April 2019

Vendor Digital Identity for State Street Corporation

Mikala Elizabeth Dunbar
Worcester Polytechnic Institute

State Street Financial Technology Collaborative Focusing on Digital Identity with Relation to the Vendor Onboarding Process

A Major Qualifying Project Report: submitted to the Faculty of the WORCESTER POLYTECHNIC INSTITUTE in partial fulfillment of the requirements for the Degree of Bachelor of Science

Written by:

Mikala Dunbar, BUS and MAC

Submitted: April 30th, 2019

Advisors: Professor Kevin Sweeney (BUS) and Professor Marcel Blais (MA)

Project Sponsor: State Street Global Services

Table of Contents

I. Abstract....3
II. Executive Summary....4
III. Introduction....8
IV. Background....10
State Street Corporation....10
Identifying Digital Identity....12
Purpose of Digital Identity....12
Importance of Digital Identity....12
Case Studies....13
Target....13
Marriot....15
Mastercard....16
V. Methodology....16
Defining Digital Identity....17
Developing a Digital Identity Profile....17
Business Process Interviews....17
Supplier Request Process Interview....18
Risk Management Process Interview....18
Supplier Entry Process Interview....19
Initial Data Projections....19
Spend Data Analysis....21
VI. Results and Analysis....22
Digital Identity Definition....22
Definition....22
Requirements....22
Digital Identity Profile....23
Profile specific to a business:....23
Business Process Flow Diagram....23
Tableau Dashboard Prototype....24
Python Analysis....26

Excel Analysis 27

Project Management Analysis 31

Data Gathering Methods 31

Team Strengths Utilization 33

Project Method Analysis 33

VII. Recommendations 34

Digital Identity Recommendations 34

Business Process Recommendations 35

Topics for Future Projects 36

Project Management Recommendations 36

VIII. Conclusion 37

IX. Works Cited 38

I. Abstract

This project focused on understanding digital identity to improve State Street Global Services' supplier onboarding and vendor identification process. Our interdisciplinary, combined graduate and undergraduate student team began by researching digital identity and conducting subject matter expert interviews to map out business processes. Using Python and Excel we analyzed supplier spend data to detect anomalies. Our team then reviewed the business process and analysis to make recommendations on digital identity usage. We finalized the project by creating a Tableau dashboard prototype for use by State Street for risk analysis.

II. Executive Summary

What is digital identity? Digital identity is typically a collection of tools that allow users to exchange information and authenticate themselves on digital platforms. Think of the tools that you use as an individual to share your information, like credit cards, passports, and drivers' licenses. These all have more information than is needed for individual identity verification. For example, when you want to buy an alcoholic drink from a restaurant, they ask for ID. They need a photo and an age. Typically, you hand them your driver's license which contains additionally your address and driver's ID number. Companies also share this burden when dealing with its information and the information of other businesses in business to business interactions. Boston Financial Services Leadership Council (BFSLC) is partnered with State Street Corporation and Worcester Polytechnic Institute as a part of a larger collaborative in the Boston area. This partnership currently focuses on digital identity in procurement.

We conducted this project in two phases, both with interdisciplinary teams of graduate and undergraduate students. Phase 1 had a business process focus and ran from September to December 2018. We focused on data analysis and digital identity development in Phase 2. Phase 2 built off Phase 1's results and worked from January to April 2019.

State Street is a global financial services company that is responsible for "more than 10%" of the world's assets (About | State Street, n.d.). State Street operates in more than 100 markets internationally. We worked with one of State Street Corporation's business units, State Street Global Services. This unit deals primarily with core custody, accounting, fund administration, shareholder recordkeeping, and procurement operations. Supplier Hub is State

Street’s current Oracle-based supplier information storage tool. It stores information like: addresses, category of company, banking information, etc. Archer is its risk management tool that sources its information from the Supplier Hub and an Inherit Risk Questionnaire (IRQ). From the World Economic Forum, it serves as a means for: exchanging user attributes, authentication, capturing user attributes, and developing a standard for system operation. Fraud is on the rise with 15.4 million US victims of ID fraud in 2016. Digitally connected consumers are 30% more likely to be victims of fraud (Pascual, Marchini, Miller, 2017). Target and Marriot are case study examples of companies being reactive with their digital identity implementation. The Mastercard case study example is an instance of proactive digital identity development.

We defined digital identity, developed a digital identity profile, conducted business process interviews, completed our initial data projections and analysis, and developed spend data analyses.

Digital Identity Definition:

A “digital identity” serves as a unique identifier for an individual, organization, or business on a digital platform. This identity can be used in transactions, communication, and other activities that require authentication.

Digital Identity Profile for Businesses:

This profile is split into uniform and additional elements. The uniform elements can be applied to all businesses while the additional elements provide additional insight into a company based on what the contractor wants to know about a vender in the case of procurement or other information needed in the financial services industry specifically.

Uniform elements of a digital identity include:

- Unique ID number
- Name as identified in tax documentation
- Headquarters address
- SIC code

Additional elements of a digital identity include:

- Related companies (ID, parent, child, etc.)
- Risk rating

Figure 6 on page 27 shows our Python analysis of State Street's vendor spend data. To detect anomalies, we graphed the top spending vendors for different years.

Additionally, we created a Tableau dashboard prototype using projected data. This is shown in Figure 3 on page 26 below. This is to visualize vendor data in a geospatial platform to aid in risk analysis.

From this analysis and research, we created a set of recommendations for State Street Global Services. The recommendations are listed below sorted by category:

Digital identity recommendations

1. Utilize the digital identity profile and integrate this into the Supplier Hub.

2. Integrate the Archer platform, a comprehensive risk rating tool, functionality into Supplier Hub to include the risk rating into the Supplier Hub.
3. Continue to work with the BFSLC to drive financial services growth in the Boston area.

Business process recommendations

1. Enhance training and workflow documentation for procurement employees on the supplier onboarding process from contracting to payment.
2. Incorporate the ISRMP (Information Security Risk Management Procedure) as a procurement tool post-IRQ check.
3. Expand risk management operations to incorporate risk adjustments using a real-time geospatial dashboard.

Topics for future projects

Additional research could be conducted in these areas of study:

1. Risk-related spend data analysis,
2. Machine learning algorithms, and
3. Real-time risk data analysis.

III. Introduction

What is digital identity? Digital identity is a tool for users to exchange information and authenticate themselves on a digital platform. Think of the tools that you use as an individual to share your information. Credit cards, passports, and tax documentation all contain too much information for what they are used for. For example, when you want to buy an alcoholic drink from a restaurant, they ask for ID. They need a photo and an age. Typically, you hand them your driver's license which contains additionally your address and driver's ID number. You also cannot use something like a Facebook profile to verify your age to the government. Individuals struggle to identify themselves on digital platforms. Companies also share this burden when dealing with its information and the information of other businesses in business to business interactions. This project addresses this problem and offers a solution.

The BFSLC continues to partner with State Street Corporation and Worcester Polytechnic Institute to research digital identity and develop a universal tool. The BFSLC "brings together CEOs and senior executives from the Boston financial services sector with academic partners to advocate for the sector in Massachusetts" (Boston Financial Services Leadership Council, n.d.). The BFSLC is also working with two other companies, Liberty Mutual and the Boston Federal Reserve, and two other academic institutions, UMass Lowell and Northeastern, to address the same issue. There is an opportunity for the Boston area to pioneer a digital identity solution for the nation, because of the available corporate dedication and institutional resources.

A streamlined, uniform digital identity is essential to operate in the financial services industry. Digital identity in procurement needs a change. It is inconsistent between platforms, costly to maintain, difficult to implement internationally, and leaves users on both sides of procurement transactions vulnerable to fraud and malicious activities. As technology improves, so should the digital identity system to provide adequate protection for customers of the industry. The issue of data identity and data security is closely tied with rising privacy concerns in society. Individuals want to know that their data and transactions are secure. To satiate their customers, companies must look towards more complex digital identity solutions.

This document will describe Worcester Polytechnic Institute's involvement in the project from the fall of 2018 to the spring of 2019. There were two phases of the project involving two different teams both including a mix of graduate and undergraduate students. Lisandra Lao (an undergraduate Mathematical Sciences student) and I were involved in both phases of the project. Two interdisciplinary graduate student teams also participated in the Fall 2018 and Spring 2019 academic semesters. The Phase 1 combined team worked from September to December 2018 and included Lisandra and me plus five graduate students from the following disciplines: computer science, business, and data analytics. Phase 1 had a focus on how digital identity affects its current business processes and how improvements in digital identity could streamline or automate some of the processes. Phase 2 built off the Phase 1 team's results. The Phase 2 team worked from January 2019 until April 2019 and had a similar mix of disciplines to Phase 1. Phase 2 had a data analytics focus since we received spend data from the sponsor at the beginning of Phase 2. This experience was invaluable and unique to other project opportunities that I have worked on through my college career. This mix of disciplines and experience levels reflect project work done in the industry between coworkers of varying experience levels and departments.

IV. Background

Before addressing the topic of digital identity, we conducted research on State Street to ensure that our suggested solutions align with State Street's business strategy, processes, and operations. We then investigated the concept of digital identity, its fundamental purpose, and its importance in the context of the financial sector procurement. To frame digital identity in a corporate context, we examined case studies of successful and unsuccessful digital identity implementations.

State Street Corporation

State Street is a global financial services company that is responsible for "more than 10%" of the world's assets (About | State Street, n.d.). State Street operates in more than 100 markets internationally. State Street Corporation consists of four separate business units:

- State Street Global Advisors,
- State Street Global Markets,
- State Street Global Services, and
- State Street Global Exchange.

State Street Global Advisors provides investment guidance and is the "third largest asset manager in the world" (State Street Global Advisors, n.d.). State Street Global Markets assists customers in managing their portfolios and is based in 30 markets. (Global Markets | State Street Corporation, n.d.). State Street Global Services is the entity with which this project worked with primarily. It covers core custody, accounting, fund administration, shareholder recordkeeping and procurement operations (Global Services | State Street, n.d.). State Street

Global Exchange helps its clients manage risk and decide on business strategies (Global Exchange | State Street, n.d.).

The diversity of State Street Corporation's operations provides unique challenges when communicating between digital systems. Many State Street acquisitions have left the company operating on multiple legacy systems internationally. One of State Street's medium-term strategic priorities as outlined in its 4Q18 earnings presentation is to "generate structural expense saves... through further efficiency and digitization initiatives" (Investor Relations | State Street, n.d.). State Street Corporation is looking for efficiency in its process and the technology to enable this.

This project evaluates State Street Global Services' Vendor Onboarding and Procurement Process. This process is facilitated, in the United States, through the Oracle system, Supplier Hub. Supplier Hub stores information such as: supplier addresses, contact information, category of company or product purchased, banking information, attributes, payment details, invoice management, and a tolerance for invoice or payment amount. To validate suppliers, the Dun & Bradstreet tool, Hoovers is used. Also, there exists a separate platform, Archer, to check the inherit supplier risk with a rating of low, medium, and high. A D_U_N_S #, a unique 9-digit identifier used by Dun & Bradstreet, is used to associate parent-child relationships within the Supplier Hub. This is helps identify companies for anti-bribery anti-corruption initiatives within State Street Global Services. Identifying these relationships can help prevent malicious transactions within the company.

Identifying Digital Identity

Digital identity is typically a collection of tools that allow users to exchange information and authenticate themselves on digital platforms. These tools often require certain information such as passwords, ACH (Automatic Clearing House) information, or pseudo-digital methods such as photographs of driver's licenses or other physical IDs (World Economic Forum, 2016). This information acts as proof that the individual is valid, like how identity operates outside of the digital world. However, digital identity faces more challenges than physical identity because it lacks the face-to-face interaction that builds trust between the operating parties. Secure digital identity, being a relatively new business need, presents opportunities to gain a competitive advantage for companies if they can implement it correctly.

Purpose of Digital Identity

Digital Identity facilitates many kinds of activities such as financial transactions, communication, and federal interactions. With many government and corporate services moving to the digital space, these entities need methods of identifying its customers through its digital platforms. Digital identity serves as a way for companies to deliver its services, authorize users, provide a means for exchanging attributes, authenticate users, capture and store user attributes, and develop a standard for system operation (World Economic Forum, 2016). A comprehensive digital identity facilitates all of these purposes.

Importance of Digital Identity

A digital identity also serves as a protection system for these facilitated transactions. Digital identity is essential to the financial services industry because the financial information collected by these companies can be used in fraudulent activities to hurt its customers. Without a secure digital identity tool, a financial services company risks major identity theft opportunities. Fraud is on the rise with 15.4 million US victims of ID fraud in 2016, 2 million more affected than in 2015. Digitally connected consumers, those who frequently shop online and utilize social networks, are 30% more likely to be victims of fraud (Pascual, A., Marchini, K., & Miller, S., 2017). With an increasingly digital world, fraud has found a way to connect to more consumers through outdated company platforms and gaps in security. As Al Pascual, senior vice president, research director, and head of fraud & security from Javelin Strategy & Research, states, "To successfully fight fraudsters, the industry needs to close the security gaps, continue to improve and consumers must be proactive." Incidents where a company is at fault for fraud can be costly and hurt a company's image for years. There exists both a social and fiscal need for implementing a uniform, secure digital identity tool.

Case Studies

In order to frame digital identity in a corporate context, we evaluated case studies of companies who have both suffered from poor digital identity protection and those who are being progressive in implementing them. Two cases, Target and Marriot, are examples where customer information was stolen because of poor preventative measures. The Mastercard case is an example of a company looking to be proactive with implementing digital identity tools.

Target

In January of 2014, Target announced that during the 2013 holiday season it had a data breach that affected more than 70 million customers. This data breach included debit and credit card information as well as personal information such as names, addresses, and phone numbers. The size and information types gathered from this data breach ranks it as one of the worst data breaches ever. This exposes all those individuals to identity theft because of the amount of information stolen. With financial and personal information together, it is much easier to fake the victim's identity (Yang, J. L., & Jayakumar, 2014). The targeting of individuals during the holiday season show that these data hackers are aiming to impact the most people possible and are tactical in their approach. This kind of targeting is something that companies need to be aware of when protecting its customers.

This scandal for Target was very costly with its fourth quarter earnings forecasting a decline in sales by 2.5%. Target's bottom line was hit from the legal backfire from the scandal as well with banks demanding reparations for issuing new cards and shoppers filing class-action lawsuits. "It's a little frightening. These bad guys are getting into some of the most secure retailers' networks, and I'm sure it's not going to stop at Target," [Avivah] Litan [a fraud and security analyst at Gartner, a research firm] said. "We need a fundamentally different paradigm here for how we manage security"" (Yang, J. L., & Jayakumar, 2014).

Target in response to the scandal emailed those affected by the crisis and provided one year of free credit monitoring and identity theft protection to all shoppers. Target also publicly stated that customers aren't liable for fraudulent charges because of the breach. The company also offered a 10% off all in-store purchases after the attack (Yang, J. L., & Jayakumar, 2014). In Figure 1 below, Target's stock price from 2013 to 2015 is shown. The stock price drops to a low at $56.06 on 2/10/2014 after the scandal broke out. However, the company recovers going into 2015 to a level greater than before the scandal. This could mean that Target's methods of reparations to victims healed its public image. In 2017, Target paid $18.5 million dollars to settle investigations from the 2013 breach (Bloomberg, 2018).

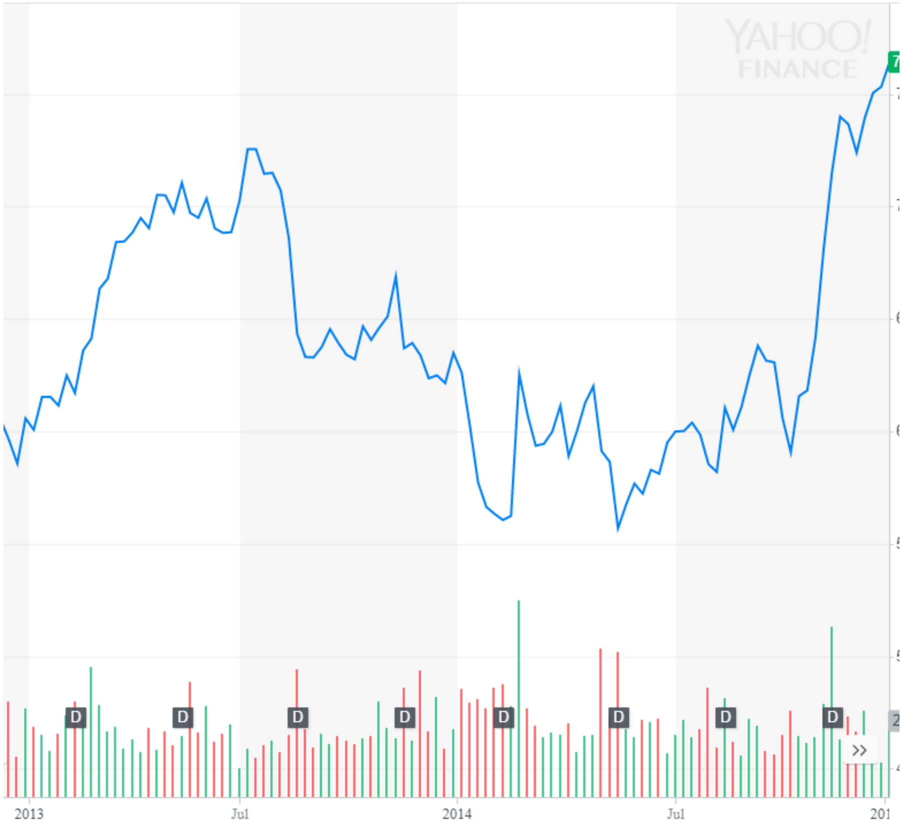


Figure 1: Target Stock Price from 1/1/2013 to 1/1/2015 (Yahoo Finance)

Marriot

In Marriot's Starwood entity, an estimated 500 million customers may have been affected by a data breach. Of those 500 million, 327 million of them had data stolen including: passport numbers, emails, mailing addresses, and potential credit card details. This breach affects customers who made reservations at Starwood properties on or before Sept 10. 2018 (Bloomberg, 2018). This is a relatively new event, so the exact severity of the issue is unknown. This is the second largest known data breach ever and will likely result in major financial losses for Marriot as they pay out legal fees. The company did state that the stolen credit card data was encrypted but it is still possible that the hackers could decrypt them with the other information that was stolen (Bloomberg, 2018).

Mastercard

Mastercard recently partnered with Microsoft to evaluate and improve how people use digital identity. Currently, verifying identity online is dependent on physical or digital proof managed by a central party. As stated in the above background, digital identity needs to be improved because of the risk of fraud and complexity. Mastercard and Microsoft are working towards a secure, instant way to verify digital identity with whomever, whenever (Mastercard, Microsoft Join Forces to Advance Digital Identity Innovations, 2018). Its plan involves a service that would allow individuals to enter, control and share their identity data on multiple devices. Mastercard is working to utilize Microsoft Azure, Microsoft's cloud platform, to build its tool. Mastercard identifies the business need that a digital identity tool like this satisfies, "Today's digital identity landscape is patchy, inconsistent and what works in one country often won't work in another. We have an opportunity to establish a system that puts people first, giving them control of their identity data and where it is used," says Ajay Bhalla, president, cyber and intelligence solutions, Mastercard" (Mastercard, Microsoft Join Forces to Advance Digital Identity Innovations, 2018).

V. Methodology

We defined digital identity, developed a digital identity profile, conducted business process interviews, completed our initial data projections and analysis, and developed spend data analyses. We conduct two different data analyses because we received additional data from the sponsor at the beginning of Phase 2.

Defining Digital Identity

We have kept the definition of digital identity simple but comprehensive. A short definition is easy to convey and interpret. To supplement the short definition, we provide additional requirements. These requirements further explain the definition and evaluate on the specific needs. Both the requirements and definition apply for both businesses and individuals.

Developing a Digital Identity Profile

A digital identity profile is a tool that companies, or individuals, can use to represent themselves digitally. It contains relevant information to whatever purpose they are endeavoring toward. We developed a business digital identity profile that fits State Street Global Services' needs. We developed this tool with information gathered from interviews with State Street employees and research into available identification tools. We decided that there should be a set of uniform elements between businesses and then a set of additional elements to the digital identity profile unique to the specific business or industry. These additional elements can be as numerous or few as needed, however too many elements can become confusing and cumbersome.

Business Process Interviews

In Phase 1, we focused on evaluating the business process to identify areas that could be improved with a better digital identity tool. To map the business processes, we conducted three major interviews with subject matter experts (SME) in the areas of: supplier request and onboarding, risk management, and supplier entry. These three major process steps gave us a glimpse into the operations of State Street Global Services to see how digital identity currently plays a role in the business and how it could be improved in the future.

For each interview, we developed an agenda with four primary questions:

- What is the goal of a successful outcome?
- Explain your process?
- What challenges have you faced?
- Describe your “wish list” for your job/process?

We followed the same methodology of four questions in each interview with specifics varying by business area. The specific questions for each interview are listed below.

Supplier Request Process Interview

- Goals: What are the ideal outcomes of successful supplier onboarding?
- Process: Walk us through the steps of the supplier onboarding into the internal network, and discuss the parties involved in this process
- Challenges: What are pain points in the current process and how do you and your colleagues work around them?
- Wishlist: What are ways the process could be improved/streamlined/automated?

Risk Management Process Interview

- Goals: What are the ideal outcomes of a successful new supplier onboarding?
- Process: Walk us through the steps of the ongoing screening process and what risk management steps are taken.

- Challenges: What are pain points in the current process and how you get around them?
- Wishlist: What are ways the process could be improved/streamlined/automated?

Supplier Entry Process Interview

- Goals: What is the ideal outcome of a successful new supplier onboarding? A successful update of an existing supplier?
- Process: Walk us through the steps of the new supplier update/entry process within Oracle.
- Challenges: What are pain points in the current process and how you get around
- them?
- Wishlist: What are ways the process could be improved/streamlined/automated?

Initial Data Projections

Prior to the authorization for the spend data from State Street Corporation, we created our own spend projection data to judge what future analysis would look like. We created this data in excel using the following fields:

- Vendor #
  - A unique identifier integer (auto numbered 1-20 in our projected data)
- Vendor Rank (1-High Profile, 10- Low Profile)
- Vendor Name
- Region
  - US, EU, EMEA
- Billing Address

- Billing City
- Billing State
- Billing Zip Code
- Billing Country Code
- Invoice #
    - Unique ten-digit integer
- Invoice Date
- Source
    - Sourceable and non-sourceable supplier relationship. A sourceable relationship is one where State Street and the supplier can negotiate pricing, e.g. computers. A nonsourceable relationship is one where State Street and the supplier cannot negotiate, and the pricing is fixed, e.g. taxes.
- Due Date
- Invoice Amount
- Status
    - The status of the invoice; overdue, closed, and open in the data.
- Amt Paid
    - The amount paid so far by the supplier.
- Check #
- Check Date
- Amount Due/Balance
- Remarks

  - Text box for additional comments on the relationship or payments.

We created a Tableau dashboard prototype to illustrate this data in Phase 1 of the project. Tableau is an interactive data visualization platform. We chose Tableau as a medium for this visualization because of State Street Global Services' prior use of Tableau in metrics reporting. We created this dashboard with a focus on profile analysis, spend analysis, and geospatial awareness.

Spend Data Analysis

At the beginning of the Phase 2, we were given global procurement spend data from State Street Corporation to analyze. The data ranged from FY 2016 to Oct 2018. The data contained the following fields:

- Taxonomy Number
  - Unique Code required for Category Mapping
- Month
- Year
- Region
  - Unique Code required for Region Mapping
- Supplier Parent Code
  - Unique Code required for Supplier Parent Mapping
- Supplier Child Code
  - Unique Code required for Supplier Child Mapping
- Spend

To analyze the data, we decided to use both a Python script to visualize the data and Excel pivot tables. To look at unique suppliers we combined the parent and child code. We wanted to look at the top spenders, the spread of total spend data, and frequency of spending. The Excel analysis was limited because of the size of the data so we did the Excel analysis on a subset of this data.

VI. Results and Analysis

In the section, we will provide an overview of the results of Phase 1 and Phase 2 and our analysis of the critical issues of the project utilizing our digital identity definition, digital identity profile, business process flow diagram, Tableau dashboard, Python analysis, Excel analysis, and a project management assessment.

Digital Identity Definition

Definition

A “digital identity” serves as a unique identifier for an individual, organization, or business on a digital platform. This identity can be used in transactions, communication, and other activities that require authentication.

Requirements

A digital identity must be secure, unique, easy to use, complex, and cross platform.

- The identity must be secure to prevent fraudulent activity.
- The person or business must be the only ones able to access the identity.
- There is only one identity per individual or company.

- This identity must be easy for the individual or company to access and utilize.
- The identification system must be complex enough to prevent fraud but simple enough for the user to access daily.
- The tool must be able to be integrated cross-platform to maximize utility from the user.

Digital Identity Profile

Profile specific to a business:

Each element must be unique to prevent confusion.

Uniform elements of a digital identity include:

- Unique ID number
- Name as identified in tax documentation
- Headquarters address
- SIC code

Additional elements of a digital identity include:

- Related companies
  - ID
  - Relationship (parent, child, etc.)
- Risk rating

Business Process Flow Diagram

Using information from the SME interviews in Phase 1, we created a business process flow diagram. Figure 2 illustrates the supplier onboarding process. The different entities are outlined on the left. The processes move between these entity boxes based on the handoffs in the process. Understanding the business process flow allows State Street Global Services’ to better understand how digital identity could streamline its handoffs and automate some of its processes. We found that the Inherit Risk Questionaire contains elements of the Information Security Risk Management Procedure, creating an overlap of information.

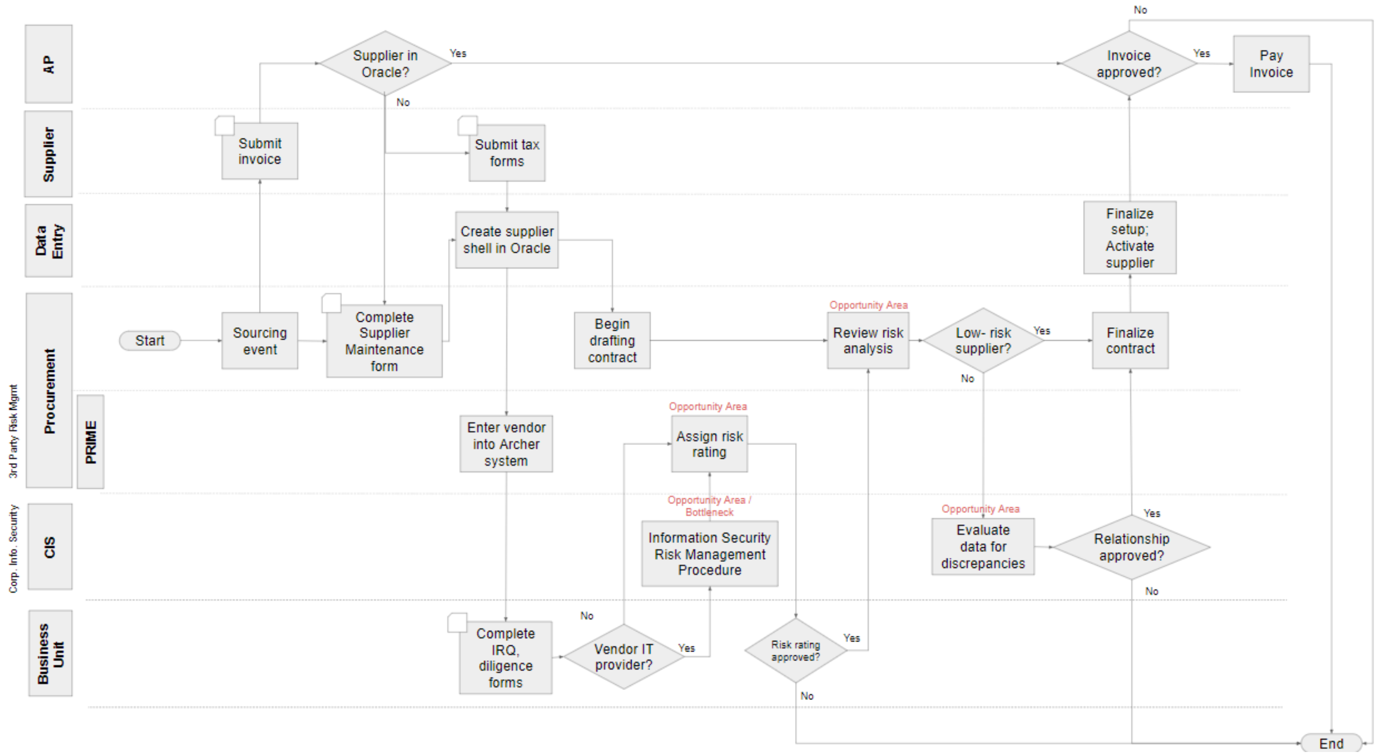


Figure 2: Business process flow diagram

Tableau Dashboard Prototype

Using the projected data, before given spend data from State Street Global Services’, we created a risk analysis dashboard prototype in Tableau. This dashboard allows for the visualization of vendors geospatially and spend analysis. Below in Figure 3, you can see these analyses pictured. Additionally, clicking the vender dot in the map view displays information specific to the vendor, Figure 4 shows an example of this.

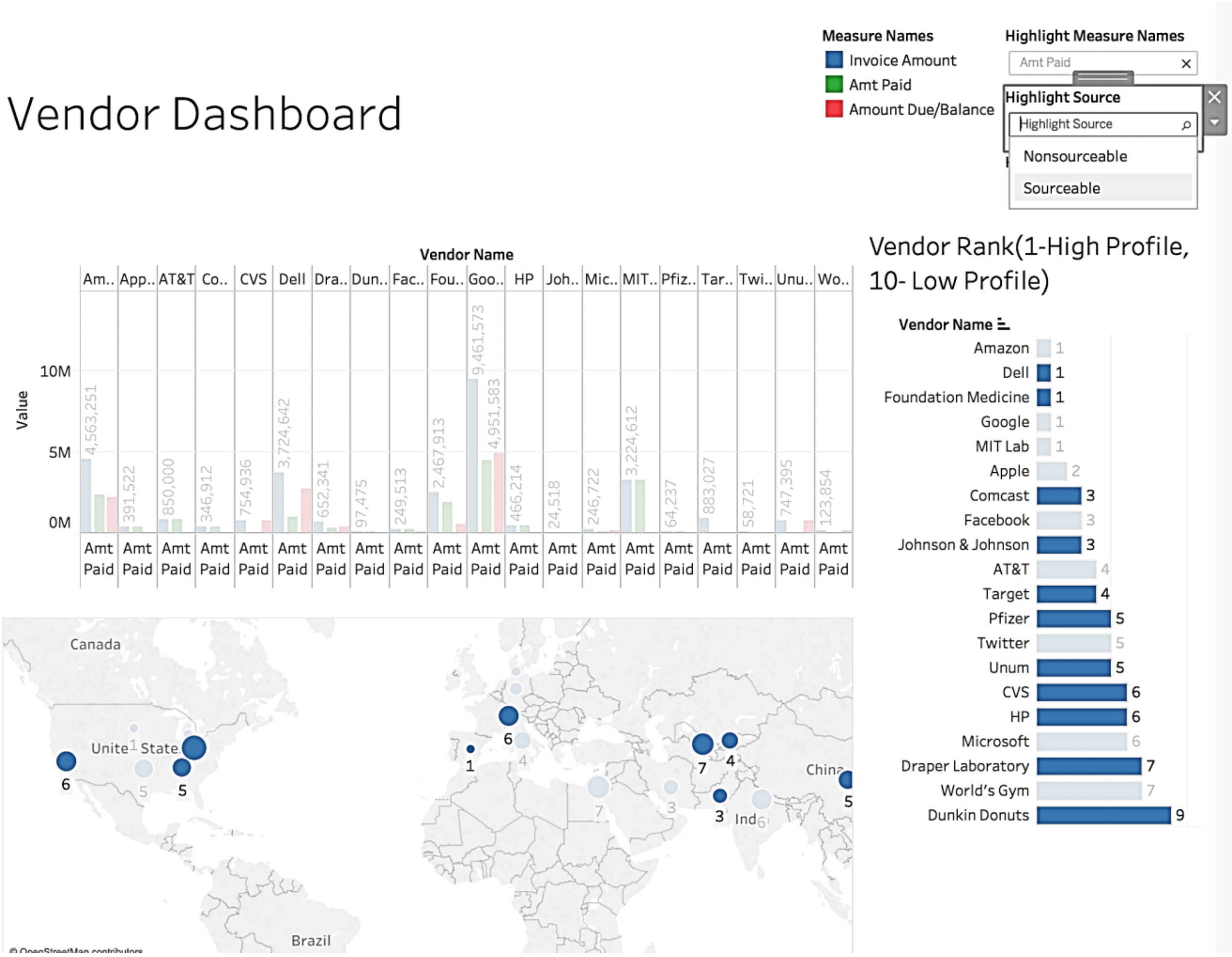
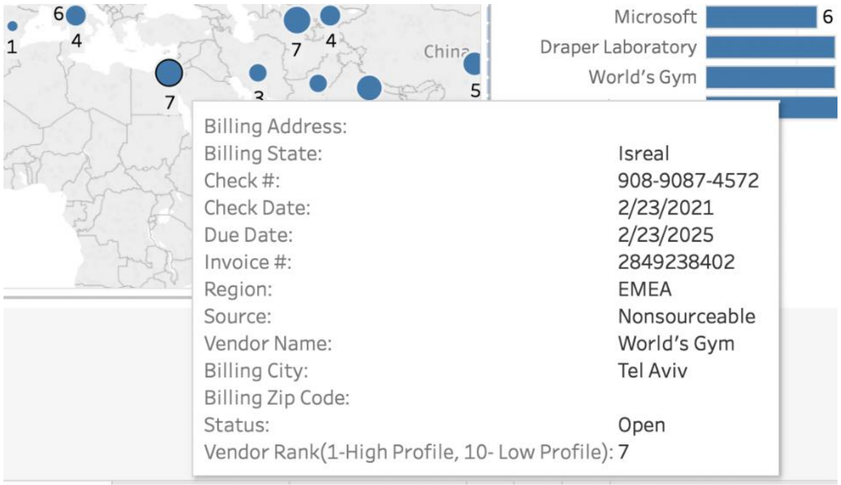


Figure 3: Tableau dashboard prototype

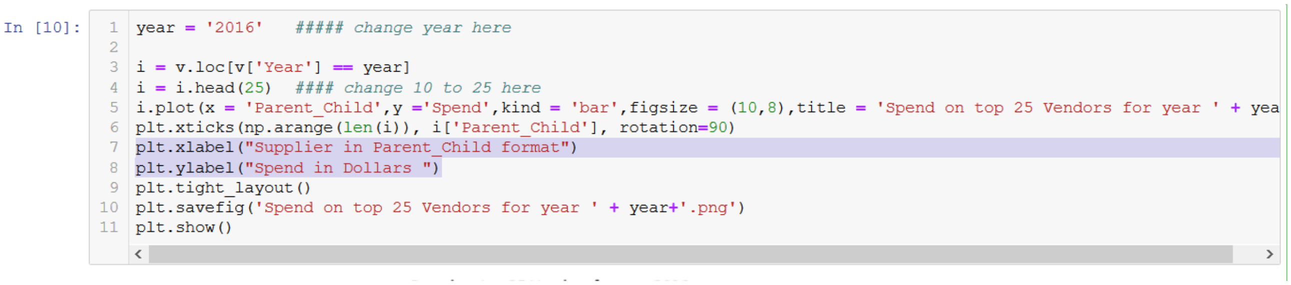


Billing Address:
Billing State: Isreal
Check #: 908-9087-4572
Check Date: 2/23/2021
Due Date: 2/23/2025
Invoice #: 2849238402
Region: EMEA
Source: Nonsourceable
Vendor Name: World's Gym
Billing City: Tel Aviv
Billing Zip Code:
Status: Open
Vendor Rank(1-High Profile, 10- Low Profile): 7

Figure 4: Tableau Dashboard Prototype Information Display

Python Analysis

Because of the size of the data, using a Python code to analyze the data is the most reasonable. Our aim is to look for anomalies in the data, specifically vendors with the largest spend totals. In Figure 5 we show the Python code to identifying these high spenders. We use a parent-child unique code combination to denote a single vendor. Figure 6 shows the top 25 vendors for the 2018 year using this code.



```
In [10]:
year = '2016'    ##### change year here

i = v.loc[v['Year'] == year]
i = i.head(25)   #### change 10 to 25 here
i.plot(x = 'Parent_Child',y ='Spend',kind = 'bar',figsize = (10,8),title = 'Spend on top 25 Vendors for year ' + yea
plt.xticks(np.arange(len(i)), i['Parent_Child'], rotation=90)
plt.xlabel("Supplier in Parent_Child format")
plt.ylabel("Spend in Dollars ")
plt.tight_layout()
plt.savefig('Spend on top 25 Vendors for year ' + year+'.png')
plt.show()
```

Figure 5: Python Code Example

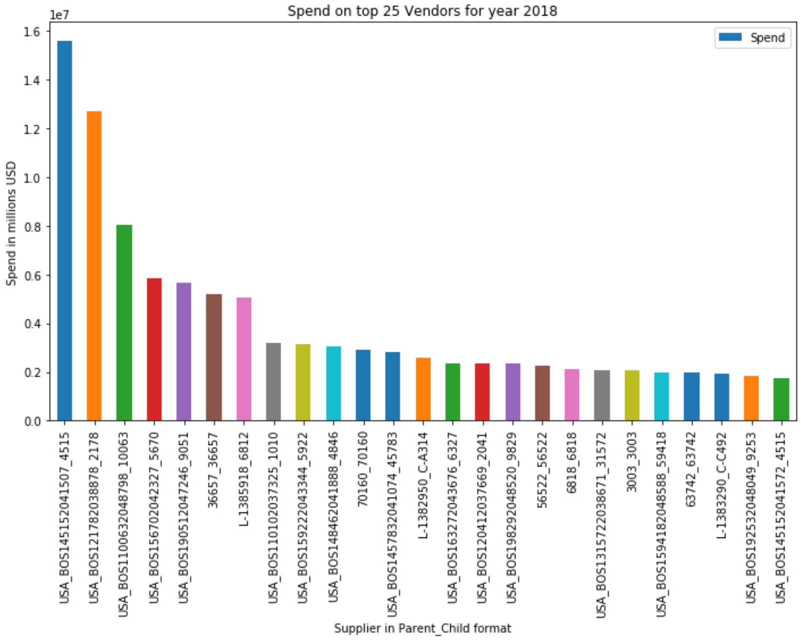
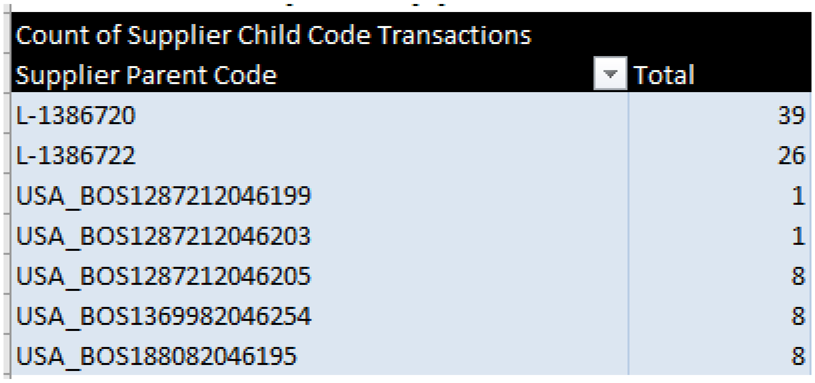


Figure 6: Spend on top 25 venders (2018)

Excel Analysis

Using a smaller, modified version of the original spend data we construct pivot tables in Excel to show various relationships between the data. The relationships that we explore are shown in figures 7-12. We can flag any large variations as anomalies in the data and use this for risk analysis.

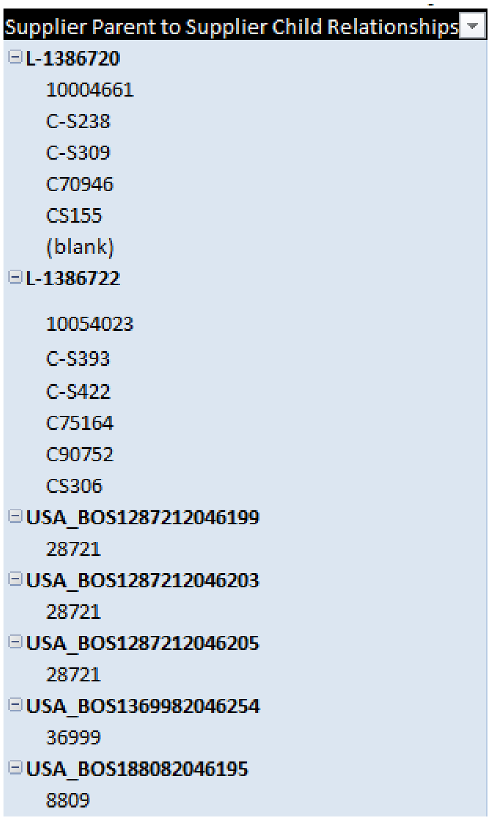
Figure 7 shows the number of transactions per supplier parent code. This accounts for all child companies under this supplier parent code.



Count of Supplier Child Code Transactions	
Supplier Parent Code	Total
L-1386720	39
L-1386722	26
USA_BOS1287212046199	1
USA_BOS1287212046203	1
USA_BOS1287212046205	8
USA_BOS1369982046254	8
USA_BOS188082046195	8

Figure 7: Transactions per supplier parent code

Figure 8 shows the parent to child relationships present in the data. These can be used to see individual unique vendors.

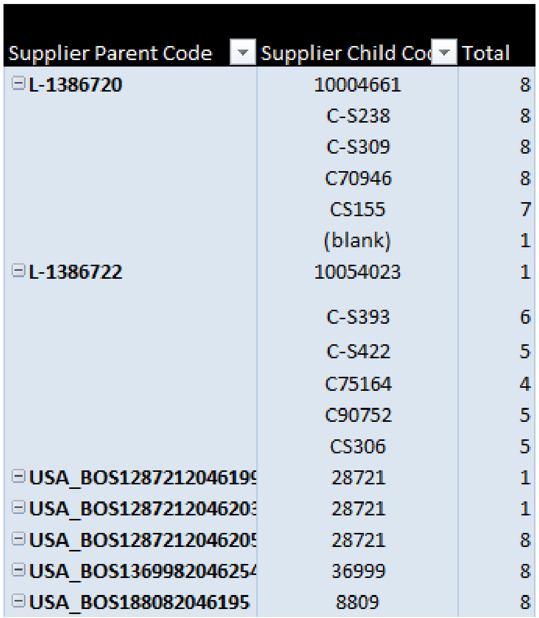


Supplier Parent to Supplier Child Relationships ▾

- ⊟ **L-1386720**
  - 10004661
  - C-S238
  - C-S309
  - C70946
  - CS155
  - (blank)
- ⊟ **L-1386722**
  - 10054023
  - C-S393
  - C-S422
  - C75164
  - C90752
  - CS306
- ⊟ **USA_BOS1287212046199**
  - 28721
- ⊟ **USA_BOS1287212046203**
  - 28721
- ⊟ **USA_BOS1287212046205**
  - 28721
- ⊟ **USA_BOS1369982046254**
  - 36999
- ⊟ **USA_BOS188082046195**
  - 8809

Figure 8: Parent to child relationships

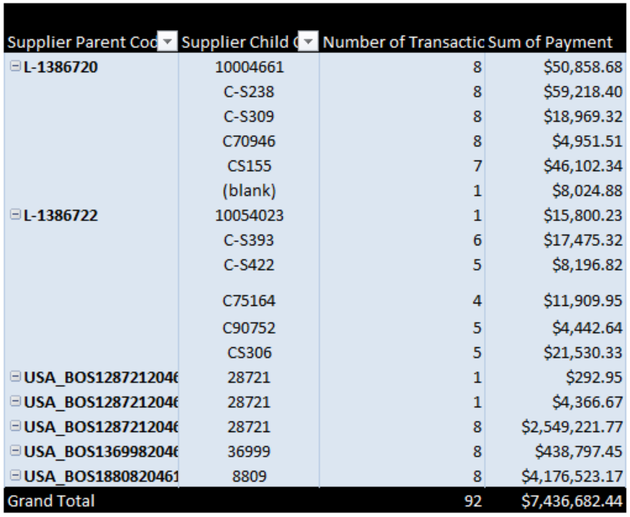
Figure 9 shows transactions per unique supplier code. This is broken into parent and child companies sorted by highest transaction number.



Supplier Parent Code	Supplier Child Co	Total
⊟L-1386720	10004661	8
	C-S238	8
	C-S309	8
	C70946	8
	CS155	7
	(blank)	1
⊟L-1386722	10054023	1
	C-S393	6
	C-S422	5
	C75164	4
	C90752	5
	CS306	5
⊟USA_BOS1287212046199	28721	1
⊟USA_BOS1287212046203	28721	1
⊟USA_BOS1287212046205	28721	8
⊟USA_BOS1369982046254	36999	8
⊟USA_BOS188082046195	8809	8

Figure 9: Transactions/supplier child code

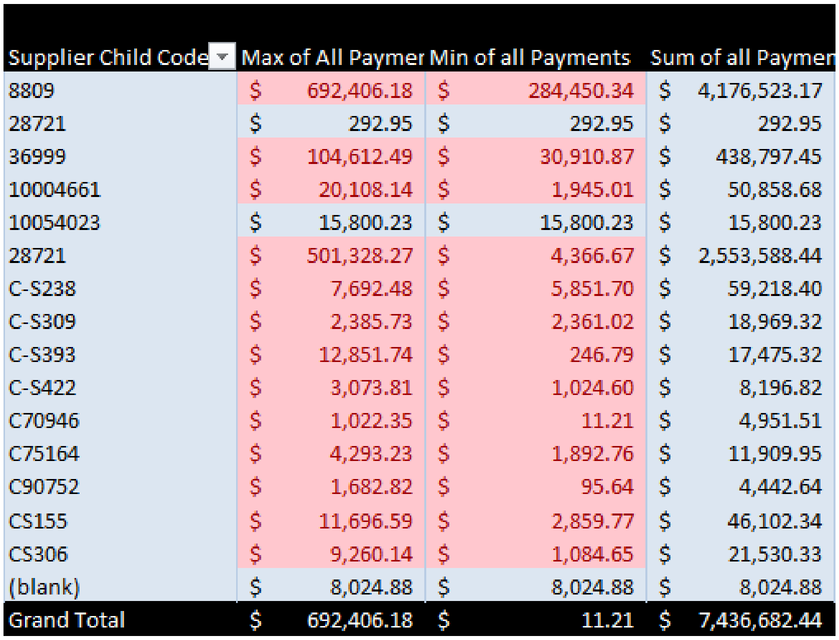
Figure 10 shows the number of transactions and total payment per unique supplier code. This is also broken into parent and child companies sorted by highest transaction number.



Supplier Parent Cod	Supplier Child C	Number of Transactic	Sum of Payment
⊟L-1386720	10004661	8	$50,858.68
	C-S238	8	$59,218.40
	C-S309	8	$18,969.32
	C70946	8	$4,951.51
	CS155	7	$46,102.34
	(blank)	1	$8,024.88
⊟L-1386722	10054023	1	$15,800.23
	C-S393	6	$17,475.32
	C-S422	5	$8,196.82
	C75164	4	$11,909.95
	C90752	5	$4,442.64
	CS306	5	$21,530.33
⊟USA_BOS1287212046	28721	1	$292.95
⊟USA_BOS1287212046	28721	1	$4,366.67
⊟USA_BOS1287212046	28721	8	$2,549,221.77
⊟USA_BOS1369982046	36999	8	$438,797.45
⊟USA_BOS1880820461	8809	8	$4,176,523.17
Grand Total		92	$7,436,682.44

Figure 10: Number of transactions & payment total per supplier child code

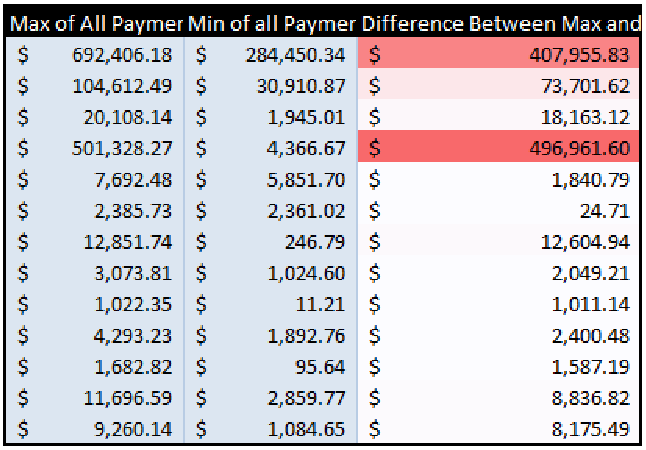
Figure 11 shows the supplier child codes and the maximum and minimum payment made by each. This table also shows the sum of all payments made by a child supplier.



Supplier Child Code	Max of All Paymer	Min of all Payments	Sum of all Paymen
8809	$ 692,406.18	$ 284,450.34	$ 4,176,523.17
28721	$ 292.95	$ 292.95	$ 292.95
36999	$ 104,612.49	$ 30,910.87	$ 438,797.45
10004661	$ 20,108.14	$ 1,945.01	$ 50,858.68
10054023	$ 15,800.23	$ 15,800.23	$ 15,800.23
28721	$ 501,328.27	$ 4,366.67	$ 2,553,588.44
C-S238	$ 7,692.48	$ 5,851.70	$ 59,218.40
C-S309	$ 2,385.73	$ 2,361.02	$ 18,969.32
C-S393	$ 12,851.74	$ 246.79	$ 17,475.32
C-S422	$ 3,073.81	$ 1,024.60	$ 8,196.82
C70946	$ 1,022.35	$ 11.21	$ 4,951.51
C75164	$ 4,293.23	$ 1,892.76	$ 11,909.95
C90752	$ 1,682.82	$ 95.64	$ 4,442.64
CS155	$ 11,696.59	$ 2,859.77	$ 46,102.34
CS306	$ 9,260.14	$ 1,084.65	$ 21,530.33
(blank)	$ 8,024.88	$ 8,024.88	$ 8,024.88
Grand Total	$ 692,406.18	$ 11.21	$ 7,436,682.44

Figure 11: Maximum and minimum payments per supplier child code

Figure 12 shows the difference between maximum and minimum payments for each supplier. The figure uses the same suppliers in the order shown in figure 11.



Max of All Paymer	Min of all Paymer	Difference Between Max and
$ 692,406.18	$ 284,450.34	$ 407,955.83
$ 104,612.49	$ 30,910.87	$ 73,701.62
$ 20,108.14	$ 1,945.01	$ 18,163.12
$ 501,328.27	$ 4,366.67	$ 496,961.60
$ 7,692.48	$ 5,851.70	$ 1,840.79
$ 2,385.73	$ 2,361.02	$ 24.71
$ 12,851.74	$ 246.79	$ 12,604.94
$ 3,073.81	$ 1,024.60	$ 2,049.21
$ 1,022.35	$ 11.21	$ 1,011.14
$ 4,293.23	$ 1,892.76	$ 2,400.48
$ 1,682.82	$ 95.64	$ 1,587.19
$ 11,696.59	$ 2,859.77	$ 8,836.82
$ 9,260.14	$ 1,084.65	$ 8,175.49

Figure 12: Difference between maximum and minimum payments

Project Management Analysis

The management of this project was unique because our Phase 1 and Phase 2 groups both had a student project manager separate from the advisors leading the groups. In both Phase 1 and Phase 2 the student was pursuing their MBA and had relevant work experience. This produced a unique project experience that mimicked projects in a company where coworkers of different departments and experience levels come together to solve a problem. Below is some analysis on our data gathering methods, team strengths utilization, and project method analysis.

Data Gathering Methods

Below is an analysis of the data gathering methods we used and their effectiveness. I discuss our interviews, team communication, and authorization process.

Interviews

We conducted several interviews throughout the two phases. The most notable were the SME interviews conducted at the end of Phase 1. Our approach to these was to send an agenda out multiple days prior to the meeting with our list of questions, list of attendees, and meeting information. We conducted the interview as a pair with one individual acting as the head interviewer while the other people took detailed minutes. We found that this was effective since one person was free to engage in the dialogue between the attendees and provoke meaningful follow-up questions, while the other focused on taking meaningful notes.

Team Communication

During Phase 1 of the project most of our communication occurred through Basecamp, a web-based project management tool that “helps you increase accountability, communicate more efficiently, and keep everyone on the same page” (How it Basecamp works, n.d.). This was effective, and we continued to use this tool into the second phase of the project; however, we used it to a lesser extent. Basecamp allowed any user to start a discussion on a certain topic and other members could reply to this discussion whenever. Basecamp also sent out email notifications with the posting of a discussion. It also had the functionality to store files within the project. Every week, we had a weekly meeting with the advisors to discuss work that had been accomplished and the anticipated future deliverables. This was effective in keeping the team on track with deadlines and allowed for easy question-asking.

In Phase 2 of the project, the preferred method of communication between members was text message and email. This was less effective since it was not one standard communication method. We also had a weekly meeting in Phase 2; however, this meeting was at a different time where the advisors could not be present. This was a less effective meeting method since we could not get direct feedback from the advisors every week and more meetings had to be set up to get advisor feedback.

Data and File Authorization

The primary method for data sharing was Box.com. This is a “Cloud Content Management” Platform (Secure File Sharing, Storage, and Collaboration, 2016). This data sharing method was effective to an extent. Many users did not have access to the data for a while and when they received access to view they could not download any of the files. Special access had to be given to some users to download this data for analysis.

Team Strengths Utilization

This section outlines our tactics for optimal teamwork and strengths utilization. I discuss the division of work and differentiation of work.

Division of Work

The division of work in both projects varied throughout the phases. We had periods of time where most of the work was on one or two members and the other members would have to wait for them to complete their work and hand it off. Additionally, we were at times waiting on receiving more data or responses from the sponsor. If we had a more consistent work schedule throughout both phases, we could have accomplished more of our goals.

Differentiation of Work

In both phases of the project, we had team members who were more technical and team members who had more of a business focus. This caused a divide in a lot of the work that we were doing. If the team had evenly shared technical and business responsibilities, we could have all gained more knowledge in those areas.

Project Method Analysis

This section is an analysis of our project design methods. The method that best fit our approach was prototyping or throwaway prototyping.

Prototyping/Throwaway Prototyping

The method of prototyping is to develop a small version of a product or deliverable to test or share for feedback. In throwaway prototyping, this product is often scrapped completely and the new feedback and planning lead to the creation of another prototype. Our project design methods in both phases followed one of these processes. We would develop a prototype of a deliverable, get feedback on the prototype, either from an advisor or sponsor, and then build off the prototype or redesign the deliverable completely. I found that this style did work well for the team and the style of the project. This project design method did however cost us time in between prototype reviews.

VII. Recommendations

We created a set of recommendations for State Street Global Services based on the research and analyses that we conducted in both Phase 1 and Phase 2 of the project. The recommendations are broken into four groups: Digital identity recommendations, business process recommendations, and topics for future projects. Finally, there is a set of project management recommendations for future student project teams.

Digital Identity Recommendations

We developed three recommendations for State Street Global Services focused on digital identity implementation and systems. These recommendations are as follows:

1. Utilize the digital identity profile and integrate this into the Supplier Hub.
2. Integrate the Archer platform functionality into Supplier Hub, by including risk rating into the Supplier Hub, to standardize information sources.

3. Continue to work with the BFSLC to drive financial services growth in the Boston area.

The utilization of the digital identity profile will simplify the information found in the Supplier Hub. Additionally, adding the risk rating into the Supplier Hub platform coincides with the integration of the Archer platform into Supplier Hub. This will standardize the sources of supplier information. Finally, we believe that State Street should continue its work with the Boston Financial Services Leadership Council to enhance both its digital identity efforts and the Boston-area's.

Business Process Recommendations

We created three recommendations for State Street Global Services focused on its current business process for supplier onboarding. The recommendations are listed below:

1. Training and workflow documentation for procurement employees on the supplier onboarding process from contracting to payment.
2. Incorporate the ISRMP (Information Security Risk Management Procedure) as a procurement tool post-IRQ check.
3. Expand risk management operations to incorporate risk adjustments using a real-time geospatial dashboard.

We discovered, through talking with State Street personnel, that some inconsistencies exist in the supplier onboarding process. To standardize this process, we suggest that there should be additional training and workflow documentation for procurement employees on the supplier onboarding process from contracting to payment. Additionally, incorporating the ISRMP into the procurement process would help avoid information overlap between that and the IRQ.

Also, we encourage the development of a geospatial risk-management tool using real-time data. Our analysis with Tableau showed that this platform would be a beneficial option to State Street Global Services.

Topics for Future Projects

We encourage State Street Global Services to continue to partner with student groups to explore more options to improve its processes. Some topics for future projects could include:

1. Risk-related spend data analysis,
2. Machine learning algorithms, and
3. Real-time risk data analysis.

Analysis of risk-related spend data could help State Street identify trends in supplier spending and the riskiness of a certain vendor. This could also help develop other trends between higher risk vendors. The Phase 1 graduate student's paper had a strong focus on potential machine learning algorithms to analyze spend data. One such topic also included fuzzy matching, that matching of similarly named suppliers that may be the same. We believe that this could be a topic that State Street could benefit from having a project team work on. Another project team could also investigate third party real-time data to evaluate risk with events such as natural disasters and political unrest. We recommend a tableau visualization for this data.

Project Management Recommendations

We also created a set of recommendations based on project management aimed at reflection and as recommendations for future student projects.

1. Provide a more structured deliverable schedule.
2. Assign unique tasks to each member or group of members for each week.
3. Be persistent in corporate communications to gain authorization quicker and examine what the data needs are prior to asking for authorizations.

We believe that a more structured deliverable schedule would help produce more results, faster throughout the short project timeframe. To fulfill this deliverable schedule each member or small group of members should have an assigned task to complete each week. This task can be specifically suited to the expertise of the member or pair two members of differing experience levels in the topic to complete the task together. This will accomplish more tasks and promote an environment of learning. Additionally, a large struggle in our project was corporate communications. We struggled to get authorization to data during Phase 1 of the project because of sparse corporate communications. We encourage dedicating one team member to communicating with the sponsor during work hours. Also, it is important to be clear on what the data needs are prior to asking for authorization. Determine what is needed, how much, and what will be needed after analysis.

VIII. Conclusion

Digital Identity remains a prominent issue in the financial services industry. For any system that exists, someone knows how to break into it. The responsibility of the company is to protect its customers as much as they can.

The burden of digital identity is currently on the consumer or institutional user. The industry should be working towards a technological solution that relieves some of this burden.

Emerging technologies like blockchain and cloud computing may be essential to creating the digital identity solution of the future. A tool that is easy to use, secure, and informative.

IX. Works Cited

About | State Street Corporation. (n.d.). Retrieved April 10, 2019, from http://www.statestreet.com/about.html

Bloomberg. (2018, November 30). 500 Million Marriott Customers Affected in Data Breach. Retrieved from http://time.com/5467773/marriott-data-breach/

Boston Financial Services Leadership Council. (n.d.). Retrieved April 10, 2019, from http://www.massinsight.com/boston-financial-services-leadership-council/

Global Exchange | State Street Corporation. (n.d.). Retrieved April 10, 2019, from http://www.statestreet.com/solutions/by-capability/ssgx.html

Global Markets | State Street Corporation. (n.d.). Retrieved April 10, 2019, from http://www.statestreet.com/solutions/by-capability/ssgm.html

Global Services | State Street Corporation. (n.d.). Retrieved April 10, 2019, from http://www.statestreet.com/solutions/by-capability/ssgs.html

How Basecamp works. (n.d.). Retrieved April 22, 2019, from https://basecamp.com/how-it-works

Investor Relations | State Street. (n.d.). Retrieved April 10, 2019, from http://investors.statestreet.com/

Mastercard, Microsoft Join Forces to Advance Digital Identity Innovations. (2018, December 3). Retrieved from https://newsroom.mastercard.com/press-releases/mastercard-microsoft-join-forces-to-advance-digital-identity-innovations/

Pascual, A., Marchini, K., & Miller, S. (2017, February 01). 2017 Identity Fraud: Securing the Connected Life. Retrieved April 10, 2019, from https://www.javelinstrategy.com/coverage-area/2017-identity-fraud

Secure File Sharing, Storage, and Collaboration. (2016, March 19). Retrieved April 22, 2019, from https://www.box.com/

State Street Global Advisors. (n.d.). Retrieved April 10, 2019, from https://www.ssga.com/home.html

Target Corporation (TGT) Stock Price, Quote, History & News. (2019, April 10). Retrieved from https://finance.yahoo.com/quote/TGT?p=TGT

World Economic Forum. (2016, August). Disruptive innovation in financial services: A blueprint for digital. Retrieved from https://www.weforum.org/reports/disruptive-innovation-in-financial-services-a-blueprint-for-digital

Yang, J. L., & Jayakumar, A. (2014, January 10). Target says up to 70 million more customers were hit by December data breach. Retrieved from https://www.washingtonpost.com/business/economy/target-says-70-million-customers-were-hit-by-dec-data-breach-more-than-first-reported/2014/01/10/0ada1026-79fe-11e3-8963-b4b654bcc9b2_story.html?noredirect=on&utm_term=.c00a479c5a99