Business Case

Biometric Access System for MTA Services

Anirudh Dave, Dhananjay Atree, Disha Thakkar, Navneet Poddar, Pallavi Varandani

Department of Technology Management and Innovation
New York University, Tandon School of Engineering

Author Note,
This Business Case is prepared for Capstone MG-GY 9503, taught by Professor Caitlin Augustin & Professor Jabril Bensedrine

TABLE OF CONTENTS

Problem Statement

The MTA is one of the largest public transportation bodies in the world. It caters to a little over 5 million riders daily. At this volume, it is possible that the system may malfunction time and again. While timeliness and efficiency have been big talking points about the MTA in recent times, we look to identify, assess and rectify the very first point of contact a potential passenger will have with this transport service. In an age of improving economic prosperity and rising competition from private alternatives, the MTA finds itself trying to stay on par with the times in terms of entry processes, technology and privacy for its accessibility options. Current systems and proposed future solutions are targeted towards improving reliability but they do not consider a few critical factors which include, but are not limited to, environmental, fare-evasion and convenience factors.

Although the MetroCard solution was a novel idea for its time and addressed many inconveniences with respect to the token system, the MTA has been suffering to keep a check on the manufacturing, maintenance and disposal of these plastic cards. Customer dissatisfaction aside, environmental activists and bodies have pointed out the difficulty of recycling used MetroCards. The plastic composition of disposed MetroCards prevents it from being mixed with other recyclable materials. It requires a completely unique recycling process which very few companies carry out, if they do at all, since the weight and volume of recycling MetroCards is negligible when compared to other MTA generated waste and hence provides little motivation to be carried out. Eliminating the production of MetroCards alone saves the MTA $10 million in costs annually.

Fare evasion has been a longstanding problem associated with MetroCards. As an extension of oneself, MetroCards continue to be misused by bypassing, theft or handing over voluntarily to a second person. Assuming only 1% out of 5 million daily riders indulge in such fare evasion activities, the MTA incurs $55 million loss in annual revenue. Automated methods of detection are missing, and the MTA still relies on law enforcement patrols to detect and apprehend fare evaders.

The world is moving from cashless to cardless systems. As the forms of payment and access change everywhere, the MTA finds itself catching up with the times, reiterating the same solution in different forms. The next phase of smart access (NFC) still involves using a ‘card’ and transitioning from magnetic strips to smart chips for tap access doesn’t addresses the underlying issues of the current MetroCard system. While these smart cards have an advantage of doubling as a debit/credit card, they are limited in the amount of money they can hold since it is still insecure due to its wireless/tap authentication method. The replacement of these cards in case of loss or theft will also be contingent upon approval from banks which leads to prolonged wait times and therefore increased customer inconvenience.

Project Plan

This Project plan gives an overview of the implementation process answering the questions: what, why, who and when. This biometric implementation project should be managed with Waterfall based feedback methodology. Looking at the size of this project, it will be executed in two phases: pilot phase and full implementation. The Work Breakdown Structure (WBS) gives an overview of the entire process. The final deliverable will be the replacement of

MetroCard with biometric fingerprint access system. The scope of this project will be limited to MTA's public transportation system to upgrade their current rider access system.

The completion of this project will require authorization from most of the departments which function under the MTA. First, the proposal will need to be approved by the Chief Development Officer. It will then be passed through the finance department where the Chief Financial Officer will sign off on the budget. The Chief of Staff and Human Resources department will then evaluate how many employees are required to see this project through and allocate personnel accordingly. The Chief of Police and the Chief Safety Officer will evaluate and clear the project based on appropriate precautions and measures to see this project through. The proposal will finally be sent to the office of the President and Managing Director who will clear the project under the guidance of the Chairman. This is based on the actual organization structure of MTA.

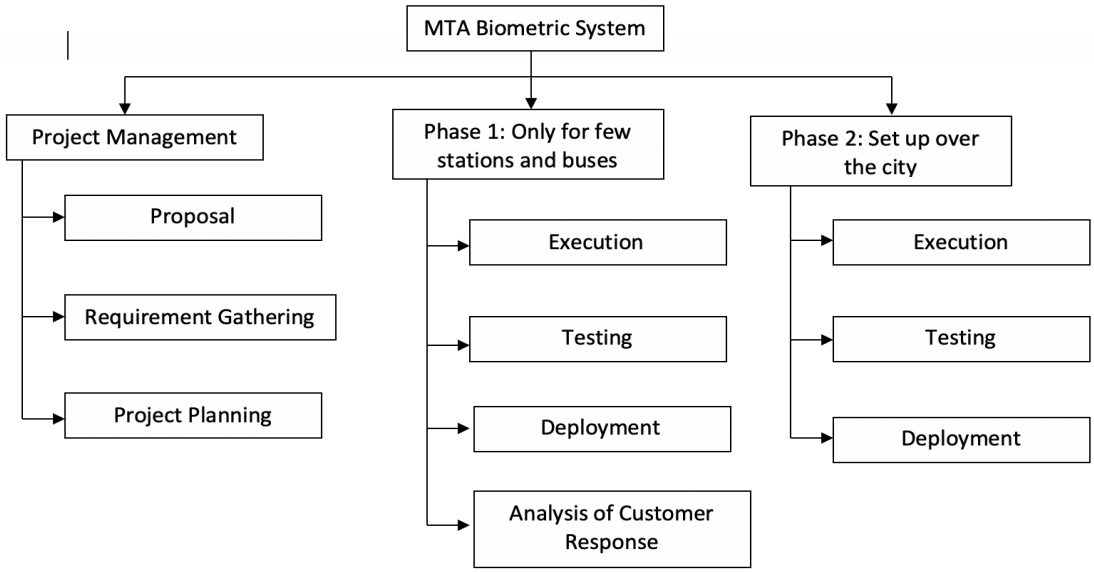

Figure 1. Work Breakdown Structure (WBS)

Before executing the two phases, a complete understanding and research of the system is vital. This can be carried out by performing initial project management steps which include submitting a proposal of the idea to the board of executives followed by gathering all the necessary requirements for the system and planning the project by creating a blueprint or prototype of the two-phase execution.

At the first phase, to analyze the performance of the new system and also to scrutinize the acceptance and satisfaction of the riders the biometric system will be set up only on few stations and in some buses. Execution at this phase would require building a mobile application for the purpose of registration using a smartphone along with modification in Entity-Relationship Schema of the original database. The Entity-Relationship Schema will have an addition of a table which contains rider information along with a unique code generated at the fingerprint scanner by its mathematical algorithm. This unique code will now act as a primary key of the database system replacing the old MetroCard numbers. Moreover, to increase the accessing time

efficiency at the turnstile new high-speed optical fibers will be installed between the servers and access point wherever required. Following these modifications at the backend fingerprint scanners will be installed at the front end which includes the turnstile, kiosk and buses.

The next step of the pilot phase will be to conduct the black box and white box testing of the new integrated system. The black box testing will examine the behavior of the scanners where the tester won't be aware of the internal structure/design of the system. This will give a pure understanding of the front-end workability with user perspective. The white box testing will be an open test where the tester will be completely aware of the internal structure/design of the system and will help to improve the algorithm efficiencies.

After successful testing of the system, the pilot phase deployment will be followed by a customer response analysis. The flaws detected from rider's response and acceptance analysis will be taken into consideration to make any required changes.

In the second phase, the entire system will be executed, tested and deployed in a similar manner all over the city. The only exception at second phase will be that the mobile application was a one-time step and won't be repeated temporarily. However, it will follow updates to next versions in the future.

Every project implementation is an organization of certain stakeholders. The major stakeholders in this transformation project are board of executive and customers. Other technical stakeholders will include the fingerprint scanner hardware company, kiosks manufacturers/dealers, software developers to develop the mobile applications and algorithms, data engineers who will be major contributors for database modifications and network engineers who will transform the optical fibers. Cyber security specialist will be one of the major technical stakeholders as they are involved to develop and maintain a secure system for the fingerprints and its related data of all the customers. In the pilot phase, CRM software is required to analyze the customer response, thus making the CRM software provider company also a stakeholder. No system is left from worn out and requires maintenance, hence, the maintenance technicians and their trainers are other major technical stakeholders.

To consider the timeliness of implementing this pilot project a Gantt chart gives a clean timeline of the project plan. As per the chart, the calculated schedule indicates complete execution duration of approximately 2 years. During the timeline, the end of every phase is a milestone achieved.

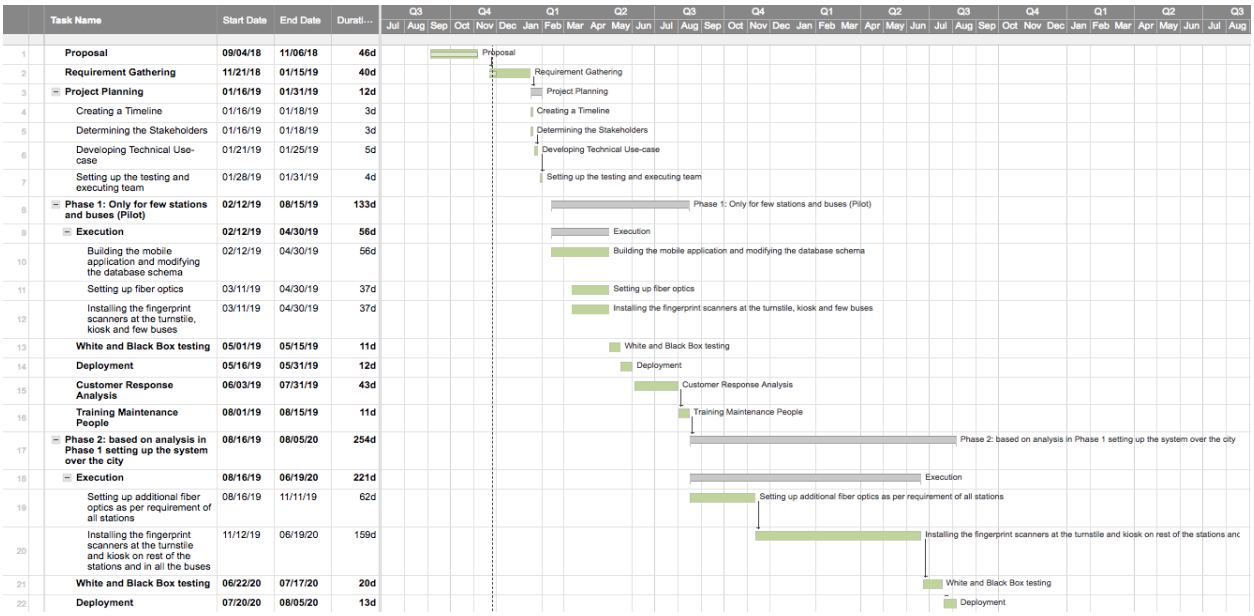

Figure 2. Project Plan

Financial Proposal

As trivial as it may seem, ticketing systems have always been an important part of a customer's transit experience. As the first point of contact in their journey, transit authorities have time and again refined their ticketing systems around the world to be cost effective while simplifying the process of access for customers. The MTA is no stranger to this evolving process.

In view of the problem, the need of the hour is a technological innovation in the transportation facility currently prevailing in New York city, a strategy that is not only cost effective but is also easily accessible by the local crowd running to and fro in the metro stations. Based on research done and as per the data from 2015-19 MTA Capital program, approximately $33.2 billion investments are encompassed to restore, augment and advance the MTA network. Currently a budget of $419 million is allocated to establish a new system through 2019 i.e. Tap Card System (NFC) which is expected to counteract against the difficulties faced by locals due to lacuna in existing MTA program. In order to implement this plan MTA is likely to approach private vendors who are expected to be the gatekeepers of one of the busiest cities in America. While this step is appreciable, an alternative which is not talked about is a system-wide improvement plan which is long-term in nature and includes improved signaling system, modernized communication and better subway access. On the whole, a System integrator designed to implement an account-based new fare payment and collection system based on biometrics.

Concentrating on this innovative technology alternative i.e. biometric implementation, the system includes installation of biometric scanners in ATMs, stations and buses. At present there exist 472 stations and 5700 buses in New York city. Considering the practical scenario of implementing a new system called Biometric Pilot Program the installation process, is likely to be

initiated on few turnstiles and thereafter taking in regard the acceptance of this system, the implementation is likely to be increased. The number of people riding through public transportation is very high therefore the proposed biometric scanners should be of high accuracy level, high-security level, long-term stability, and medium cost. So, based on our research, the 'CrossMatch verifier 300 LC 2.0' scanner machines can meet all these requirements (CrossMatch Verifier 300 LC 2.0, 2018).

Crossmatch designs solutions using scientifically proven biometric technologies which have flexible enrollment procedure and strong multi-factor authentication software. These scanners can be based on MTA needs. The Verifier 300 LC 2.0 provides high quality fingerprint images while maintaining sub-pixel geometric accuracy and is available with USB 2.0 connectivity. The compact size of this device makes it easy to integrate into existing applications. A kiosk-ready version is available to further simplify this integration procedure.

Assumptions for cost calculations

Following assumptions are taken for cost estimation purpose:

1. Total number of stations are 472.
2. Total number of buses are 5700.
3. 15 turnstiles per station
4. 5 kiosks per station.

Installing a scanner will include following cost:

1. Price of scanner
2. Installation cost at the turnstiles, ATM's, and buses.
3. Considering miscellaneous cost, i.e. wear and tear cost, damage cost, etc.

Cost Calculations

Generally, prices of installing biometric scanners range from **$5000 to $7000**. The package for biometric system includes the biometric scanner, a specialized locking system, software integration and installation. Since this will be bulk installation, the charges would be minimum which can be calculated as below:

A) Calculation of per unit cost

Sr. No.	Particulars	Amount
1.	Cost of finger scanner machine	$499
2.	Installation and maintenance cost of scanner machine	$5000
	PER UNIT COST	**$5499**

B) Calculation of Total cost

Sr. No.	Particulars	Buses	Stations
1.	Total Number	5700	472

2.	Average Turnstiles/ATMs per station respectively	-	15	5
OVERALL SET-UP (nos)		5700	7080	2360
3.	Per Unit Cost ($)	5499	5499	5499
TOTAL INSTALLATION COST (Approx.) ($)		**$31M**	**$39M**	**$13M**
INSURANCE COST, Annually ($)		**$24000**		
TOTAL COST (Approx.)		**$84M**		

Forecasting the recovery of invested resources and finances for a government funded project is a tricky process. It is almost certain that the government stands to gain next to nothing in terms of profits. There is no direct Return on Investment that can be calculated. The ROI is only realized through indirect channels when the subsidized service improves the quality of life for all stakeholders involved. The stakeholders will thus positively or negatively influence the economy of a region. The taxes that are generated through this indirect process from stakeholders eventually fills the government treasury for future projects.

Risks

Risk management is important for any organization because it helps in identifying potential problems before we confront them. A process cannot define its future or objective without identifying risks; our plan of implementing biometrics at MTA is no different. A project of this magnitude is bound to see delays and failures unless it is managed smartly. Preparing for such failures before they occur with appropriate contingency plans is critical to the success of this project.

Biometrics has been receiving an overwhelming rate of adoption since its inception. As it trickled down to more consumer products, manufacturing was scaled to meet demand and costs for such products have significantly reduced over time. It is considered as one of the most secure mechanisms of authenticating and authorizing access to personnel.

Although the advantages associated with biometrics are many and not limited to the ones mentioned above, there are multiple vulnerabilities faced by this technology. Some examples include compromising personal information, changing regulations and high latency.

Listed below are the applicable risks that can impact our project within its scope.

Strategic Risk

Given the ever-changing technological landscape, it is not unreasonable to state that public access systems can and will be updated incrementally with better technology, as is the case with smart cards. Currently, MTA is in the process of implementing tap cards for access by the end of 2019; the feature which was already in place for the MARTA Rail System in Atlanta (United States) as well as New Delhi Metro (India), by 2006 and 2008 respectively. However,

our plan to change the existing system is relatively novel when compared to other commuter services.

We understand that biometrics could be replaced in the future as well but, as a more robust technology, it is a sustainable option which also lays the framework for more advanced access systems in the future. It will be the backbone of the next generation of access systems the MTA will be able to implement.

Ensuring that the finger recognition service accommodates the needs of the handicapped and children will also have an underlying impact on the long-term strategy. Such challenges will require that the biometrics technology continues to evolve in parallel with machine learning solutions over time.

Compliance and Privacy Risk

General Data Protection Regulation (GDPR) is a regulation in the European Union which protects the privacy of the European nationals in and outside of Europe. Of the six principles of GDPR, one of the key principles that would impact biometrics is the 'Integrity & Confidentiality' principle.

This is a known risk that can impact the operations of MTA for European travelers (approximately 3.5 Million per year). To curb this issue, MTA could come to an agreement with the European Union to make the commute for their people seamless.

The absence of similar legislation in the United States has interesting consequences associated with it. The MTA is currently free to leverage biometric technology for their use in any way they see fit for their commuters. However, if a bill to the same effect is passed, it would lead to covering overhead costs that the MTA will have to incur to make their existing systems comply with the law. Such a cost cannot be quantified until the passed legislation is studied carefully and appropriate fixes are installed to the system

The Assembly Bill A9793 of the New York State Senate establishes the biometric privacy act. Its single major drawback though is that it is applicable only to private entities. Since MTA is a state-owned organization, the present regulations do not limit it to apply and use biometric technology for the benefit of its commuters. Given the fact that U.S. government agencies are increasingly adopting a range of biometric technologies, a regulation limiting its use does seem to be looming large in the years to come.

Security Risk

Database is one of the important assets for any organization. Everyday hackers' attacks on these database systems to steal their sensitive data. Among all the different kind of organizations, government organizations are most vulnerable to these kind of breaches because of their old-fashioned networks and poor security measures. To assess this risk for our biometric project, first let's understand the data flow through a block diagram.

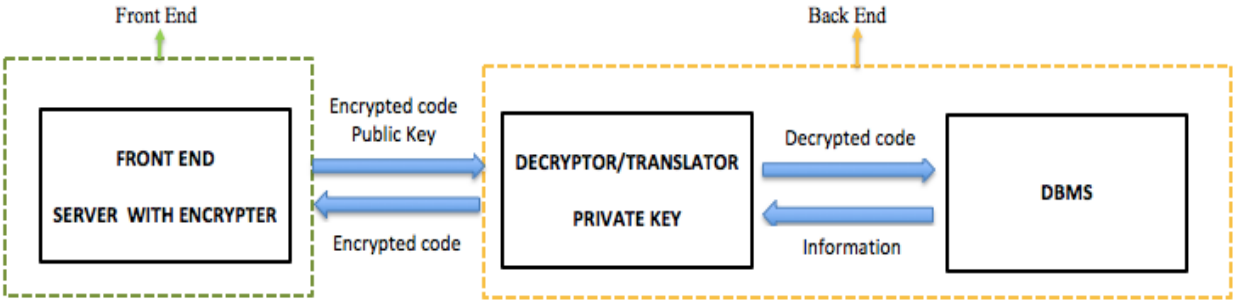

Figure 3. Data Flow Diagram

As show in Figure 2, the front-end server will send the user data in encrypted form to back end. Then back end server will first decrypt the data to pull out the information from central database system. This output information will be sent to front end as encrypted code. There is possibility of data breach between front end and back end server. The ease of data breach depends on the type of encryption and decryption methodology used in a system. The stronger the methodology, lesser is the possibility of the breach. However, strong methodology does not imply complete data breach protection but to protect the data it is necessary to have stronger methodology otherwise the cost of breach with strong methodology will be extremely high.

To protect the impacted individual user and MTA's reputation, biometric database should be covered under some cyber security insurance plan. These insurance plans will help MTA to cover legal defense expenses and liability expenses if they get sued by someone for data breach.

Financial Risk

According to our research, the total investment will be approximately $84 million. We need to ensure that we have enough cash flow to meet the planned financial obligations. Apart from assessing the project success at several milestones, we need to devise a plan to evaluate the finances too.

At times, even the best planned projects go overboard on the budget. To curb this issue, we can put certain checkpoints in place. At each quarter of the investment used ($21 million) the progress can be evaluated, and financials may be compared to previously forecasted figures. It is possible that the project might be within the budgetary requirements but then checks must be carried out that quality is not being compromised. If the expenses go overboard, management will have to understand the reason for the inflation and extra costs and adjust cash flow accordingly to match projected expenses. Also, keeping aside extra capital to absorb future unknown events will ensure availability of funds at all the stages of this technology implementation.

References

CrossMatch Verifier 300 LC 2.0. (2018, December 5). Retrieved from fulcrum biometrics: https://www.fulcrumbiometrics.com/CrossMatch-Verifier-300-LC-2-0-p/101210.htm