data to enhance and improve the overall operational efficiency and subsequently improve their customer experience.

Aswin has a Bachelor’s degree in Electronics & Electrical Engineering from Anna University & Masters in Program Management from SP Jain Center of Management, Singapore.

Aswin is married to Megha Venugopal and they welcomed their first child, Baby Ayra in 2016.
THANK YOU!