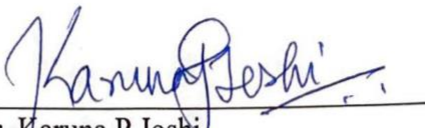


APPROVAL SHEET

Title of Dissertation: A Semantically rich knowledge graph for Mobile Wallets transaction compliance

Name of Candidate: Ankur Nagar
Master's in Information Systems, 2019

Dissertation and Abstract Approved: _____


Dr. Karuna P Joshi
Assistant Professor
Department of Information System

Date Approved: 6/18/2019

ABSTRACT

Title of Document:

***A SEMANTICALLY RICH KNOWLEDGE GRAPH
FOR MOBILE WALLETS TRANSACTION
COMPLIANCE.***

Ankur Nagar, MS IS, 2019

Directed By:

Assistant Professor, Dr. karuna Joshi
Department of Information Systems

Mobile payments are on the rise and as the popularity is growing it's important to understand the regulation framework behind it. Till today, mobile wallets regulations are in the grey area of USA legal policies. There are no such compliance polices which are specific to mobile wallets. Whatever policies are for banking transactions same may apply to mobile payment transactions as well. Thus, making it difficult for the consumer and provider to understand how they are legally bind to such regulations. Banking regulations are large textual document which are currently only available in textual documents and require significant manual effort to ensure their compliance are met. As a first step towards this vision of a holistic mobile wallets compliance knowledge graph, we have created a semantically rich policy-based knowledge representation of the regulations which applies to the mobile payment. In the Ontology, we have also identified the deontic expressions such as Permissions, Obligations from these regulations for consumer & providers. We have evaluated the ontology with qualitative & quantitative measures and validated this Knowledge Graph against the policies of major vendors that deals with mobile payments. This Knowledge Graph, that is available in the public domain, can be used by practitioners to automate mobile wallets transaction compliance in their organization.

A SEMANTICALLY RICH KNOWLEDGE GRAPH FOR MOBILE WALLETS
TRANSACTION COMPLIANCE

By

Ankur Nagar

Thesis submitted to the Faculty of the Graduate School of the
University of Maryland, Baltimore County, in partial fulfillment
of the requirements for the degree of
Master OF SCIENCE IN
INFORMATION SYSTEMS
2019

© Copyright by
Ankur Nagar
2019

This is dedicated to my family and friends

Acknowledgements

I would like to thank my advisor Dr. Karuna P. Joshi for giving me constant guidance and support throughout my course of study and research at UMBC. I am really grateful to Dr. Karuna Joshi for me letting me work under her guidance, motivating & advising me to do quality research. I would like to thank my committee members, Dr. Zhiyuan Chen, Dr. Vandana Janeja for reviewing my thesis. Also, my sincere thanks to Ebiquity and KnACC friends/lab mates for the constant support. Indeed, my experience while doing research has been fruitful and motivational because of faculty and friends of KnACC lab at UMBC. Last but not least, I would like to thank my parents Mr. Dinesh Kumar Nagar and Mrs. Rita Nagar, my sister Ankita, my brother in law Raveen Kumar and my niece Ananya Kumar. Thank you so much for your support and blessings!

Table of Contents

<i>Acknowledgements</i>	<i>iii</i>
<i>List of Tables.....</i>	<i>v</i>
<i>List of Figures.....</i>	<i>vi</i>
<i>Chapter 1: Introduction</i>	<i>1</i>
Section 1: Mobile Wallets.....	1
Section 2: Banking Regulations.....	2
Section 3: Motivation	3
<i>Chapter 2: Related Work</i>	<i>8</i>
Section 1: Semantic Web.....	8
Section 2: Text Extraction.....	9
Section 3: Key regulations for Mobile Payments	10
<i>Chapter 3: Methodology</i>	<i>15</i>
Figure 1: Architecture Flow	16
Section 1: Data Collection.....	16
Section 2: Data Preprocessing.....	17
Section 2.1: Key Term Extraction.....	19
Section 2.2: Deontic Expressions.....	20
<i>Chapter 4: Mobile Wallets Ontology</i>	<i>23</i>
Section 1: Ontology Development	23
Section 2: SWRL Rule	32
Section 3: SPARQL Query	34
<i>Chapter 5: Evaluation & Validation.....</i>	<i>37</i>
Section 1: Evaluation Qualitative:	37
Section 2: Evaluation Quantitative:	38
<i>Chapter 6: UI Development.....</i>	<i>40</i>
<i>Chapter 7: Conclusion & Future Work.....</i>	<i>44</i>
<i>Chapter 8: Appedix.....</i>	<i>45</i>
<i>Chapter 9: References</i>	<i>58</i>

List of Tables

<i>Key Terms of PCI DSS</i>	19
<i>Ontology Metrics</i>	24
<i>Data Properties</i>	27

List of Figures

<i>Architecture Flow</i>	16
<i>Business Architecture Model</i>	17
<i>Word cloud for regulation's key terms</i>	19
<i>Deontic Expressions Sentence Distribution</i>	22
<i>High Level Ontology</i>	24
<i>Skeleton of Regulation class</i>	26
<i>Data Property of EFTA, TILA, GLBA, PCI MA</i>	30
<i>Ontology Object Properties</i>	31
<i>Instances Count per Class</i>	32
<i>SWRL Rules</i>	33
<i>SWRL rule Inference Output</i>	33
<i>SWRL rule Inference Output for Consumer Class</i>	34
<i>SPARQL Query Results - Consumers Perspective</i>	36
<i>SPARQL Query Results - Provider Perspective</i>	36
<i>Validation Results</i>	39
<i>Key Words present in Organization policies</i>	39
<i>Drop Down menu for Use Case Scenarios</i>	40
<i>Regulation for EFTA Provider Obligations</i>	41
<i>Regulation for Consumer Liability</i>	42
<i>Regulation for Error Resolution Policy</i>	4

Chapter 1: Introduction

Section 1: Mobile Wallets

Mobile wallet is an application on your mobile device that stores payment information from a credit card or debit card and allows you to use your device to make purchases. The main benefit of mobile wallets is convenience. Store all your payment card information in one place, so you don't have to carry the cards with you, means no longer carrying a wallet. A digital wallet can provide two-way communication between a consumer and a merchant. Mobile payments, however, are different and should not be confused with mobile banking. A mobile payment is commonly defined as “the process of using a hand-held device to pay for a product or service, either remotely or at a point of sale”. They are not limited to the parties involved in traditional banking services nor are they limited to standard banking services, mobile payments are much more complex and often involve numerous parties.

Digital wallets are going to transform the world of consumer payments and commerce [1]. Digital wallets are the computer software applications that stores and transmits payment authorization data for one or more credit, debit, gift card accounts [1]. The consumer loads the payment account data into the digital wallet, the digital wallet functions as a payment device for the selected account, transmitting the data to merchants to authorize payment [1]. By storing payment authorization data, digital wallets function analogously to physical wallets that contain multiple payment cards used to transmit payment authorization data [1].

Section 2: Banking Regulations

Mobile payments are on the rise and as the popularity is growing it's important to understand the regulation framework behind it. Till today, mobile wallets regulations are in the grey area when it comes USA legal framework. There are no such compliance policies which are specific to mobile wallets. Whatever policies are for banking transactions same may apply to mobile payment transactions as well. Thus, making it difficult for the consumer and provider to understand what and how many laws may apply and how each of them are legally bind to such regulations. Banking regulations are large textual document which are currently available in textual documents and require significant manual effort to ensure their compliance are met. Mobile wallets in the coming future of technology advancements are bound to change the traditional way of transaction lifecycle. In USA the mobile wallets regulations are still in the grey area. The regulations are aligned with banking regulations that are present in the United States of America. Most of the regulations that are applied to banking sector also applied to mobile wallets.

As the popularity of mobile payments is growing, it becomes necessarily important to understand the legal framework in which mobile wallets operates [2]. Consumers need to know their rights and responsibilities. They need to be alert to the financial risks they are exposed to and the legal remedies available when transactions go awry [2]. Financial institutions and other companies that facilitate mobile payments need clear rules describing their obligations, rights, and liability as they develop new mobile payment products and contract with consumers for mobile payment services [2]. While the banking is one of heavily guarded regulations industry, the regulations of mobile wallets are still circling around the grey areas of these laws and

regulations. The regulation that apply to the mobile wallet transaction and are part of this research study are mentioned below

1. Electronic Fund Transfer Act (EFTA) / Regulation E [3]
2. Truth in Lending Act (TILA) / Regulation Z [4]
3. PCI Mobile Payment Acceptance Security Guidelines [5]
4. Gramm-Leach-Bliley Act (GLBA) Privacy and Data Security Provisions [6]
5. Unfair, Deceptive, or Abusive Acts or Practices (UDAP) under the Federal Trade Commission (FTC) Act
6. Unfair, Deceptive or Abusive Acts or Practices (UDAAP) under the Consumer Financial Protection Act of 2010
7. Federal Deposit Insurance¹⁸ or NCUA Share Insurance

Section 3: Motivation

Digital/Mobile wallets are starting to more popular because of the ease of services it provides to the end user. However, the question remains to what extent do the consumer using the mobile payments and provider building such application know in terms of liabilities and policies. Our research is based on the use case scenarios of Consumers and Providers. Below are some of scenarios we took into considerations:

1. Consumer Perspective:

- a. What are Consumers Obligations?
- b. What are Consumers liabilities in-case of fraud, loss of device, theft?
- c. What rights does the Consumer hold for Mobile Wallets compliance policies?

2. *Providers Perspective:*

- a. What are the Provider Obligations for Mobile Wallets compliance policies?
- b. What are Provider Obligations for resolving an error in Mobile payments involving usage of a debit card?
- c. What disclosers policies for the Provider dealing in Mobile Payments?
- d. What data protection policies are to be followed by Provider when giving a service like Mobile Wallets?

In order to answer these questions, we need to look across all the regulation documents. In depth, we may need to find out the policies related to such scenarios. This will require a lot of manual effort and it will be extensively time consuming.

Research on such legal documents has always been an active area of research. However, the work on automating the process to extract the rules from these regulation documents are limited and need more exposure. In our previous work [7] [8] [9] we have identified the various compliance regulations that apply to data privacy, credit card compliance and on cloud service level agreements. As part of this research project we will be using regulation documents like Electronic Fund Transfer Act/ Regulation E, Truth in Billing Act/ Regulation Z, PCI Mobile Payment Acceptance Security Guidelines and Gramm-Leach-Bliley Act (GLBA) Privacy and Data Security Provisions. All these documents are long, complex and require legal expertise because it is a time consuming and labor-intensive process. Developing a cognitive assistant module for such long and complex documents will provide significant help in answering questions to above mentioned scenarios which requires significant amount of manual human intervention. At the same time, it will also help businesses as well as legal experts to analyze the legal elements easily

and efficiently. These regulation documents are available in electronic form on United States Government Publishing Office Websites and on various paid websites like Payment Card Industry Security Standards Council website, but because of its semi- structured organizational structure it is quite a challenge to look all of the relevant sections that a user may need to review to answer a particular question.

Keyword searches may also return vast numbers of desirable matches requiring large amounts of manual intervention of humans to review, analyze and sort the relevant and irrelevant responses [10]. The organizational structure of these banking regulation documents also makes it difficult to compare relevant sections and titles because indexing of the information through sectional tables of contents is carried out at relatively high levels within the regulatory sections [10]. As part of our Automated Legal Document Analytics (ALDA) project [11], we have been developing innovative approaches to transform legal regulation documents from textual databases to machine processable graph-based datasets using Semantic Web languages and by applying Deep Learning and Natural Language Processing (NLP) techniques. Most of these long and textual regulation documents are available in XML format. Dealing with heterogeneous legal facts and rules in semi-structured format like XML is difficult in terms of answering user queries and performing analysis on various legal element. Hence, building ontologies for legal documents is one of the possible efficient solutions to capture various facts and rules of legal documents in order to perform analytics and answer queries. Our long-term goal is to develop a system that for any given action or question, can highlight all the statutes, policies, laws and case law across different domains like medical, Data Privacy, Financial regulations, Cloud SLAs etc. that might be applicable on it and offer preliminary support to the end user. As a shorter-term

vision, we are aiming to develop a machine understandable process which can automatically extract elements from these banking regulation documents for mobile wallets compliance policy and answer questions like “What are the provider obligation for mobile wallets regulation policies”?

In previous work [7] [9] [10] [8] [11] we have developed cognitive framework to automatically parse and extract knowledge from legal documents and represent it using an Ontology. The framework captures knowledge in form of key terms, rules, topic summaries, relationships between various legal terms, semantically similar terminologies, deontic expressions and cross-referenced legal facts and rules. As a first step towards this vision of a holistic data compliance knowledge graph, we have created a semantically rich policy-based knowledge graph for Mobile Wallets transaction compliance. We used Semantic Web technologies like OWL, RDF and SPARQL, Natural Language Processing (NLP) and text mining techniques to create this graph which is machine processable. Hence, it can also contribute significantly to automating the continuous monitoring of data operation, transfer, and sharing. In this paper, we describe this knowledge graph in detail along with the methodology we have used to build it. We have validated this Knowledge Graph against the policies of five major mobile wallets vendors that deal in mobile payments. This Knowledge Graph, that is available in the public domain, can be used by practitioners to significantly to understand the roles of providers and consumers and how providers and consumers are bind by these regulations.

In chapter 2 we have described the related work and chapter 3 we describe our methodology of building the knowledge graph and we provide in detail the ontology we have

developed using OWL in chapter 4. In chapter 5 we provide details about result by validating our knowledge graph with various mobile wallets vendor's policies. In Chapter 6, we talk about how we have built a user interface which will help in providing the knowledge in web application prototype and lastly, we end with conclusions and future work in chapter 7.

Chapter 2: Related Work

Section 1: Semantic Web

In a services environment, consumers and providers need to be able to exchange vital information, queries, and requests with some assurance that they share a similar and common meaning [8]. This is important not only for the data but also for the data protection policies followed by service consumers or providers [8]. One possible approach to this issue is to employ Semantic Web techniques for modeling and reasoning about regulation policies for mobile wallets transactions. We have used this approach for developing our knowledge graph and applied reasoner to infer the data for knowledge representation. The Semantic Web deals primarily with data instead of documents[8]. It allows data to be annotated with machine understandable meta-data, permitting the automation of their retrieval and their usage in incorrect contexts [8]. Semantic Web technologies include languages such as Resource Description Framework (RDF) [12] and Web Ontology Language (OWL) [13]for defining ontologies and describing meta-data using these ontologies as well as tools for reasoning over these descriptions. These technologies can be used to provide common semantics of privacy information and policies enabling all agents who understand basic Semantic Web technologies to communicate and use each other's data and Services effectively[8][9].

In our prior work [7] [9] [8] we have developed knowledge graph for data protection policies, credit card transaction policies, data privacy and applied semantic web technology like RDF [12], OWL [13] and have used SPARQL [14] for querying the knowledge to represent in

readable format. For the research work of mobile wallets transaction compliance, we will be using the same approach along with user interface which will help the end users a platform to query the regulation in a much more efficient manner.

Section 2: Text Extraction

Researchers have used and implemented Natural Language Processing technique to extract relevant information from the large corpus of text documents. In the research, Rusu et. al. [15] the authors suggested the technique to extract the information and relevant phrases in the form of subject-predicate-object triplets [8]. To do so Parse Trees were generated from English sentences and triplets were extracted from the parse trees [8] [9] [15]. In the research work of Etzioni et. al. [16], the author developed the KNOWITALL system which helped in automation of extracting large collections of facts from the Web in an unsupervised, domain-independent, and scalable manner [8] [9]. The author used the approach of Pattern Learning to address this challenge [8] [9] [16]. In another research, other important NLP technique approach was implemented for information extraction from unstructured text is ‘Noun Phrase Extraction’ [8]. Author Rusu et. al. in [15] showed the technique of creating triplets by considering ‘Noun Phrases’ obtained via various part-of-speech taggers [8]. Different automated techniques have been used for extracting the permissions and obligations from legal documents [8] [9]. Techniques such as text mining and semantic techniques have been explored and applied by various authors in the past [8] [9] [17] [18]. In the research work of Kagal et al. [19] [20], the authors proposed an ontology-based policy framework to model conversation specifications and policies using obligations and permissions [8] [9] [19] [20].

Section 3: Key regulations for Mobile Payments

The world is seeing lot of technology and digital advancement in the financial sector. As these new technologies get developed and get implemented in the payment space, the regulatory body applicable for implementing regulations in these matters must ensure that appropriate protections are in place to safeguard consumers from fraud and unauthorized transactions. At the same time, providers should also know what policies they need to follow when developing technology like mobile wallets. At large, still in USA we have the same regulation as for mobile banking and trading banking. Some of the major regulations that are being used for this research study are described below:

1. Electronic Fund Transfer Act/ Regulation E

The Electronic Funds Transfer Act (EFTA) was passed in the year 1978 and codified into law through the FED's Regulation E [21]. The EFTA contains rules and policies for electronic fund transfers (EFT)'s, which can include any transaction initiated through a computer, telephone, magnetic tape, or electronic terminal [21]. These types of transactions can be initiated through automated teller machines (ATM's), debit card transactions, and direct deposits and withdrawals from a bank account [21]. The regulation generally applies to any financial institutions, but certain provisions apply to "any person" or any provider dealing in mobile wallets applications or mobile payments. The law applies to mobile wallet too when the underlying payment is made from a consumer's account via an EFT. EFTA is mainly for regulations in banking sector when there is a payment involving a debit card and now that in mobile wallets also a payment can be done through a debit card hence EFTA act applies to mobile wallet too. Some of the key obligations for this act is that the rule establishes the consumer rights to a number of disclosures

and error resolution procedures for unauthorized or otherwise erroneous transactions [22]. The disclosures include upfront disclosures regarding, among other things, the terms and conditions of the EFT service and how error resolution procedures will work [22].

2. Truth in Billing Act/ Regulation Z

The Truth in Lending Act (TILA) is part of regulation z, which was codified under FED Regulation Z that establishes the rules surrounding consumer credit [21]. TILA act was formed to give consumers a better sense of the available credit options and to better understand the costs of various credit lines [21]. TILA is meant to apply to creditors that offer credit products such as credit cards but may apply to mobile payment systems when a mobile payment is funded by a credit card or other TILA covered credit account. It applies to mobile wallets compliance policy when the underlying source of payment is a credit card (or other credit account covered by TILA and Regulation Z) [22]. Some of the key obligations that are part of TILA act are that the Creditors or any organizations are required to provide disclosures to consumers describing costs including interest rate, billing rights, and dispute procedures [22]. Like EFTA deals in Debit card usage similarly TILA act deals in policies regulated for credit card usage.

3. Gramm-Leach-Bliley Act (GLBA) Privacy and Data Security Provisions

Gramm Leach Bliley Act was enacted on 1999 and was set up for data security guidelines and privacy rules for depository institutions and any nonbank engaged in financial activity [21]. The GLBA applies to any financial institution or nonbank engaged in financial activity that handles the personal information of a customer registered for the service, in this case it is mobile wallets providers. Data security provisions in the GLBA act sets up guidelines for necessary safeguarding of customer nonpublic information that includes customer addresses, phone

numbers, bank account numbers, social security numbers, income, and credit histories [21]. The law has been made to protect customer's Personal Identifiable Information (PII). Some of the key obligations that GLBA act provides are that the institutions are required to provide consumers with the notices regarding the privacy of nonpublic personal information and allow them to opt out of certain types of information sharing [22]. The GLBA data security provisions give guidance on the appropriate safeguarding of customer information [22]. Thus, this act establishes the rules for consumer privacy and customer data security.

4. PCI Mobile Payment Acceptance Security Guidelines for Developers

The Payment Card Industry Security Standards Council (PCI SSC) recognizes that merchants may use consumer electronic handheld devices like smartphones, tablets, wearables—or collectively, “mobile devices” that are not solely dedicated to payment acceptance for transaction processing [5]. For instance, a merchant might use an off-the-shelf mobile device for both personal use and payment acceptance [5]. Most of these devices do not meet security characteristics required by generally accepted information security standards [5]. The purpose of this policy document is to let stakeholders responsible for the architecture, design, and development of mobile applications and their associated environment within a mobile device that merchants use for payment acceptance. The provider developing mobile wallets can use the document guidelines to help them design appropriate security controls within their software and hardware products [5]. These controls can then be applied to mobile payment-acceptance environments, thus supporting the deployment of more secure solutions.

The document clearly points out that it is not a comprehensive guide to PA DSS compliance. Rather, it is just designed as a policy to help organizations interpret the PA DSS requirements in

the context of mobile devices. The PCI mobile payment guidelines contain three objectives for securing mobile payment transactions:

“Objective 1: Prevent account data from being intercepted when entered into a mobile device. If P2PE is not being used, developers must ensure that a secure transmission path exists between the device used to swipe or input card data and the mobile device” [5].

“Objective 2: Prevent account data from compromise while processed or stored within the mobile device. Any account data stored temporarily on the device must be protected within a secure storage environment. Data retained on the device after transaction authorization must be protected with hashing, truncation or encryption combined with acceptable key management practices” [5].

“Objective 3: Prevent account data from interception upon transmission out of the mobile device. When cardholder data is transmitted from the device to the next step in the authorization process, it must be protected with strong encryption, such as that provided by Secure Sockets Layer (SSL)/Transport Layer Security (TLS)”. [5]

Apart from having guidelines for securing mobile transactions, the guidelines also include a list of 15 certain points that should be used when configuring the mobile device itself:

1. “Prevent unauthorized logical device access” [5].
2. “Create server-side controls and report unauthorized access” [5].
3. “Prevent escalation of privileges” [5].
4. “Create the ability to remotely disable the payment application” [5].
5. “Detect theft or loss” [5].

6. “Harden supporting systems” [5].
7. “Prefer online transactions” [5].
8. “Conform to secure coding, engineering and testing” [5].
9. “Protect against known vulnerabilities” [5].
10. “Protect the mobile device from unauthorized applications” [5].
11. “Protect the mobile device from malware” [5].
12. “Protect the mobile device from unauthorized attachments” [5].
13. “Create instructional materials for implementation and use” [5].
14. “Support secure merchant receipts” [5].
15. “Provide an indication of secure state” [5].

Chapter 3: Methodology

In this section, we describe our methodology to build and validate our mobile wallets transaction compliance ontology. Our aim is to present a rich policy-based knowledge representation of the banking regulations that applies to mobile payments. Our methodology is divided into five different phases. Figure 1 shows the overall representation of our architecture flow. The five phases of our methodology are:

- 1. Data Collection:** Performed extensive research in identifying the regulations that may apply to mobile wallets compliance. More explanation can be found in section 1 of this chapter.
- 2. Data Preprocessing:** For all the four policy regulations we extracted the relevant sections and key terms from the repository. More explanation can be found in section 2 of this chapter.
- 3. Ontology Development:** Created an Ontology by combining all the four regulations. Detailed information can be found in chapter 4 of this research.
- 4. Evaluation & Validation:** The validation of built the knowledge graph was done using publicly available organization policies dealing in mobile wallets. This topic has been explained in detailed in chapter 5 of this research.
- 5. Web Application Development:** A web application was built to showcase the knowledge representation to the end user in much more efficient manner. This process has been explained in detailed in chapter 6 of the research.

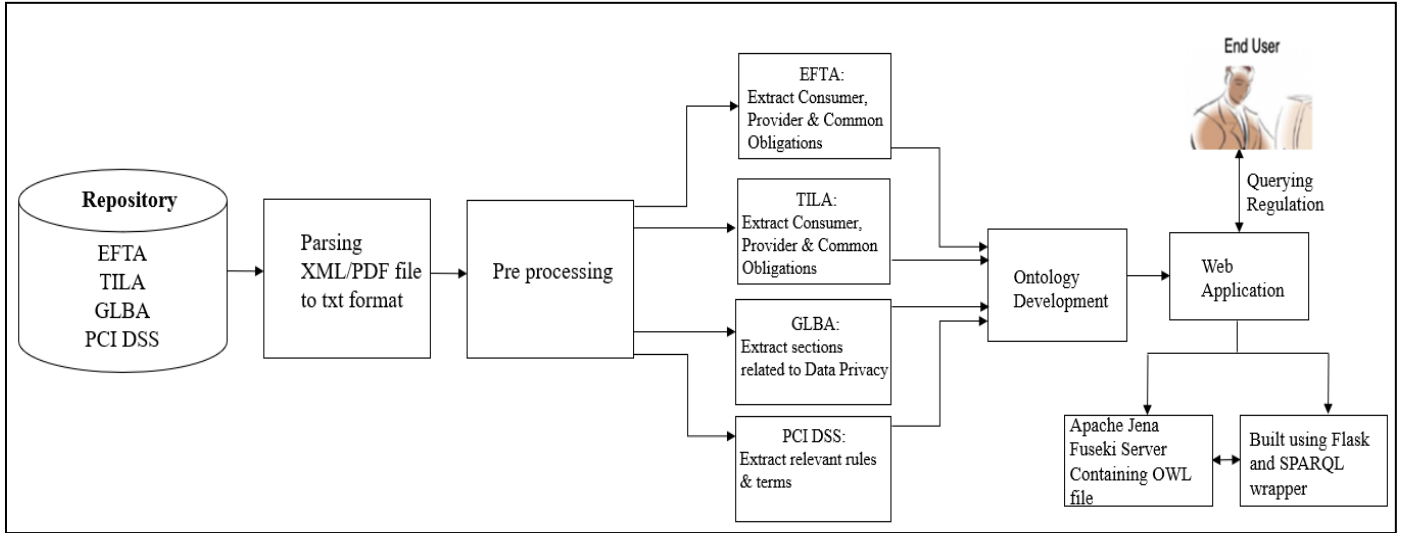


Figure 1: Architecture Flow

Section 1: Data Collection

This was the very first process in the methodology. In the initial stage, we wanted to know how the mobile wallets process works and how the system is designed. As we have been saying from the beginning, there are no such compliance polices which are specific to mobile wallets. Whatever policies are present for banking transactions same may apply to mobile payment transactions as well. So, once this was figured out that same regulation policies would be applied then we extensively researched for the banking regulations as per our context. We were looking for the regulations which aligned towards the usage of debit cards and credit cards, protection of Personal Identifiable Information (PII) of customers stored by financial institutions and the policy to build an application which deals in mobile payments.

Based on these contexts for our research we found the regulation Electronic Fund Transfer Act (EFTA) which is linked to usage of debit cards, gift cards. Similarly, we found regulation Truth in Billing Act (TILA) which is linked to usage of credit cards and Gramm-Leach-Bliley Act (GLBA) which is related to protection of Personal Identifiable Information

(PII) of customers stored by financial institutions. Finally, the policy document PCI Mobile Payment Acceptance Security Guidelines for Developers was found and was linked to the guidelines of building an application dealing in mobile payments. These reasoning and research helped us in building a business model for our research. Figure 2 below represents the business architecture model for our research.

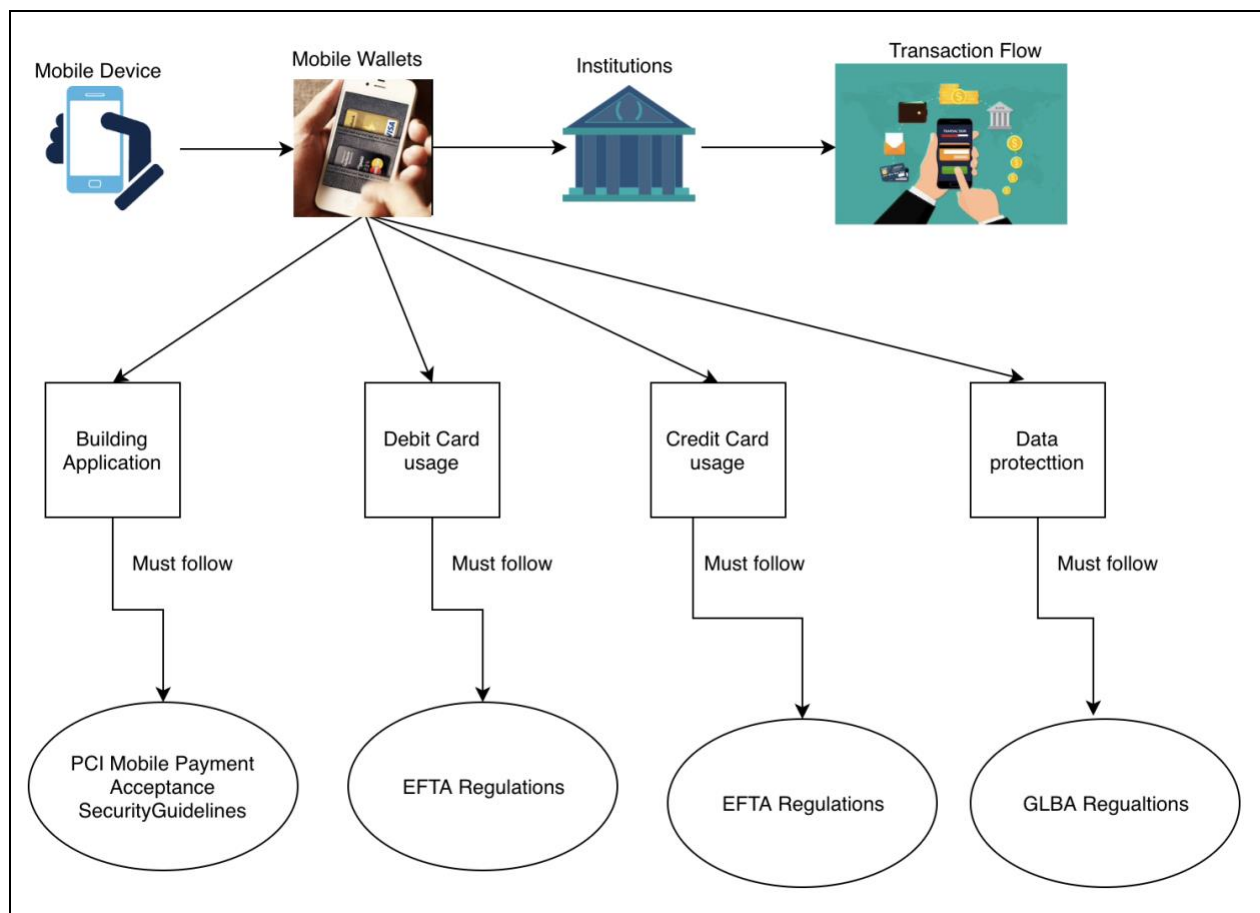


Figure 2: Business Architecture Model

Section 2: Data Preprocessing

In one of our previous work, we have developed a simple knowledge for the PCI DSS regulation based on the 12 requirements defined by the PCI DSS council [7] [23]. The goal of the PCI DSS is to protect cardholder data wherever it is processed, stored or transmitted [7] [23].

The security controls and processes required by PCI DSS are important for protecting cardholder account data, including the PAN – the Primary Account Number printed on the front of transaction card [7] [23]. This includes sensitive data that is printed on a card or stored on a card's magnetic stripe or chip – and personal identification numbers entered by the cardholder [7] [23] . In general, if an organization deals in card transactions then it must follow the key policies listed in the PCI DSS checklist [7] [23]. The very first step in our preprocessing process was to integrate the PCI DSS ontology work in this research. This is because the mobile payments are part of transaction flow that happens later in the process after the setup of mobile wallets has happened and the end user has initiated a payment using mobile wallets. Once the payment is initiated then organizations must adhere to PCI DSS guidelines [23]. In the next stage of our system we extracted the repository of EFTA Act [3], TILA Act [4], GLBA Act [6] and PCI MA Policies [5]. In our previous work [7], we were able to extract relevant key terms from the 12 PCI DSS documents and build knowledge graph accordingly [7]. Similarly, for all of these banking regulations we will be extracting relevant sections and terms accordingly to build semantic rich knowledge graph.

The Code of Federal Regulation documents includes EFTA, GLBA and TILA. The structure of these documents is present in XML format. After the creating the repository of these XML files we needed to convert these documents into txt format to develop our knowledge graph module. To perform XML parsing into text, we made use of ElementTree Python library [24]. The title of the section is present in the *<subject> tag*, section number of the document is present in the *<sectno> tag* and finally, textual contents of the documents in the XML files are present in the *<p> tag*. All these tags are part of tag called *<section> tag*, with the help of this

library we parsed to the *<section>* tag where the contents all three tags were stored in three different python lists. After this process, we did the next step in preprocessing stage which is to determine key terms and Deontic expressions. These two processes are explained in detailed below:

Section 2.1: Key Term Extraction

As mentioned above, in our previous work of PCI DSS [7], we extracted the relevant key terms that were important in context when an organization falls under PCI DSS compliance [7].

Table 1 below lists the relevant key terms from PCI DSS policies [7]

Key terms	Frequency
Maintain	10
Control	13
Establish	5
Access	43
unauthorized	6
Ensure	10

Table 1: Key Terms of PCI DSS [7]

Similarly, we aimed to identify all the relevant key terms for all the four regulations in this research. We made use of Term Frequency and Inverse Document frequency (TF-IDF) [25] to determine the relevant entities from the documents. This also helped us in mapping the instance for our ontology, shown below in word cloud.

sentence would fall into. This method is vital in answering to questions like "When should consumer notify the provider in case of fraud or loss of device", the answer to such questions should clearly specify four deontic expressions which includes Permissions(Do's), Obligation(mandatory Do's), Prohibition(Don'ts) and Dispensation(Nonmandatory conditions). We have classified the sentences into Permissions and Obligations in our research.

In our previous work, we used text mining techniques to extract deontic rules from cloud SLA documents [9], PCI DSS documents [7] and GDPR policies [8]. We have used similar approach to classify the sentences into Permissions and Obligations. We made use of NLTK library [27] in Python which helped in POS tagging for each of the sentences present in all four documents. After that, we formulated grammatical rules based on the POS tags to acquire rules in the form of permissions and obligation. Figure 4 below shows the distribution of deontic sentences for all the regulation documents. The following are the grammar rules we used to classify text into deontic expression:

- Permissions:

< Noun/Pronoun > < deontic > < verb >

- Obligations:

< Noun/Pronoun > < deontic > < adverb > < verb >

Deontic Expression is vital in answering to questions like

- **“What are Provider policies for periodic statement in case of late payment?”**
- **“When should consumer notify the provider in case of fraud or loss of device?”**

Permissions: *“The amount of any late payment fee and any increased periodic rate(s) (expressed as an annual percentage rate(s)) that may be imposed on the account as a result of late payment.*

*If a range of late payment fees **may** be assessed, the card issuer may state the range of fees, or the highest fee and an indication that the fee imposed could be lower. If the rate **may** be increased for more than one feature or balance, the card issuer may state the range of rates or the highest rate that could apply and at the issuer's option an indication that the rate imposed could be lower.” [4] [TILA, Section 1026.7 Periodic statements]*

Obligations: *“Timely notice is given. If the consumer notifies the financial institution within two business days after learning of the loss or theft of the access device, the consumer's liability **shall** not exceed the lesser of \$50 or the number of unauthorized transfers that occur before notice to the financial institution.”[3] [EFTA/Regulation E, Section 205.6 Liability of consumer for unauthorized transfers]*

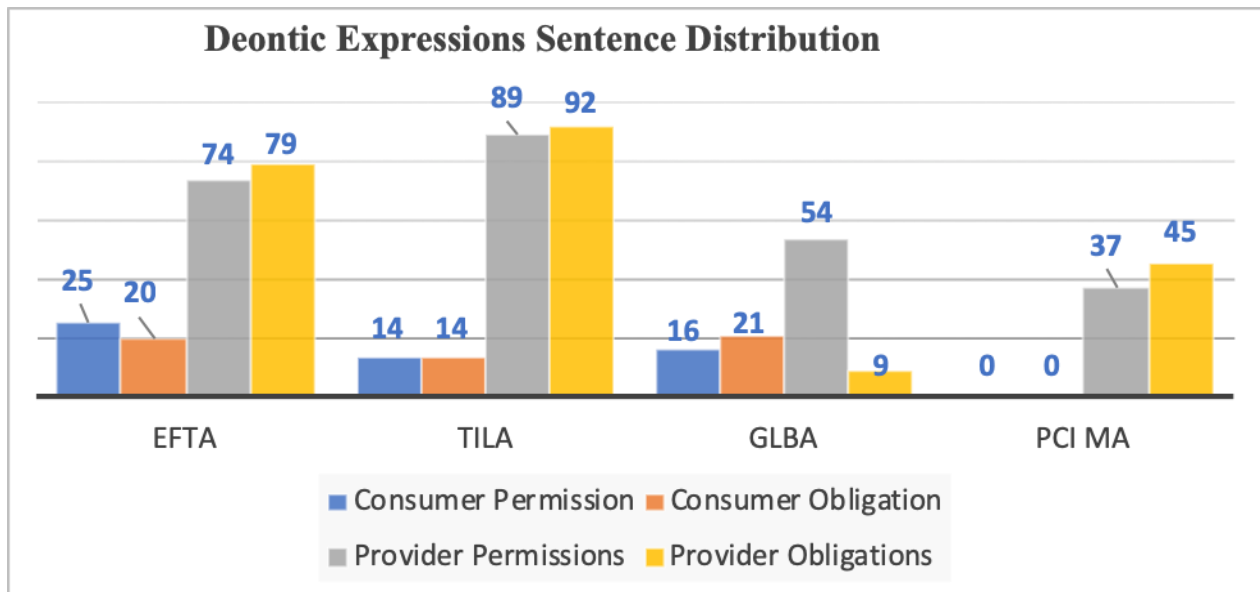


Figure 4: Deontic Expressions Sentence Distribution

Chapter 4: Mobile Wallets Ontology

Section 1: Ontology Development

An ontology can be defined as a common vocabulary for researchers which will be helpful in sharing information of a domain [7]. To be more specific an Ontology model is said to be the classification of entities which models the relationship between the defined entities. For our framework, we have used OWL [13] and RDF [12] language to capture the rules defined by the regulations used for this research. These are open source languages developed by WWW Consortium (W3C) and so our ontology, which is in public domain, can be easily adopted by organizations dealing in mobile payments. It is also platform independent and so can be easily integrated with PCI DSS [23] and many other data regulation entities. RDF [12] is a language which helps in encoding knowledge on web space so to make the information understandable to electronic agents searching for domain related information [7]. In general, ontologies are used to capture information for domain of interest. In this knowledge graph of mobile wallets compliance policies, we have also incorporated our previously built PCI DSS Ontology [7]. We made of software application called Protégé [28], “A free, open-source ontology editor and framework for building intelligent systems” [28]. Figure 5 below represents the high-level overview of our Ontology.

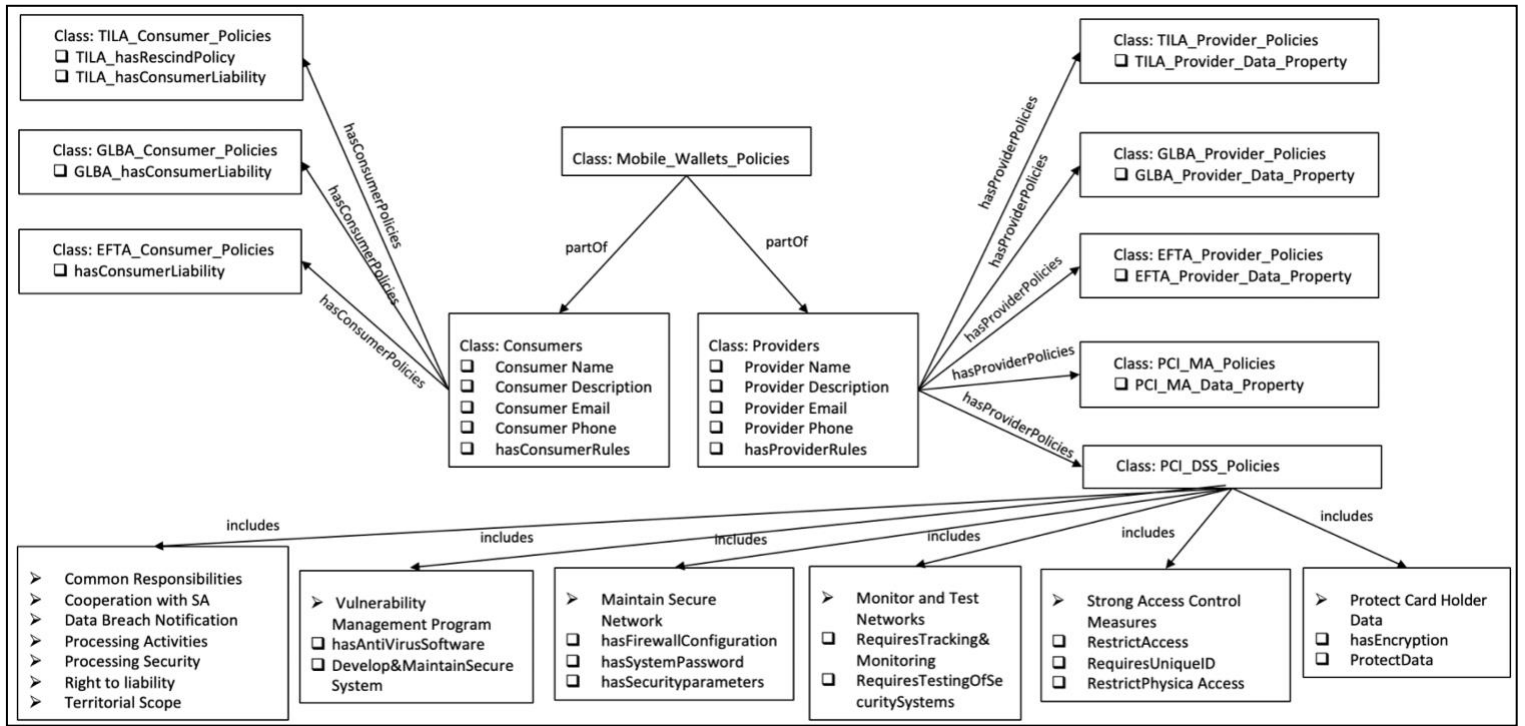


Figure 5: High Level Ontology

For the Mobile Wallets Compliance Ontology, the metric is mentioned below in Table 2:

Metric Names	Counts
Axiom	1135
Logical axiom count	793
Declaration axioms count	342
Class count	35
Object property count	13
Data property count	73
Individual count	221
Annotation Property count	3
DL expressivity	ALCHI(D)

Table 2: Ontology Metrics

We have seven super classes along with the imported PCI DSS Ontology [7]. These seven classes are:

1. **Consumers:** The Consumers class contains all the rules which are in a way getting inferenced as consumer policies for Mobile Wallets transaction compliance.
2. **Providers:** The Providers class contains all the rules which are in a way getting inferenced as provider policies for Mobile Wallets transaction compliance.
3. **Regulations:** The Regulations class has many sub classes and it is the base where all the four regulation is designed in such way that these are getting inferenced to class like **Consumers** and **Providers**.
4. **Consumer_Obligations:** The Consumer_Obligations class contains all the rules extracted with help of deontic logic as obligation rules for consumers.
5. **Consumer_Permissions:** The Consumer_Permissions class contains all the rules extracted with help of deontic logic as permission rules for consumers.
6. **Provider_Obligations:** The Provider_Obligations class contains all the rules extracted with help of deontic logic as obligations rules for providers.
7. **Provider_Permissions:** The Provider_Permissions class contains all the rules extracted with help of deontic logic as permissions rules for providers.

We have regulation that is considered as a base class for developing our mobile wallets ontology. The regulation has four sub classes “EFTA”, “GLBA” , “TILA” and “PCI MA”. Each of these classes have their own sub classes. The skeleton of the Regulation class is present below in figure 6. The Skeleton of EFTA class is like it has four more subclasses named as

EFTA_Definitions, EFTA_Sections, EFTA_Titles and EFTA_Policies. Further, the EFTA_Policies class three more subclasses named as EFTA_Consumer_Policies, EFTA_Common_Policies and EFTA_Provider_Policies. Similarly, for TILA class it has four more subclasses named as TILA_Definitions, TILA_Sections, TILA_Titles and TILA_Policies. Further, the TILA_Policies class three more subclasses named as TILA_Consumer_Policies, TILA_Common_Policies and TILA_Provider_Policies. Just like above, GLBA class also has four classes GLBA_Definitions, GLBA_Sections, GLBA_Titles and GLBA_Policies. Finally, the GLBA_Policies class three more subclasses named as GLBA_Consumer_Policies, GLBA_Common_Policies and GLBA_Provider_Policies. At last the PCI_MA class has two sub classes named as PCI_MA_Definitions and PCI_MA_Policies.

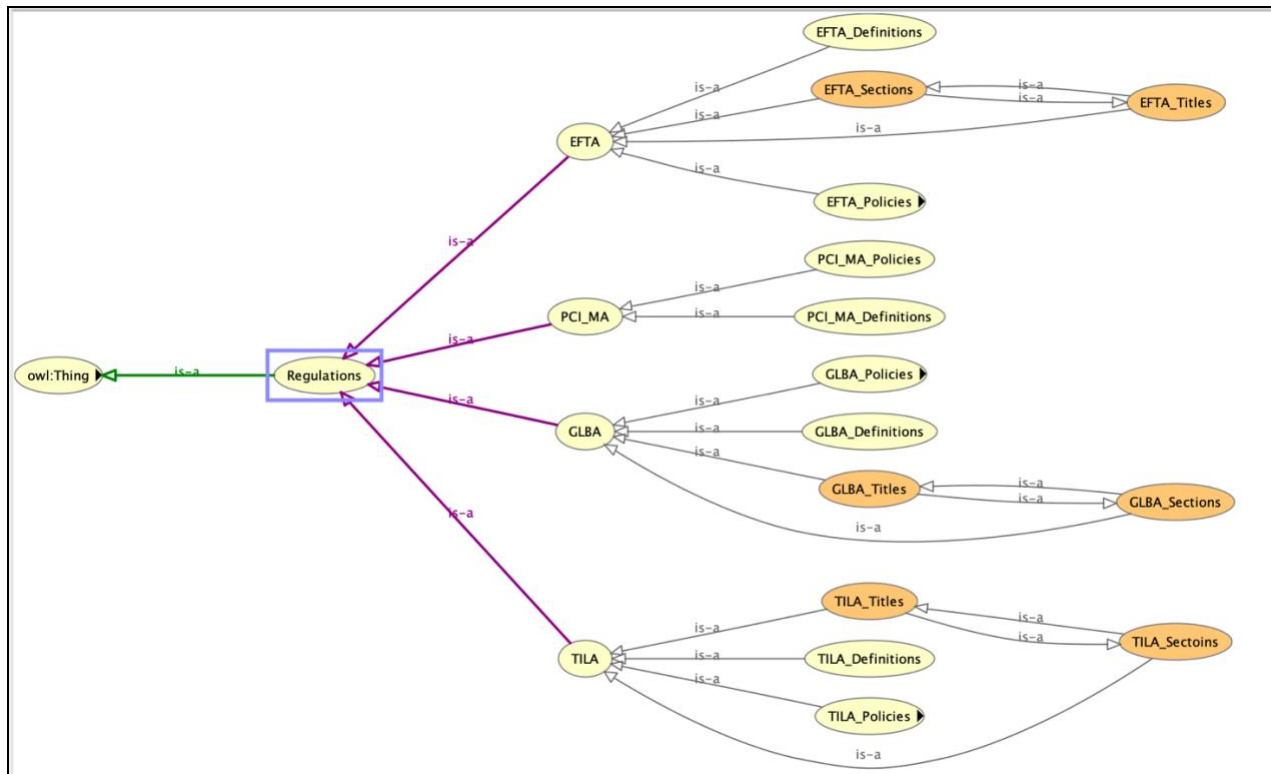


Figure 6: Skeleton of Regulation class

Each of these classes have total of 65 Data Properties created for EFTA, TILA, GLBA and PCI MA class. Figure 7 below shows the bar graph of Data Property for each of the classes. The Data property table of each of the classes is mentioned below in table 3. These Data Property helps in defining the instances the data value and all the values of data type string. In OWL terminology the “Domain” of these properties are its corresponding classes and the “Range” is “xsd:string”.

Data Property	Class
EFTA_means	EFTA_Definitions
hasPurpose	EFTA_Common_Policies
hasAuthority	EFTA_Common_Policies
hasCommonLiability	EFTA_Common_Policies
hasConsumerLiability	EFTA_Consumer_Policies
provideReceipts	EFTA_Provider_Policies
hasProviderLiability	EFTA_Provider_Policies
hasCoverage	EFTA_Provider_Policies
providePreauthorizedTransferNotice	EFTA_Provider_Policies
provideGeneralDisclosures	EFTA_Provider_Policies
provideNotice	EFTA_Provider_Policies
provideErrorResolution	EFTA_Provider_Policies
provideInitialDisclosures	EFTA_Provider_Policies
provideStatement	EFTA_Provider_Policies
GLBA_means	GLBA_Definitions
GLBA_hasScope	GLBA_Common_Policies

GLBA_hasPurpose	GLBA_Common_Policies
GLBA_hasConsumerLiability	GLBA_Consumer_Policies
GLBA_hasOptOutNotice	GLBA_Provider_Policies
GLBA_useModelPrivacyForm	GLBA_Provider_Policies
GLBA_provideDelivery	GLBA_Provider_Policies
GLBA_provideSharingInfoLimits	GLBA_Provider_Policies
GLBA_provideAnnualNotice	GLBA_Provider_Policies
GLBA_provideDiscloserLimits	GLBA_Provider_Policies
GLBA_provideInitialNotice	GLBA_Provider_Policies
GLBA_provideRediscloserLimits	GLBA_Provider_Policies
GLBA_hasRevisedNotice	GLBA_Provider_Policies
GLBA_IncludeInformation	GLBA_Provider_Policies
PCI_MA_means	PCI_MA_Definitions
PCI_MA_hasSecurePolicy	PCI_MA_Policies
PCI_MA_hasVulnerabilitiesPolicy	PCI_MA_Policies
PCI_MA_hasAuditingPolicy	PCI_MA_Policies
PCI_MA_hastheftpolicy	PCI_MA_Policies
PCI_MA_hasSecureStatePolicy	PCI_MA_Policies
PCI_MA_provideApplicationHardening	PCI_MA_Policies
PCI_MA_provideHardeningPolicy	PCI_MA_Policies
PCI_MA_hasUnauthorizedAttachmentPolicy	PCI_MA_Policies
PCI_MA_hasTransmissionPolicy	PCI_MA_Policies
PCI_MA_hasMalwarePolicy	PCI_MA_Policies

PCI_MA_hasUnauthorizeAccessPolicy	PCI_MA_Policies
PCI_MA_hasUnauthorizedApplicationPolicy	PCI_MA_Policies
PCI_MA_hasInterceptionProtections	PCI_MA_Policies
PCI_MA_hasServerSideControlsPolicy	PCI_MA_Policies
PCI_MA_hasCompromiseProtections	PCI_MA_Policies
PCI_MA_hasSecureMerchantReceipts	PCI_MA_Policies
PCI_MA_hasPrivilegesPolicy	PCI_MA_Policies
PCI_MA_hasRemotelyDisablePolicy	PCI_MA_Policies
TILA_means	TILA_Definitions
TILA_hasCoverage	TILA_Common_Policies
TILA_hasFinanceCharge	TILA_Common_Policies
TILA_hasPurpose	TILA_Common_Policies
TILA_hasAuthority	TILA_Common_Policies
TILA_hasRescindPolicy	TILA_Consumer_Policies
TILA_hasConsumerLiability	TILA_Consumer_Policies
TILA_hasAdvertisingPolicy	TILA_Provider_Policies
TILA_provideDisclosure_requirements	TILA_Provider_Policies
TILA_provideStatement	TILA_Provider_Policies
TILA_provideErrorResolution	TILA_Provider_Policies
TILA_hasPaymentsPolicy	TILA_Provider_Policies
TILA_hasTerminationPolicy	TILA_Provider_Policies
TILA_provideAccountOpeningDisClosures	TILA_Provider_Policies
TILA_provideGeneralDisclosures	TILA_Provider_Policies

TILA_hasTransactionIdentification	TILA_Provider_Policies
TILA_hasCreditBalancePolicy	TILA_Provider_Policies

Table 3: Data Properties



Figure 7: Data Property of EFTA, TILA, GLBA, PCI MA

Similarly, we also have created Object Properties to determine and link the instances with each other. We have total of 13 object properties which has helped in linking the instances in our ontology. Figure 8 below shows the object properties of our Mobile Wallets Ontology.

Object Property	Description
has_EFTASectionNumber	To link EFTA Section class with EFTA Title class.
has_GLBASectionNumber	To link GLBA Section class with GLBA Title class.
has_TILASectionNumber	To link TILA Section class with TILA Title class.
hasConsumerPolicies	To link Consumer class with consumer policies class present under EFTA Polices, GLBA & TILA Policies Class
hasProviderPolicies	To link Provider class with Provider policies class present under EFTA, GLBA, PCI MA & TILA Policies Class
partof_ConsumerPolicy	To link consumer policies class present under EFTA Polices, GLBA & TILA Policies Class with Consumers Class
partof_EFTA	To link each EFTA Policies class with EFTA Section and EFTA Titles
partof_EFTATitle	To link EFTA TITLE class with EFTA Section class.
partof_GLBA	To link each GLBA Policies class with GLBA Section and GLBA Titles
partof_GLBATitle	To link GLBA TITLE class with GLBA Section class.
partof_TILA	To link each TILA Policies class with TILA Section and TILA Titles
partof_TITLATitle	To link TILA TITLE class with TILA Section class.
partofProvider_Policy	To link Provider policies class present under EFTA Polices, GLBA & TILA Policies Class with Providers Class

Figure 8: Ontology Object Properties

As mentioned above, we have six more classes like Consumers, Providers, Consumer_Obligations, Consumer_Permissions, Provider_Permissions and Provider_Obligations. Classes like Consumer_Obligations, Consumer_Permissions, Provider_Permissions and Provider_Obligations contains extracted deontic expression sentences in their instances. These sentences were extracted as mentioned in Chapter 3 of this research. The two other class Consumers and Providers are created to showcase the dynamic version of our ontology. These two classes are created to infer all the consumer rules present in the classes like EFTA_Consumer_Policies, GLBA_Consumer_Policies, TILA_Consumer_Policies. Similarly, the Provider class infers all the rules present in the classes like EFTA_Provider_Policies, GLBA_Provider_Policies, TILA_Provider_Policies. In future, if we want update rules or add rules then we will have to just make changes in the related classes thus

make it easier for the end user perform query. Also, the Consumers class has data property named as “hasConsumerRules” and the Providers class has data property “hasProviderRules”. The inference part is explained later in the section showcasing the dynamic characteristic our ontology.

After the creation of Classes, Data Properties and Object Properties we created instances based on the key terms finding mentioned in chapter 3 of this search. Figure 9 below shows the Instance Count per each class in Mobile Wallets Compliance Ontology

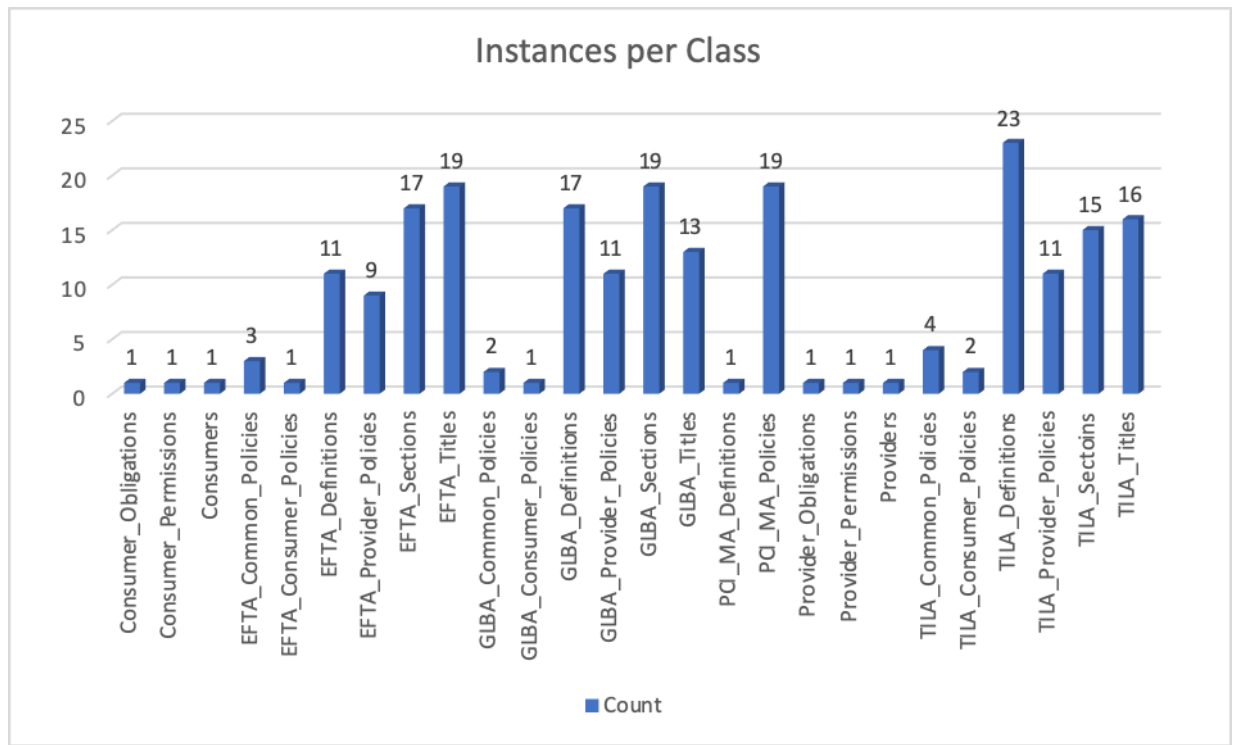


Figure 9: Instances Count per Class

Section 2: SWRL Rule

The Semantic Web Rule Language (SWRL) is considered as a proposed language for the Semantic Web that can be used to express rules as well as logic, combining OWL DL or OWL Lite with a subset of the Rule Markup Language [29]. “Rules are of the form of an implication between an antecedent (body) and consequent (head). The intended meaning can be read as:

whenever the conditions specified in the antecedent hold, then the conditions specified in the consequent must also hold” [29]. In our Mobile Wallets Ontology, we have also used SWRL to get more inference and make the Ontology much more semantically rich. Some of the rules are mentioned below:

SWRL Rules	Description
$mw:EFTA_Sections(?S) \wedge mw:partof_EFTATitle(?S, ?T) \rightarrow mw:has_EFTASectionNumber(?T, ?S)$	To infer EFTA Section number for EFTA Titles
$mw:Consumers(?S) \wedge mw:TILA_Consumer_Policies(?T) \wedge mw:TILA_hasConsumerLiability(?T, ?Z) \rightarrow mw:hasConsumerRules(?S, ?Z)$	To get the Data Property under Consumer class from TILA_Consumer class
$mw:Providers(?T) \wedge mw:partofProvider_Policy(?S, ?T) \wedge mw:TILA_Provider_Policies(?S) \rightarrow mw:hasProviderPolicies(?T, ?S)$	To get all the individuals under Provider class from TILA_Provider class
$mw:GLBA_Consumer_Policies(?S) \wedge mw:Consumers(?T) \wedge mw:partof_ConsumerPolicy(?S, ?T) \rightarrow mw:hasConsumerPolicies(?T, ?S)$	To get all the individuals under Consumer class from GLBA_Consumer class
$mw:TILA_Consumer_Policies(?S) \wedge mw:Consumers(?T) \wedge mw:partof_ConsumerPolicy(?S, ?T) \rightarrow mw:hasConsumerPolicies(?T, ?S)$	To get all the individuals under Consumer class from TILA_Consumer class
$mw:partof_GLBATitle(?S, ?T) \wedge mw:GLBA_Titles(?T) \wedge mw:GLBA_Sections(?S) \rightarrow mw:has_GLBASectionNumber(?T, ?S)$	To fetch GLBA Title's Section Number
$mw:EFTA_Policies(?S) \wedge mw:partof_EFTA(?T, ?S) \wedge mw:EFTA_Sections(?T) \rightarrow mw:has_EFTASectionNumber(?S, ?T)$	To infer EFTA Section number and link EFTA instances to EFTA Titles
$mw:EFTA_Policies(?S) \wedge mw:partof_EFTA(?T, ?S) \wedge mw:EFTA_Titles(?T) \rightarrow mw:partof_EFTATitle(?S, ?T)$	To infer EFTA Section number and link EFTA instances to EFTA Titles
$mw:Providers(?S) \wedge mw:TILA_Provider_Policies(?T) \wedge mw:TILA_Providers_Data_Property(?T, ?Z) \rightarrow mw:hasProviderRules(?S, ?Z)$	To get all the Data Property under Provider class from TILA_Provider class
$mw:Providers(?S) \wedge mw:GLBA_Provider_Policies(?T) \wedge mw:GLBA_Providers_Data_Property(?T, ?Z) \rightarrow mw:hasProviderRules(?S, ?Z)$	To get all the Data Property under Provider class from GLBA_Provider class
$mw:Providers(?S) \wedge mw:PCI_MA_Policies(?T) \wedge mw:PCI_MA_Property(?T, ?Z) \rightarrow mw:hasProviderRules(?S, ?Z)$	To get all the Data Property under Provider class from PCI_MA class
$mw:Providers(?T) \wedge mw:partofProvider_Policy(?S, ?T) \wedge mw:EFTA_Provider_Policies(?S) \rightarrow mw:hasProviderPolicies(?T, ?S)$	To get all the individuals under Provider class from EFTA_Provider class
$mw:Providers(?T) \wedge mw:GLBA_Provider_Policies(?S) \wedge mw:partofProvider_Policy(?S, ?T) \rightarrow mw:hasProviderPolicies(?T, ?S)$	To get all the individual under Provider class from GLBA_Provider class
$mw:EFTA_Consumer_Policies(?S) \wedge mw:Consumers(?T) \wedge mw:partof_ConsumerPolicy(?S, ?T) \rightarrow mw:hasConsumerPolicies(?T, ?S)$	To get all the individuals under Consumer class from EFTA_Consumer class
$mw:Consumers(?S) \wedge mw:EFTA_Consumer_Policies(?T) \wedge mw:hasConsumerLiability(?T, ?Z) \rightarrow mw:hasConsumerRules(?S, ?Z)$	To get all the Data Property under Consumer class from EFTA_Consumer class
$mw:Consumers(?S) \wedge mw:GLBA_Consumer_Policies(?T) \wedge mw:GLBA_hasConsumerLiability(?T, ?Z) \rightarrow mw:hasConsumerRules(?S, ?Z)$	To get the Data Property under Consumer class from GLBA_Consumer class
$mw:Consumers(?S) \wedge mw:TILA_Consumer_Policies(?T) \wedge mw:TILA_hasRescindPolicy(?T, ?Z) \rightarrow mw:hasConsumerRules(?S, ?Z)$	To get the Data Property under Consumer class from TILA_Consumer class

Figure 10: SWRL Rules

One of the results because of SWRL rules helped in linking EFTA Section class and EFTA Title class. Since Section 205.1 of EFTA Regulation [3] is named as title “Authority & Purpose”. SWRL rule helped in identifying the instance *Authority & Purpose* with object property *has_EFTASectionNumber* as part of Instance *Sec 205.1*. Please find the screenshot below:

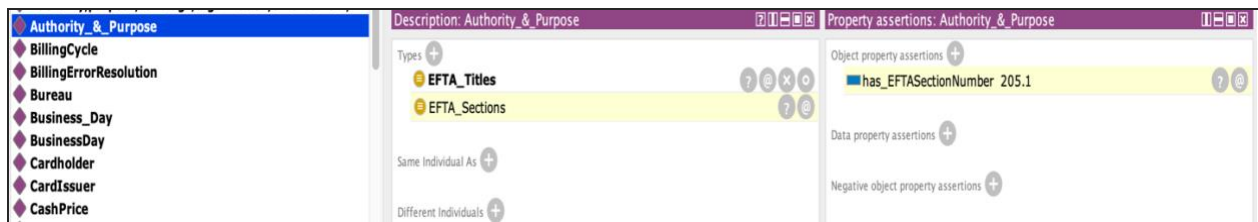


Figure 11: SWRL Rule Inference Output

Likewise SWRL rule played a major role in inferencing all the consumer property instances to the instance **Consumer_Rules**. As mentioned above, Consumer_Rules is an instance of Class

Consumer which contains all the Consumer policies applicable for Mobile Wallets Transaction Compliance. Please find the screen shot below:

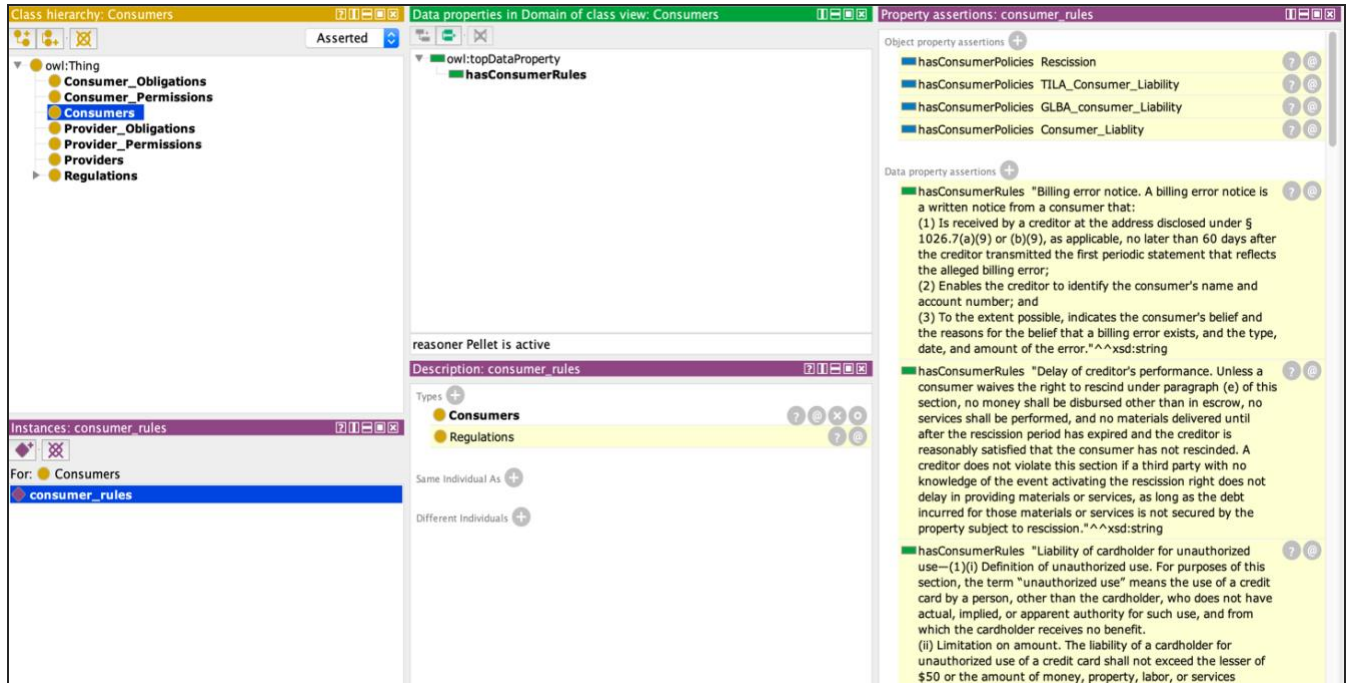


Figure 12: SWRL rule Inference Output for Consumer Class

Section 3: SPARQL Query

SPARQL stands for SPARQL Protocol and RDF Query Language and is an RDF query language—that is, a semantic query language for database which helps to retrieve and manipulate data stored in Resource Description Framework (RDF) [12] format [30]. With the help of SPARQL Query we were able to fetch the instances knowledge base and retrieve the output. The output of SPARQL queries helped us in answering all the use case questions. Please find the output screenshot to all the use case questions mentioned in Chapter 1 below. Some of the use case questions align with our consumer and providers perspective are shown below:

Consumers Perspective:

What are Consumers Obligations?

What are Consumers liabilities in-case of fraud, loss of device, theft?

What rights does the Consumer hold for Mobile Wallets compliance policies?

Providers Perspective:

What are the Provider Obligations for Mobile Wallets compliance policies?

What are Provider Obligations for resolving an error in Mobile payments involving usage of a debit card?

What disclosers policies for the Provider dealing in Mobile Payments?

What are data protection policies to be followed by the Provider when giving service like Mobile Wallets?

The output of some these use case questions is present in below Figure 13 and Figure 14 showcasing how after the building our knowledge graph SPARQL query helped in answering the key questions.

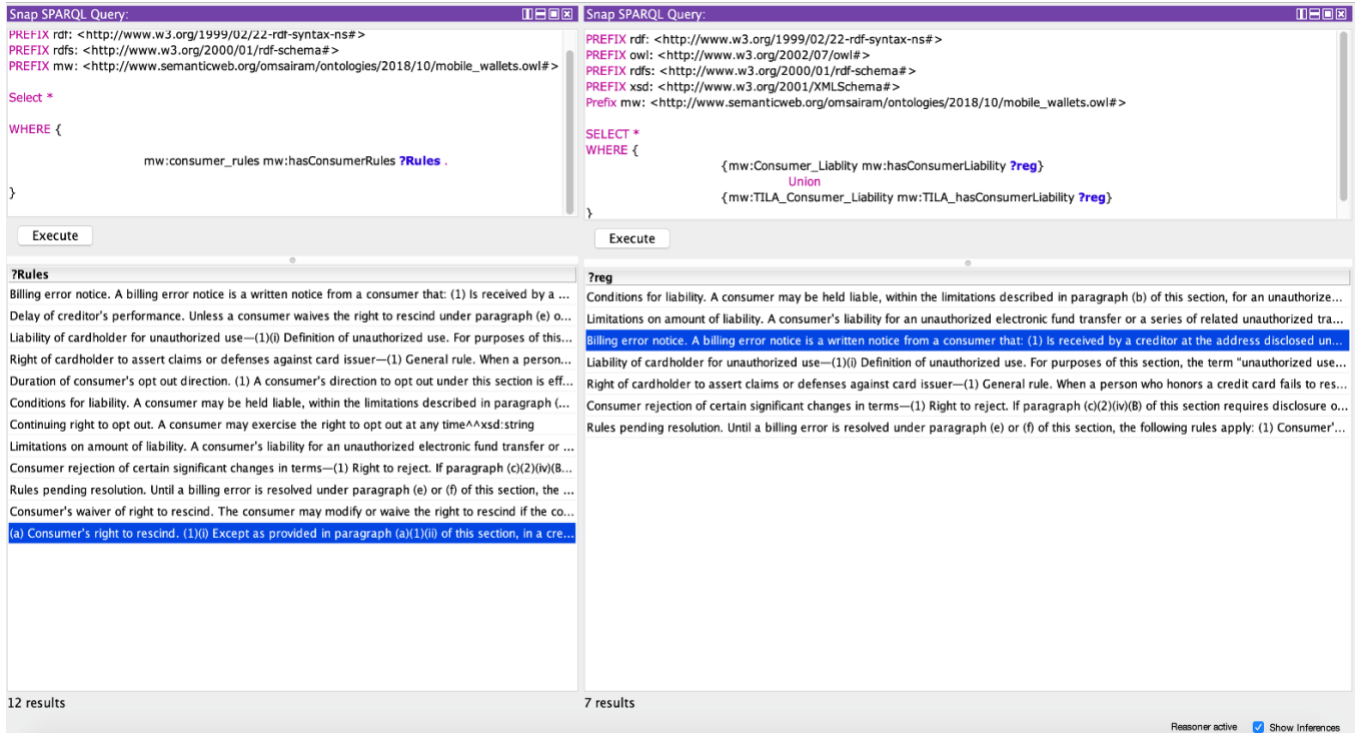


Figure 13: SPARQL Query Results - Consumers Perspective
What are consumer liabilities in case of fraud, loss of access device?

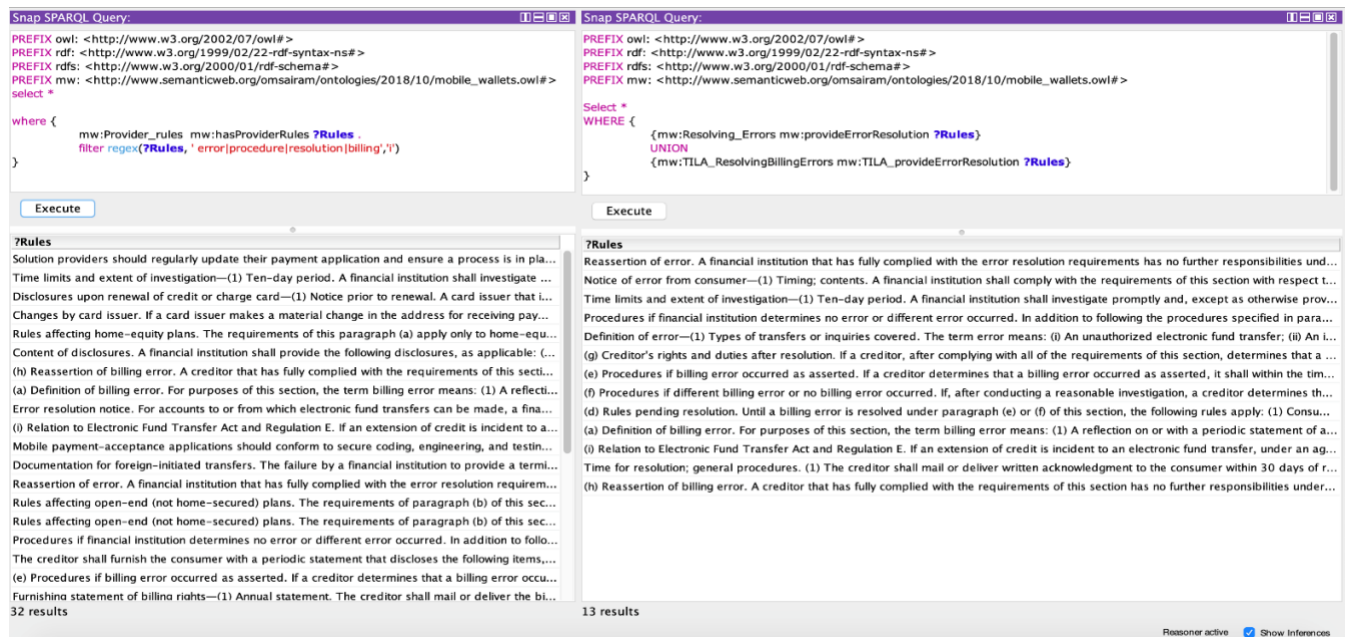


Figure 14: SPARQL Query Results Provider's Perspective
What are provider liabilities in error resolving process?

Chapter 5: Evaluation & Validation

Section 1: Evaluation Qualitative:

The evaluation was done using the two approaches Qualitative and Quantitative metrics; we have used the same use case scenarios to evaluate the knowledge graph module. Below measures were used for Qualitative approach:

Qualitative Metrics: Group of subjects measured the ontology using the below metrics and each ontology measures out of 5 (the benchmark for each measure is 3)

“**Accuracy** is a criterion that states if the definitions, descriptions of classes, properties, and individuals in an ontology are correct.” [32]

“**Completeness** measures if the domain of interest is appropriately covered in this ontology.” [32]

“**Conciseness** is the criteria that state if the ontology includes irrelevant elements with regards to the domain to be covered.” [32]

“**Adaptability** measures how far the ontology anticipates its uses. An ontology should offer the conceptual foundation for a range of anticipated tasks.” [32]

“**Clarity** measures how effectively the ontology communicates the intended meaning of the defined terms. Definitions should be objective and independent of the context.” [32]

“**Computational** efficiency measures the ability of the used tools to work with the ontology, the speed that reasoners need to fulfill the required tasks.” [32]

“**Consistency** describes that the ontology does not include or allow for any contradictions.” [32]

Average measure for each of the metrics came was 4.5 out of an overall score of 5.

Section 2: Evaluation Quantitative:

To check the accuracy rate, we considered precision and recall as main methods to figure out how many records are classified correctly to measure results relevancy and number of genuinely relevant results that are an outcome of this method. Since the basis of this scenario is on multi-class, so we need to use the sum of numerators and sum of all the denominators from below equations. Also, we checked for average accuracy in finding the average per class effectiveness of a classifier.

$$\left| \begin{array}{l} Precision = \frac{TP}{TP+FP} \\ Recall = \frac{TP}{FN+TP} \\ Accuracy = \frac{TP+TN}{FP+TN+FN+TP} \end{array} \right| [33]$$

(TP – True Positive, FN – False Negative, TN - True Negative and FP – False Positive)[33]

		Actual	
		Positive	Negative
Predicted	Positive	True Positive	False Positive
	Negative	False Negative	True Negative

Results obtained for the above measures are: Accuracy = 64.95% Precision= 55.2% Recall= 92.5%.

Another important metric that we checked is the F1 score for multi-class, which is the macro-averaged F1 score. It is calculated based on precision and recall values that we are obtained from the above equations to provide harmonic mean.

$$\left| Macro\ Averaged\ F1\ score = \frac{1}{n} \sum_{i=1}^n 2 * \frac{precision * recall}{precision + recall} \right|$$

Section 3: Validation:

For the validation process, we referenced the policies of major mobile wallet providers. We considered significant mobile wallet providers in the market where a massive number of transactions happen daily like Google Pay, Samsung Pay, Apple Pay, Venmo, Square Cash, and PayPal. We then searched for the key terms *Consumer, Error, Privacy, Disclosures, protections, statements, fraud, loss, and liability*. Figure 15 shows the policies that are used for the validation procedure and the frequency of these key terms in all the policies. We have utilized these key terms to populate the instances of respective classes in ontology.

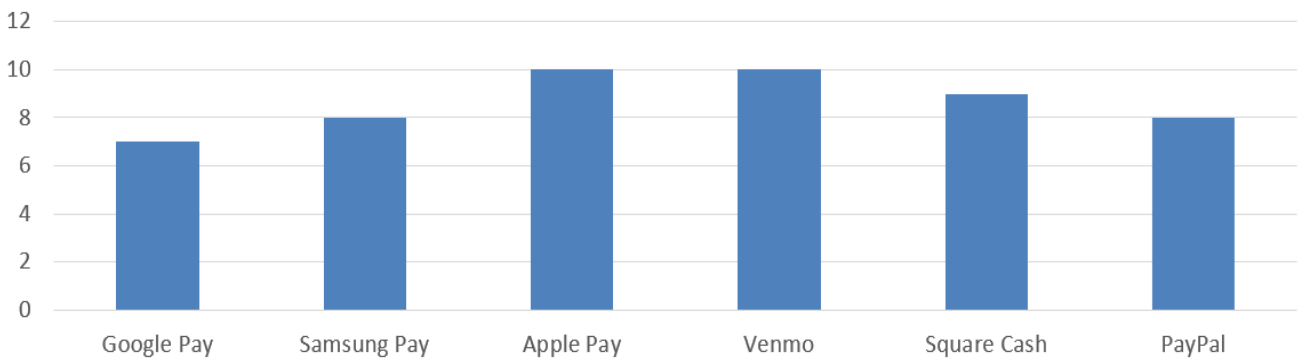


Figure 15: Validation Results

<p>B. Your Liability for Unauthorized Transfers.</p> <p>Tell us AT ONCE if you believe your Eligible Device is lost or stolen, your Credentials have been compromised, or your Apple Pay Cash Account has been accessed without your permission. Reporting such loss, theft, compromise, or unauthorized access by calling us at (877) 233-8562 is the best way of keeping your possible losses down. You could lose all the money in your Payment Account. If you tell us within 2 business days after you learn of the loss or theft of your Eligible Device, the compromise of your Credentials, or the unauthorized access of your Apple Pay Cash Account, you can lose no more than \$50 if someone used your registered Payment Account without your permission. If you do NOT tell us within 2 business days after you learn of the loss or theft of your Eligible Device, the compromise of your Credentials, or the unauthorized access of your Apple Pay Cash Account, and we can prove that we could have stopped someone from using your registered Payment Account without your permission if you had told us, you could lose as much as \$500.</p> <p>Also, if your Apple Pay Cash Account information available on your Eligible Device or any transaction history that we send you shows transfers that you did not make with your registered Payment Account, tell us at once. If you do not tell us within 60 days after: (i) you electronically access your registered Payment Account information on your Eligible Device or (ii) we provide you with a transaction history for your registered Payment Account, you may not get back any money you lost after the 60 days if we can prove that we could have stopped someone from taking money from your registered Payment Account if you had told us in time. If a good reason (such as a long trip or hospital stay) kept you from telling us, we will extend the time periods.</p>	<p>Through the Visa System below). (b) Transaction Not Routed Through the Visa System. Unauthorized transactions that are not routed through Visa are not protected by the Visa Zero Liability Protection policy. These types of transactions include point of sale, PIN, PINless or other debit transactions not processed by Visa. If you tell us within two business days after you learn of any unauthorized transactions or the loss of your PIN, you will lose no more than \$50 if someone accessed your Card Account without your permission. If you do NOT tell us within two business days after you learn of an unauthorized transaction or the loss of your PIN, and we can prove we could have stopped someone from accessing your Card Account without your permission if you had told us, you could lose as much as \$500. Also, if your Card Account transaction history or other information shows transfers that you did not make or authorize, tell us at once. If you do not tell us within 60 days after the information is made available to you, you may not get back any money you lost after the 60 days if we can prove that we could have stopped someone from taking the money if you had told us in time. If a good reason (such as a long trip, a hospital stay, or other extenuating circumstances) kept you from telling us, we will extend the times specified above to a reasonable period. You agree to cooperate reasonably with us in our attempts to recover funds from, and to assist in the prosecution of, any unauthorized users of your Card Account.</p>
<p>Apple Pay</p> <p>B. Unauthorized Payment Transactions</p> <p>Statement of Your Liability. Please tell us IMMEDIATELY if you believe your Google Payments Account username and password have been lost or stolen. You may contact us via phone at: 1-888-986-7944 or email at our Contact Us page, or by writing to us at:</p> <p>Google Payment Corp. – Complaints Handling P.O. Box 727 Mountain View, CA 94042</p> <p>Please be aware that you could lose all the money in your Google Pay Balance.</p> <p>If you inform us within 2 business days after you learn of the loss or theft of your Google Payments Account username and password, you can lose no more than \$50 if someone used your Google Payments Account username and password without your permission. However, if you do NOT inform us within 2 business days after you learn of the loss or theft of your Google Payments Account username and password, and we can prove we could have stopped someone from using your Google Payments Account username and password without your permission if you had informed us, you could lose as much as \$500.</p>	<p>error promptly. If we need more time, however, we may take up to 45 days to investigate the complaint or question. If we decide to do this, we will credit your Card Account for return of the credit amount to your Cash App within ten business days for the amount you think is in error, so that you will have the use of the funds credited to your Cash App for funding your Card Account during the time it takes us to complete our investigation. If we ask you to put your complaint in writing and we do not receive it within ten business days, we may not credit your Card Account. For errors involving new Card Accounts we may take up to 90 days to investigate a complaint or question. For new Card Accounts, we may take up to 20 business days to credit your Card Account for return of the credit amount to your Cash App for the amount you think is an error. We will tell you the results within three business days after completing our investigation. If we decide that there was no error, we will send you a written explanation. You may ask for copies of the documents that we used in our investigation. If you need more information about our error resolution process, contact Customer Service.</p>
<p>Google Pay</p>	<p>Venmo</p>

Figure 16: Key Words present in Organization policies

Chapter 6: UI Development

As shown in our architecture flow diagram, this was one of the last steps where we have built a rudimentary UI for information retrieval process. In order to build this we have utilized Python Apache Flask [34] library for web application framework along with HTML and JavaScript. For our SPARQL backend we have made use of SPARQL WRAPPER[35] library to connect our query which has end point to Apache Jena Fuseski Server. Also, Apache Jena local host address is <http://localhost:3030/> and FLASK web application local host address: <http://127.0.0.1:5000>. Below are some of the snapshots of our UI application

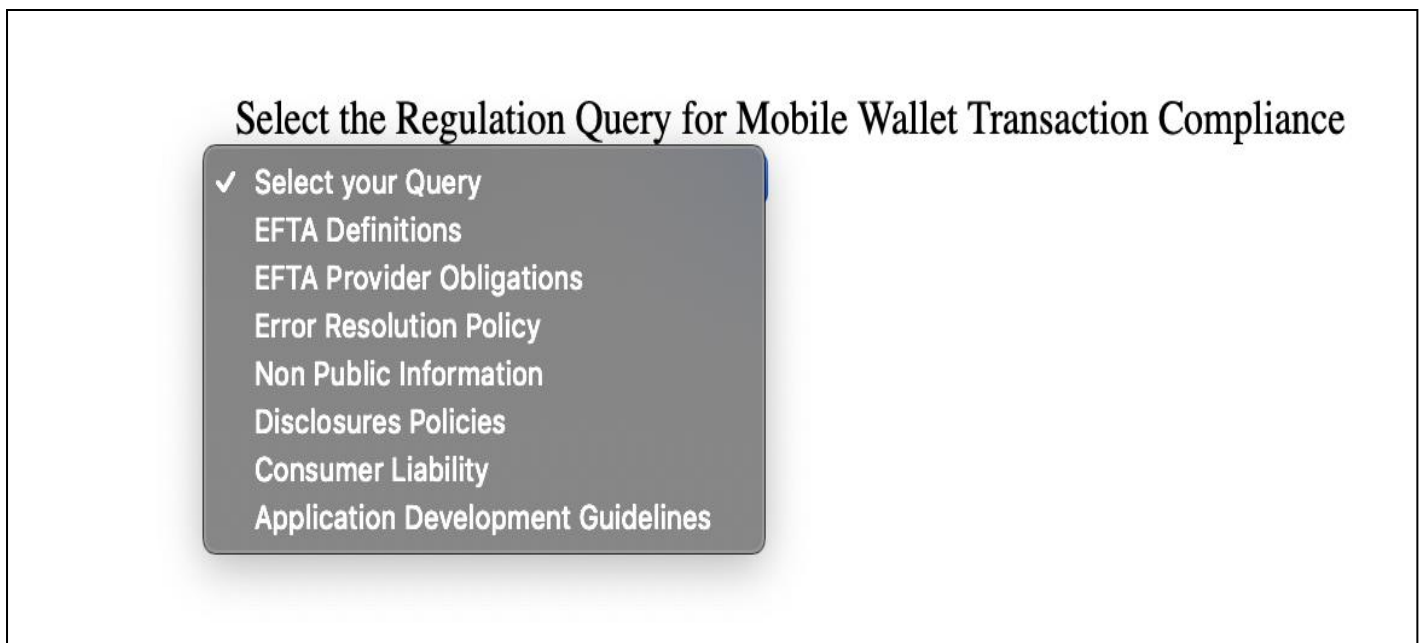


Figure 17: Drop Down menu for Use Case Scenarios

Select the Regulation Query for Mobile Wallet Transaction Compliance

EFTA Provider Obligations

Automatic transfers by account-holding institution. Any transfer of funds under an agreement between a consumer and a financial institution which provides that the institution will initiate individual transfers without a specific request from the consumer:\n(i) Between a consumer's accounts within the financial institution;\n(ii) From a consumer's account to an account of a member of the consumer's family held in the same financial institution; or\n(iii) Between a consumer's account and an account of the financial institution, except that these transfers remain subject to § 205.10(e) regarding compulsory use and sections 915 and 916 of the act regarding civil and criminal liability. ",

"Collection of returned item fees via electronic fund transfer--(i) General. The person initiating an electronic fund transfer to collect a fee for the return of an electronic fund transfer or a check that is unpaid, including due to insufficient or uncollected funds in the consumer's account, must obtain the consumer's authorization for each transfer. A consumer authorizes a one-time electronic fund transfer from his or her account to pay the fee for the returned item or transfer if the person collecting the fee provides notice to the consumer stating that the person may electronically collect the fee, and the consumer goes forward with the underlying transaction. The notice must state that the fee will be collected by means of an electronic fund transfer from the consumer's account if the payment is returned unpaid and must disclose the dollar amount of the fee. If the fee may vary due to the amount of the transaction or due to other factors, then, except as otherwise provided in paragraph (b)(3)(ii) of this section, the person collecting the fee may disclose, in place of the dollar amount of the fee, an explanation of how the fee will be determined.\n(ii) Point-of-sale transactions. If a fee for an electronic fund transfer or check returned unpaid may be collected electronically in connection with a point-of-sale transaction, the person initiating an electronic fund transfer to collect the fee must post the notice described in paragraph (b)(3)(i) of this section in a prominent and conspicuous location. The person also must either provide the consumer with a copy of the posted notice (or a substantially similar notice) at the time of the transaction, or mail the copy (or a substantially similar notice) to the consumer's address as soon as reasonably practicable after the person initiates the electronic fund transfer to collect the fee. If the amount of the fee may vary due to the amount of the transaction or due to other factors, the posted notice may explain how the fee will be determined, but the notice provided to the consumer must state the dollar amount of the fee if the amount can be calculated at the time the notice is provided or mailed to the consumer.\n(iii) Delayed compliance date for fee disclosure. Through December 31, 2007, the notice required to be provided to consumers under paragraph (b)(3)(ii) of this section in connection with a point-of-sale transaction, whether given to the consumer at the time of the transaction or subsequently mailed to the consumer, need not include either the dollar amount of any fee collected electronically for a check or electronic fund transfer returned unpaid or an explanation of how the amount of the fee will be determined.\n(c) Exclusions from coverage. The term electronic fund transfer does not include:\n(1) Checks. Any transfer of funds originated by check, draft, or similar paper instrument; or any payment made by check, draft, or similar paper instrument at an electronic terminal.\n(2) Check guarantee or authorization. Any transfer of funds that guarantees payment or authorizes acceptance of a check, draft, or similar paper instrument but that does not directly result in a debit or credit to a consumer's account.\n(3) Wire or other similar transfers. Any transfer of funds through Fedwire or through a similar wire transfer system that is used primarily for transfers between financial institutions or between businesses. ",

"Receipts at electronic terminals--General. Except as provided in paragraph (e) of this section, a financial institution shall make a receipt available to a consumer at the time the consumer initiates an electronic fund transfer at an electronic terminal. The receipt shall set forth the following information, as applicable:\n(1) Amount. The amount of the transfer. A transaction fee may be included in this amount, provided the amount of the fee is disclosed on the receipt and displayed on or at the terminal.\n(2) Date. The date the consumer initiates the transfer.\n(3) Type. The type of transfer and the type of the consumer's account(s) to or from which funds are transferred. The type of account may be omitted if the access device used is able to access only one account at that terminal.\n(4) Identification. A number or code that identifies the consumer's account or accounts, or the access device used to initiate the transfer. The number or code need not exceed four digits or letters to comply with the requirements of this paragraph (a)(4).\n(5) Terminal location. The location of the terminal where the transfer is initiated, or an identification such as a code or terminal number. Except in limited circumstances where all terminals are located in the same city or state, if the location is disclosed, it shall include the city and state or foreign country and one of the following:\n(i) The street address; or\n(ii) A generally accepted name for the specific location; or\n(iii) The name of the owner or operator of the terminal if other than the account-holding institution.\n(6) Third party transfer. The name of any third party to or from whom funds are transferred. ",

"Exception for receipts in small-value transfers. A financial institution is not subject to the requirement to make available a receipt under paragraph (a) of this section if the amount of the transfer is \$15 or less ",

"Extension of time limits. If the consumer's delay in notifying the financial institution was due to extenuating circumstances, the institution shall extend the times specified above to a reasonable period. ",

"Notice to financial institution. (i) Notice to a financial institution is given when a consumer takes steps reasonably necessary to provide the institution with the pertinent information, whether or not a particular employee or agent of the institution actually receives the information.\n(ii) The consumer may notify the institution in person, by telephone, or in writing.\n(iii) Written notice is considered given at the time the consumer mails the notice or delivers it for transmission to the institution by any other usual means. Notice may be considered constructively given when the institution becomes aware of circumstances leading to the reasonable belief that an unauthorized transfer to or from the consumer's account has been or may be made. ",

"Periodic statements. For an account to or from which electronic fund transfers can be made, a financial institution shall send a periodic statement for each monthly cycle in which a net electronic fund transfer has occurred; and shall send a periodic statement at least quarterly if no transfer has occurred. The statement shall set forth the following information, as applicable:\n(1) Transaction information. For each electronic fund transfer occurring during the cycle:\n(i) The amount of the transfer;\n(ii) The date the transfer was credited o

Figure 18: Regulation for EFTA Provider Obligations

Select the Regulation Query for Mobile Wallet Transaction Compliance

Consumer Liability

Conditions for liability. A consumer may be held liable, within the limitations described in paragraph (b) of this section, for an unauthorized electronic fund transfer involving the consumer's account only if the financial institution has provided the disclosures required by § 205.7(b)(1), (2), and (3). If the unauthorized transfer involved an access device, it must be an accepted access device and the financial institution must have provided a means to identify the consumer to whom it was issued ",

"Limitations on amount of liability. A consumer's liability for an unauthorized electronic fund transfer or a series of related unauthorized transfers shall be determined as follows:
 \n(1) Timely notice given. If the consumer notifies the financial institution within two business days after learning of the loss or theft of the access device, the consumer's liability shall not exceed the lesser of \$50 or the amount of unauthorized transfers that occur before notice to the financial institution.\n(2) Timely notice not given. If the consumer fails to notify the financial institution within two business days after learning of the loss or theft of the access device, the consumer's liability shall not exceed the lesser of \$500 or the sum of:\n(i) \$50 or the amount of unauthorized transfers that occur within the two business days, whichever is less; and\n(ii) The amount of unauthorized transfers that occur after the close of two business days and before notice to the institution, provided the institution establishes that these transfers would not have occurred had the consumer notified the institution within that two-day period.\n(3) Periodic statement; timely notice not given. A consumer must report an unauthorized electronic fund transfer that appears on a periodic statement within 60 days of the financial institution's transmittal of the statement to avoid liability for subsequent transfers. If the consumer fails to do so, the consumer's liability shall not exceed the amount of the unauthorized transfers that occur after the close of the 60 days and before notice to the institution, and that the institution establishes would not have occurred had the consumer notified the institution within the 60-day period. When an access device is involved in the unauthorized transfer, the consumer may be liable for other amounts set forth in paragraphs (b)(1) or (b)(2) of this section, as applicable.\n(4) Extension of time limits. If the consumer's delay in notifying the financial institution was due to extenuating circumstances, the institution shall extend the times specified above to a reasonable period.\n(5) Notice to financial institution. (i) Notice to a financial institution is given when a consumer takes steps reasonably necessary to provide the institution with the pertinent information, whether or not a particular employee or agent of the institution actually receives the information.\n(ii) The consumer may notify the institution in person, by telephone, or in writing.\n(iii) Written notice is considered given at the time the consumer mails the notice or delivers it for transmission to the institution by any other usual means. Notice may be considered constructively given when the institution becomes aware of circumstances leading to the reasonable belief that an unauthorized transfer to or from the consumer's account has been or may be made.\n(6) Liability under state law or agreement. If state law or an agreement between the consumer and the financial institution imposes less liability than is provided by this section, the consumer's liability shall not exceed the amount imposed under the state law or agreement. ",

"Liability of cardholder for unauthorized use--(1)(i) Definition of unauthorized use. For purposes of this section, the term "unauthorized use" means the use of a credit card by a person, other than the cardholder, who does not have actual, implied, or apparent authority for such use, and from which the cardholder receives no benefit.\n(ii) Limitation on amount. The liability of a cardholder for unauthorized use of a credit card shall not exceed the lesser of \$50 or the amount of money, property, labor, or services obtained by the unauthorized use before notification to the card issuer under paragraph (b)(3) of this section.\n(2) Conditions of liability. A cardholder shall be liable for unauthorized use of a credit card only if:\n(i) The credit card is an accepted credit card;\n(ii) The card issuer has provided adequate notice of the cardholder's maximum potential liability and of means by which the card issuer may be notified of loss or theft of the card. The notice shall state that the cardholder's liability shall not exceed \$50 (or any lesser amount) and that the cardholder may give oral or written notification, and shall describe a means of notification (for example, a telephone number, an address, or both); and\n(iii) The card issuer has provided a means to identify the cardholder on the account or the authorized user of the card.\n(3) Notification to card issuer. Notification to a card issuer is given when steps have been taken as may be reasonably required in the ordinary course of business to provide the card issuer with the pertinent information about the loss, theft, or possible unauthorized use of a credit card, regardless of whether any particular officer, employee, or agent of the card issuer does, in fact, receive the information. Notification may be given, at the option of the person giving it, in person, by telephone, or in writing. Notification in writing is considered given at the time of receipt or, whether or not received, at the expiration of the time ordinarily required for transmission, whichever is earlier.\n(4) Effect of other applicable law or agreement. If state law or an agreement between a cardholder and the card issuer imposes lesser liability than that provided in this paragraph, the lesser liability shall govern.\n(5) Business use of credit cards. If 10 or more credit cards are issued by one card issuer for use by the employees of an organization, this section does not prohibit the card issuer and the organization from agreeing to liability for unauthorized use without regard to this section. However, liability for unauthorized use may be imposed on an employee of the organization, by either the card issuer or the organization, only in accordance with this section ",

"Billing error notice. A billing error notice is a written notice from a consumer that:\n(1) Is received by a creditor at the address disclosed under § 1026.7(a)(9) or (b)(9), as applicable, no later than 60 days after the creditor transmitted the first periodic statement that reflects the alleged billing error;\n(2) Enables the creditor to identify the consumer's name and account number; and\n(3) To the extent possible, indicates the consumer's belief and the reasons for the belief that a billing error exists, and the type, date, and amount of the error. ",

"Right of cardholder to assert claims or defenses against card issuer--(1) General rule. When a person who honors a credit card fails to resolve satisfactorily a dispute as to property or services purchased with the credit card in a consumer credit transaction, the cardholder may assert against the card issuer all claims (other than tort claims) and defenses arising out of the transaction and relating to the failure to resolve the dispute. The cardholder may withhold payment up to the amount of credit outstanding for the property or services that gave rise to the dispute and any finance or other charges imposed on that amount.\n(2) Adverse credit reports prohibited. If, in accordance with paragraph (c)(1) of this section, the cardholder withholds payment of the amount of credit outstanding for the disputed transaction, the card issuer shall not report that amount as delinquent until the dispute is settled or judgment is rendered.\n(3) Limitations--(i) General. The rights stated in paragraphs (c)(1) and (c)(2) of this section apply only if:\n(A) The cardholder has made a good faith

Figure 19: Regulation for Consumer Liability

Select the Regulation Query for Mobile Wallet Transaction Compliance

Error Resolution Policy

Definition of error—(1) Types of transfers or inquiries covered. The term error means:\n(i) An unauthorized electronic fund transfer;\n(ii) An incorrect electronic fund transfer to or from the consumer's account;\n(iii) The omission of an electronic fund transfer from a periodic statement;\n(iv) A computational or bookkeeping error made by the financial institution relating to an electronic fund transfer;\n(v) The consumer's receipt of an incorrect amount of money from an electronic terminal;\n(vi) An electronic fund transfer not identified in accordance with §§ 205.9 or 205.10(a); or\n(vii) The consumer's request for documentation required by §§ 205.9 or 205.10(a) or for additional information or clarification concerning an electronic fund transfer, including a request the consumer makes to determine whether an error exists under paragraphs (a)(1) (i) through (vi) of this section.\n(2) Types of inquiries not covered. The term error does not include:\n(i) A routine inquiry about the consumer's account balance;\n(ii) A request for information for tax or other recordkeeping purposes; or\n(iii) A request for duplicate copies of documentation. ",

"Procedures if financial institution determines no error or different error occurred. In addition to following the procedures specified in paragraph (c) of this section, the financial institution shall follow the procedures set forth in this paragraph (d) if it determines that no error occurred or that an error occurred in a manner or amount different from that described by the consumer:\n(1) Written explanation. The institution's report of the results of its investigation shall include a written explanation of the institution's findings and shall note the consumer's right to request the documents that the institution relied on in making its determination. Upon request, the institution shall promptly provide copies of the documents.\n(2) Debiting provisional credit. Upon debiting a provisionally credited amount, the financial institution shall:\n(i) Notify the consumer of the date and amount of the debiting;\n(ii) Notify the consumer that the institution will honor checks, drafts, or similar instruments payable to third parties and preauthorized transfers from the consumer's account (without charge to the consumer as a result of an overdraft) for five business days after the notification. The institution shall honor items as specified in the notice, but need honor only items that it would have paid if the provisionally credited funds had not been debited. ",

"Time limits and extent of investigation—(1) Ten-day period. A financial institution shall investigate promptly and, except as otherwise provided in this paragraph (c), shall determine whether an error occurred within 10 business days of receiving a notice of error. The institution shall report the results to the consumer within three business days after completing its investigation. The institution shall correct the error within one business day after determining that an error occurred.\n(2) Forty-five day period. If the financial institution is unable to complete its investigation within 10 business days, the institution may take up to 45 days from receipt of a notice of error to investigate and determine whether an error occurred, provided the institution does the following:\n(i) Provisionally credits the consumer's account in the amount of the alleged error (including interest where applicable) within 10 business days of receiving the error notice. If the financial institution has a reasonable basis for believing that an unauthorized electronic fund transfer has occurred and the institution has satisfied the requirements of § 205.6(a), the institution may withhold a maximum of \$50 from the amount credited. An institution need not provisionally credit the consumer's account if:\n(A) The institution requires but does not receive written confirmation within 10 business days of an oral notice of error; or\n(B) The alleged error involves an account that is subject to Regulation T (Securities Credit by Brokers and Dealers, 12 CFR part 220);\n(ii) Informs the consumer, within two business days after the provisional crediting, of the amount and date of the provisional crediting and gives the consumer full use of the funds during the investigation;\n(iii) Corrects the error, if any, within one business day after determining that an error occurred; and\n(iv) Reports the results to the consumer within three business days after completing its investigation (including, if applicable, notice that a provisional credit has been made final).\n(3) Extension of time periods. The time periods in paragraphs (c)(1) and (c)(2) of this section are extended as follows:\n(i) The applicable time is 20 business days in place of 10 business days under paragraphs (c)(1) and (c)(2) of this section if the notice of error involves an electronic fund transfer to or from the account within 30 days after the first deposit to the account was made.\n(ii) The applicable time is 90 days in place of 45 days under paragraph (c)(2) of this section, for completing an investigation, if a notice of error involves an electronic fund transfer that:\n(A) Was not initiated within a state;\n(B) Resulted from a point-of-sale debit card transaction; or\n(C) Occurred within 30 days after the first deposit to the account was made.\n(4) Investigation. With the exception of transfers covered by § 205.14, a financial institution's review of its own records regarding an alleged error satisfies the requirements of this section if:\n(i) The alleged error concerns a transfer to or from a third party; and\n(ii) There is no agreement between the institution and the third party for the type of electronic fund transfer involved ",

"Reassertion of error. A financial institution that has fully complied with the error resolution requirements has no further responsibilities under this section should the consumer later reassert the same error, except in the case of an error asserted by the consumer following receipt of information provided under paragraph (a)(1)(vii) of this section. ",

"Notice of error from consumer—(1) Timing; contents. A financial institution shall comply with the requirements of this section with respect to any oral or written notice of error from the consumer that:\n(i) Is received by the institution no later than 60 days after the institution sends the periodic statement or provides the passbook documentation, required by § 205.9, on which the alleged error is first reflected;\n(ii) Enables the institution to identify the consumer's name and account number; and\n(iii) Indicates why the consumer believes an error exists and includes to the extent possible the type, date, and amount of the error, except for requests described in paragraph (a)(1)(vii) of this section.\n(2) Written confirmation. A financial institution may require the consumer to give written confirmation of an error within 10 business days of an oral notice. An institution that requires written confirmation shall inform the consumer of the requirement and provide the address where confirmation must be sent when the consumer gives the oral notification.\n(3) Request for documentation or clarifications. When a notice of error is based on documentation or clarification that the consumer requested under paragraph (a)(1)(vii) of this section, the consumer's notice of error is timely if received by the financial institution no later than 60 days after the institution sends the information requested. ",

"(h) Reassertion of billing error. A creditor that has fully complied with the requirements of this section has no further responsibilities under this section (other than as provided in paragraph (g)(4) of this section) if a consumer reasserts substantially the same billing error. ",

Figure 20: Regulation for Error Resolution Policy

Chapter 7: Conclusion & Future Work

In this work, we have used PCI-DSS and mobile wallet policies to create a knowledge graph. As these regulations are in textual format, it is difficult for the organizations to check if they are following all the regulations listed in these vast documents. In the process of converting the textual documents into an ontology, we first utilized the regulations text to identify the most common terms. Once the key terms are identified, we have searched them in the organizational policies. As most of the key terms occurred in multiple organizational policies, we have used them to populate the instances of related classes our ontology.

Overall, as the study is done on various organizational policies, the assurance in ontology is decent and can be applied to any organization privacy document. This ontology can be used to send the notification to consumers or provider if there is any violation. We have also built a rudimentary UI in showing the information retrieval process. One interesting observation is that most of the key terms are found in all the mobile wallet policies that are used in this research.

In terms of our future work, we are working on building the module to implement the methodology like Apache Lucene and Elastic search which will help in full text search as part of information retrieval process. Also, we will look into incorporating semantically similar terms present in policies to make the overall process richer and more efficient.

Chapter 8: Appendix

8.1 Code for key terms and Deontic logic

```
import math
import xml.etree.ElementTree as ET
import re
import nltk
from nltk.corpus import stopwords
from nltk.stem.porter import PorterStemmer
from nltk.tokenize import RegexpTokenizer
from nltk.stem.wordnet import WordNetLemmatizer
from nltk.tokenize import word_tokenize
from wordcloud import WordCloud, STOPWORDS, ImageColorGenerator
import matplotlib.pyplot as plt
from sklearn.feature_extraction.text import CountVectorizer
import re
from nltk.tokenize import PunktSentenceTokenizer

def tf(word, blob):
    return blob.words.count(word) / len(blob.words)

def n_containing(word, bloblist):
    return 1 + sum(1 for blob in bloblist if word in blob)

def idf(word, bloblist):
    return math.log(float(1 + len(bloblist)) / float(n_containing(word, bloblist)))

def tfidf(word, blob, bloblist):
    return tf(word, blob) * idf(word, bloblist)

md = set()
section_number = []
section_titles = []
section_details = []
section_details1 = []

source1 = open('/Users/omsairam/Desktop/Financial Regulations research/Data
Set/Research_Data_Set/CFR_EFTA.xml')
```



```

tree = ET.parse(source1)
root = tree.getroot()

for child in root.iter('SECTION'):
    list1 = []

    for sect_no in child.iter('SECTNO'):
        list1.append(sect_no.text)
        # print(sect_no.text)
    for section_t in child.iter('SUBJECT'):
        list1.append(section_t.text)
        # print(section_t.text)
    for content in child.iter('P'):
        list1.append(content.text)
        for content_details in content:
            list1.append(content_details.text)
            list1.append(content_details.tail)

    body = ".join(str(word) for word in list1).lower()
    section_details1.append(body)
section_details = list(filter(None, section_details1))
#print(section_details)
provider_list = ['institutions','institution']

obligations = ['shall', 'should', 'must']
permissions = ['may', 'can', 'could', 'will']

consumer=[]
provider=[]
c_ob = []
c_perm=[]
p_ob=[]
p_perm=[]
consumer_permissions=[]

for reg_details in section_details:
    if any(word in reg_details for word in provider_list):
        provider.append(reg_details)
    else:
        consumer.append(reg_details)

# print(provider)

for details_pro in provider:

    tokenized_sentences = nltk.sent_tokenize(str(details_pro))

```

```

tokenized_words_in_sentences = [nltk.word_tokenize(file) for file in tokenized_sentences]
# # use pos_tag function with tagset='universal' for other charset
pos_sentences = [nltk.pos_tag(words_in_sentence) for words_in_sentence in
tokenized_words_in_sentences]

```

```

for sentences in pos_sentences:

```

```

    for i in range(0, len(sentences)):
        # print(sentences)

        if sentences[i][0] in obligations:
            if sentences[i+1][1] == 'VB':
                p_ob.append(sentences)

        elif sentences[i][0] in permissions:
            if sentences[i + 1][1] == 'VB':
                p_perm.append(sentences)

```

```

for details_con in consumer:

```

```

    tokenized_sentences = nltk.sent_tokenize(str(details_con))
    tokenized_words_in_sentences = [nltk.word_tokenize(file) for file in tokenized_sentences]
    # # use pos_tag function with tagset='universal' for other charset
    pos_sentences = [nltk.pos_tag(words_in_sentence) for words_in_sentence in
tokenized_words_in_sentences]

```

```

for sentences in pos_sentences:

```

```

    for i in range(0, len(sentences)):
        # print(sentences)

        if sentences[i][0] in obligations:
            if sentences[i+1][1] == 'VB':
                c_ob.append(sentences)

        elif sentences[i][0] in permissions:
            if sentences[i + 1][1] == 'VB':
                c_perm.append(sentences)

```

```

print(len(c_perm))
print(len(c_ob))

```

```
print(len(p_perm))
print(len(p_ob))
```

```
document1 = section_details[0].lower()
document2 = section_details[1].lower()
document3 = section_details[2].lower()
document4 = section_details[3].lower()
document5 = section_details[4].lower()
document6 = section_details[5].lower()
document7 = section_details[6].lower()
document8 = section_details[7].lower()
document9 = section_details[8].lower()
document10 = section_details[9].lower()
document11 = section_details[10].lower()
document12 = section_details[11].lower()
document13 = section_details[12].lower()
document14 = section_details[13].lower()
document15 = section_details[14].lower()
document16 = section_details[15].lower()
document17 = section_details[16].lower()
document18 = section_details[17].lower()
document19 = section_details[18].lower()
document20 = section_details[19].lower()
```

```
blob1 = tb(document1)
blob2 = tb(document2)
blob3 = tb(document3)
blob4 = tb(document4)
blob5 = tb(document5)
blob6 = tb(document6)
blob7 = tb(document7)
blob8 = tb(document8)
blob9 = tb(document9)
blob10 = tb(document10)
blob11 = tb(document11)
blob12 = tb(document12)
blob13 = tb(document13)
blob14 = tb(document14)
blob15 = tb(document15)
blob16 = tb(document16)
blob17 = tb(document17)
blob18 = tb(document18)
blob19 = tb(document19)
blob20 = tb(document20)
```

```

bloblist = [blob1, blob2, blob3, blob4, blob5, blob6, blob7, blob8, blob9,
            blob10, blob11, blob12, blob13, blob14, blob15, blob16, blob17, blob18]
new_word = []

for i, blob in enumerate(bloblist):
    print("Top words in document {}".format(i + 1))
    scores = {word: tfidf(word, blob, bloblist) for word in blob.words}
    sorted_words = sorted(scores.items(), key=lambda x: x[1], reverse=True)
    for word, score in sorted_words[:10]:
        print("\tWord: {}, TF-IDF: {}".format(word, round(score, 5)))

```

8.2 Code for word Cloud

```

import math
import pandas as pd
import re
import nltk
#nltk.download('stopwords')
from nltk.corpus import stopwords
from nltk.stem.porter import PorterStemmer
from nltk.tokenize import RegexpTokenizer
#nltk.download('wordnet')
from nltk.stem.wordnet import WordNetLemmatizer

dataset = pd.read_csv('/Users/omsairam/Desktop/Financial Regulations research/Data
Set/EFTA.txt', engine='python', sep='\s*', encoding='ISO-8859-1')
#Fetch wordcount for each abstract

# print(dataset['Regulation'])
dataset['word_count'] = dataset.apply(lambda x: len(str(x)))
print(dataset['word_count'])

# print(dataset.word_count.describe())

freq = pd.Series(' '.join(dataset).split()).value_counts()[:20]
print(freq)

freq1 = pd.Series(' '.join(dataset
                            ).split()).value_counts()[-20:]

print(freq1)
stop_words = set(stopwords.words('english'))
corpus = []

```

```

for i in range(0, 557):
    # Remove punctuations
    text = re.sub('[^a-zA-Z]', ' ', str(dataset))

    # Convert to lowercase
    text = text.lower()

    # remove tags
    text = re.sub("</?.*?>", " <& ", text)

    # remove special characters and digits
    text = re.sub("(\\d|\\W)+", " ", text)

    ##Convert to list from string
    text = text.split()

    ##Stemming
    ps = PorterStemmer()
    # Lemmatisation
    lem = WordNetLemmatizer()
    text = [lem.lemmatize(word) for word in text if not word in
            stop_words]

    text = " ".join(text)
    corpus.append(text)
# print(corpus)
from os import path
from PIL import Image

from wordcloud import WordCloud, STOPWORDS, ImageColorGenerator
import matplotlib.pyplot as plt
wordcloud = WordCloud(
    background_color='white',
    stopwords=stop_words,
    max_words=100,
    max_font_size=50,
    random_state=42
).generate(str(corpus))
print(wordcloud)
fig = plt.figure(1)
plt.imshow(wordcloud)
plt.axis('off')
plt.show()
fig.savefig("word1.png", dpi=900)

from sklearn.feature_extraction.text import CountVectorizer
import re

```

```

cv=CountVectorizer(max_df=0.8,stop_words=stop_words, max_features=10000,
ngram_range=(1,3))
X=cv.fit_transform(corpus)

```

8.3 Python Code for UI development using Apache Flask and SPARQL Wrapper

```

#!/usr/bin/env python
from SPARQLWrapper import SPARQLWrapper, JSON, SPARQLWrapper2
from flask import Flask, render_template, jsonify, request

app = Flask(__name__)

objlist = []

@app.route('/getres', methods=['GET', 'POST'])
def getETFA_Definitions():
    valType = request.get_data().decode('utf-8')
    # print("hello")
    # print(valType)
    if valType == "EFTA Definitions":
        sparql = SPARQLWrapper2("http://localhost:3030/ds")
        sparql.setMethod("POST")
        body = f"""
        PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
        PREFIX owl: <http://www.w3.org/2002/07/owl#>
        PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
        PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
        Prefix mw:
        <http://www.semanticweb.org/omsairam/ontologies/2018/10/mobile_wallets.owl#>
        SELECT *
        WHERE {{ ?define rdf:type mw:EFTA_Definitions.
                ?define mw:EFTA_means ?mean }}
        """

    elif valType == "What are EFTA Providers Obligations?":
        sparql = SPARQLWrapper2("http://localhost:3030/ds")
        sparql.setMethod("POST")
        body = """
        PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
        PREFIX owl: <http://www.w3.org/2002/07/owl#>
        PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
        PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
        Prefix mw:
        <http://www.semanticweb.org/omsairam/ontologies/2018/10/mobile_wallets.owl#>

```

```

SELECT *
WHERE {{mw:Coverage mw:hasCoverage ?reg} UNION {mw:Receipts
mw:provideReceipts ?reg}
UNION
      {mw:Provider_Liability mw:hasProviderLiability ?reg}
UNION
      {mw:Periodic_Statements mw:provideStatement ?reg}
UNION
      {mw:Initial_Disclosures mw:provideInitialDisclosures ?reg}
UNION
      {mw:Resolving_Errors mw:provideErrorResolution ?reg}
UNION
      {mw:Terms_Notice mw:provideNotice ?reg}
UNION
      {mw:General_Disclosures mw:provideGeneralDisclosures ?reg}
UNION
      {mw:Preauthorized_Transfers mw:providePreauthorizedTransferNotice ?reg}}
"""

```

elif valType == "What are Error resolution policies for Providers?":

```
sparql = SPARQLWrapper2("http://localhost:3030/ds")
```

```
sparql.setMethod("POST")
```

```
body = """
```

```
    PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
```

```
    PREFIX owl: <http://www.w3.org/2002/07/owl#>
```

```
    PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
```

```
    PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
```

```
    Prefix mw:
```

```
<http://www.semanticweb.org/omsairam/ontologies/2018/10/mobile_wallets.owl#>
```

```
    Select *
```

```
    WHERE {{mw:Resolving_Errors mw:provideErrorResolution ?reg}
```

```
    UNION
```

```
    {mw:TILA_ResolvingBillingErrors mw:TILA_provideErrorResolution
```

```
?reg}}
```

```
    """
```

elif valType == "What policies should providers follow for notices regarding non public personal information?":

```
sparql = SPARQLWrapper2("http://localhost:3030/ds")
```

```
sparql.setMethod("POST")
```

```
body = """
```

```
    PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
```

```
    PREFIX owl: <http://www.w3.org/2002/07/owl#>
```

```
    PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
```

```
    PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
```

```
    Prefix mw:
```

```
<http://www.semanticweb.org/omsairam/ontologies/2018/10/mobile_wallets.owl#>
```

```
    SELECT *
```

```

        WHERE { {mw:InitialPrivacyNotice mw:GLBA_provideInitialNotice ?reg}
        Union
        {mw:OptOutForm mw:GLBA_hasOptOutNotice ?reg}
        UNION
        {mw:DisclosureLimits mw:GLBA_provideDiscloserLimits ?reg}
        UNION
        {mw:SharingLimits mw:GLBA_provideSharingInfoLimits ?reg} }

    """
elif valType == "What disclosures policies should providers adhere to?":
    sparql = SPARQLWrapper2("http://localhost:3030/ds")
    sparql.setMethod("POST")
    body = """
        PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
        PREFIX owl: <http://www.w3.org/2002/07/owl#>
        PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
        PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
        Prefix mw:
        <http://www.semanticweb.org/omsairam/ontologies/2018/10/mobile_wallets.owl#>
        SELECT *
        WHERE {

            {mw:General_Disclosures mw:provideGeneralDisclosures ?reg}
            Union
            {mw:Initial_Disclosures mw:provideInitialDisclosures ?reg}
            UNION
            {mw:TILA_DisclosureRequirements
mw:TILA_provideDisclosure_requirements ?reg}
            Union
            {mw:TILA_General_Disclosures mw:TILA_provideGeneralDisclosures
?reg}

            UNION
            {mw:TILA_Initial_Disclosures
mw:TILA_provideAccountOpeningDisClosures ?reg}
        }
    """
elif valType == "What are consumer liabilities in case of fraud, loss of access device?":
    sparql = SPARQLWrapper2("http://localhost:3030/ds")
    sparql.setMethod("POST")
    body = """
        PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
        PREFIX owl: <http://www.w3.org/2002/07/owl#>
        PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
        PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
        Prefix mw:
        <http://www.semanticweb.org/omsairam/ontologies/2018/10/mobile_wallets.owl#>

```



```

SELECT *
WHERE {
    {mw:Consumer_Liability mw:hasConsumerLiability ?reg}
    Union
    {mw:TILA_Consumer_Liability mw:TILA_hasConsumerLiability
?reg}

    }
}

"""
elif valType == "What guidelines are required for mobile payment applications?":
    sparql = SPARQLWrapper2("http://localhost:3030/ds")
    sparql.setMethod("POST")
    body = """
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX owl: <http://www.w3.org/2002/07/owl#>
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
Prefix mw:
<http://www.semanticweb.org/omsairam/ontologies/2018/10/mobile_wallets.owl#>
SELECT *
WHERE {
    {mw:AccountDataEntry mw:AccountDataEntry ?reg}
    Union
    {mw:Application mw:PCI_MA_provideApplicationHardening ?reg}
    Union
    {mw:AuditMechanisms mw:PCI_MA_hasAdutingPolicy ?reg}
    Union
    {mw:CodingSecurity mw:PCI_MA_hasSecurePolicy ?reg}
    UNION
    {mw:EscalationPrivilege mw:PCI_MA_hasPrivilegesPolicy ?reg }
    UNION
    {mw:LogicalDeviceAccess mw:PCI_MA_hasServerSideControlsPolicy
?reg}

    UNION
    {mw:MalwareDetection mw:PCI_MA_hasMalwarePolicy ?reg}
    UNION
    {mw:PaymentDisability
mw:PCI_MA_hasRemotelyDisablePolicy ?reg}
    UNION
    {mw:ProtectionRules
mw:PCI_MA_hasUnauthorizeAccessPolicy ?reg}
    UNION
    {mw:Receipt mw:PCI_MA_hasSecureMerchantReceipts ?reg}
    UNION
    {mw:SecureState mw:PCI_MA_hasSecureStatePolicy ?reg}
    UNION

```

```

        {mw:ServerSideControls
mw:PCI_MA_hasServerSideControlsPolicy ?reg}
        UNION
        {mw:StoredData mw:PCI_MA_hasCompromiseProtections ?reg}
        UNION
        {mw:SupportingSystems mw:PCI_MA_provideHardeningPolicy
?reg}
        UNION
        {mw:TheftDetection mw:PCI_MA_hastheftpolicy ?reg}
        UNION
        {mw:TransmitData mw:PCI_MA_hasTrasmissionPolicy ?reg}
        UNION
        {mw:UnauthorizeApplication
mw:PCI_MA_hasUnauthorizedApplicationPolicy ?reg}
        UNION
        {mw:UnauthorizeAttachment
mw:PCI_MA_hasUnauthorizeAttachmentPolicy ?reg}
        UNION
        {mw:Vulnerability mw:PCI_MA_hasVulnerabilitiesPolicy ?reg}}
    """"

```

```

sparql.setQuery(body)
sparql.setReturnFormat(JSON)
objlist = []
for result in sparql.query().bindings:
    if valType == "EFTA Definitions":
        listval = '{}: {}'.format(result["define"].value, result["mean"].value)
        # for values in result["define"].value:
        #     print(values.split(' '))
    elif valType == "What are EFTA Providers Obligations?":
        listval = '{} '.format(result["reg"].value)
    elif valType == "What are Error resolution policies for Providers?":
        listval = '{} '.format(result["reg"].value)
    elif valType == "What policies should providers follow for notices regarding non public
personal information?":
        listval = '{} '.format(result["reg"].value)
    elif valType == "What disclosures policies should providers adhere to?":
        listval = '{} '.format(result["reg"].value)
    elif valType == "What are consumer liabilities in case of fraud, loss of access device?":
        listval = '{} '.format(result["reg"].value)
    elif valType == "What guidelines are required for mobile payment applications?":
        listval = '{} '.format(result["reg"].value)

    objlist.append(listval.replace("'", ""))
return jsonify(objlist)

```

```

@app.route('/')
def moblie_Wallets():
    return render_template('mw.html')

if __name__ == '__main__':
    app.run(debug=True)

```

8.4 HTML & Java Script Code for Web application Development

```

<!DOCTYPE html>
<html>
  <head>
    <title>Mobile Wallets.html</title>
    <meta http-equiv="keywords" content="keyword1,keyword2,keyword3">
    <meta http-equiv="description" content="this is my page">
    <meta http-equiv="content-type" content="text/html; charset=UTF-8">
    <script type="text/javascript" src="../jquery/jquery-1.11/jquery.min.js"></script>
    <script type="text/javascript" src="../jquery/jquery-highlight/jquery-
highlight.js"></script>
    <script rel="text/javascript" type="text/javascript" href="js/jquery-
1.11.3.min.js"></script>
    <script type="text/javascript" src="http://code.jquery.com/jquery
2.1.4.min.js"></script>
    <script src="http://ajax.googleapis.com/ajax/libs/jquery/1.11.1/jquery.min.js"></script>

    <style>
      highlight { background-color: #1d5987; }
    </style>
  </head>
  <body>
    <div style="margin-left:500px;margin-top: 50px">
      Select the Regulation Query for Mobile Wallet Transaction Compliance
    </div>
    <div>
      <form class="form-inline" method="POST" action="/getres">

        <select id="selectVal" onchange="pyfunc(value);" name="selVal" style="margin-
left:500px;">
          <option value="select" selected>Select your Query</option>
          <option value="EFTA Definitions">EFTA Definitions</option>
          <option value="What are EFTA Providers Obligations?">EFTA Provider
Obligations</option>

```

```

        <option value="What are Error resolution policies for Providers?">Error
Resolution Policy</option>
        <option value="What policies should providers follow for notices regarding non
public personal information?">Non Public Information</option>
        <option value="What disclosures policies should providers adhere
to?">Disclosures Policies</option>
        <option value="What are consumer liabilities in case of fraud, loss of access
device?">Consumer Liability</option>
        <option value="What guidelines are required for mobile payment
applications?">Application Development Guidelines</option>

    </select>
</form>
</div>
<pre id="json" class="result" style="word-wrap:break-word">

</pre>
<script>
    function pyfunc(val) {
        $('#json').empty();
        cbval = $('#selectVal').val();
        var jqXHR = $.ajax({
type: "POST",
url: "/getres",
async: false,
data: cbval,
        success: function(data) {
            $('#json').html(JSON.stringify(data, null, '  \n').replace('[, ' ').replace(']', '
').replace('","').replace('\n', ' '));
        }
    });
    return jqXHR.responseText;
}
</script>

</div>
</body>
</html>

```

8.5 Mobile Wallets Ontology

https://github.com/anku2/Projects/blob/master/Mobile_Wallet_CP.owl

Chapter 9: References

- [1] A. J. LEVITIN†, "UNIVERSITY of PENNSYLVANIA LAW REVIEW".
- [2] P. M. E. Budnitz, "The Legal Framework of Mobile Payments," 2016.
- [3] C. o. F. Regulations, "Electronic Fund Transfer Act/ Regulation E," [Online]. Available: <https://www.govinfo.gov/content/pkg/CFR-2012-title12-vol2/xml/CFR-2012-title12-vol2-part205.xml>.
- [4] C. o. F. Regulations, "Truth in Lending Act/ Regulation Z," [Online]. Available: <https://www.govinfo.gov/content/pkg/CFR-2012-title12-vol8/xml/CFR-2012-title12-vol8-part1026.xml>.
- [5] P. S. S. C. Emerging Technologies, "PCI Mobile Payment Acceptance Security Guidelines," September 2017. [Online]. Available: https://www.pcisecuritystandards.org/documents/PCI_Mobile_Payment_Acceptance_Security_Guidelines_for_Developers_v2_0.pdf.
- [6] C. o. F. Regulations, "GRAMM-LEACH-BLILEY ACT," [Online]. Available: <https://www.govinfo.gov/content/pkg/CFR-2014-title17-vol2/xml/CFR-2014-title17-vol2-part160.xml>.
- [7] D. K. J. Ankur Nagar, "A Semantically Rich Knowledge Representation of PCI DSS for Cloud Services," in ICACON, 2018.
- [8] A. N. D. K. P. J. Lavanya Ellur, "An Integrated Knowledge Graph to Automate GDPR and PCI DSS Compliance," in IEEE Big Data, Seattle, 2018.
- [9] C. P. Dr Karuna Joshi, "Automating cloud service level agreements using semantic technologies," in IEEE International Conference on Cloud Engineering (IC2E). IEEE Computer Society.

- [10] S. Saha, Semantically Rich Framework to Automate Extraction and Representation of Legal Knowledge, 2018.
- [11] "ALDA," [Online]. Available: <https://ebiquity.umbc.edu/project/html/id/105/ALDA-Automated-Legal-Document-Analytics> .
- [12] "Resource description framework (rdf)." [Online]. Available: <http://www.w3.org/RDF/>.
- [13] "Owl web ontology language." [Online]. Available: <http://www.w3.org/TR/owl-features/>.
- [14] "<https://www.w3.org/TR/rdf-sparql-query/>".
- [15] L. D. B. F. M. G. a. D. M. D. Rusu, " "Triplet extraction from sentences," in in Proceedings of the 10th International Multiconference" Information Society-IS, 2007, pp. 8– 12.
- [16] M. C. D. D. A. P. T. S. S. S. D. S. W. a. A. Y. O. Etzioni, "Unsupervised namedentity extraction from the web: An experimental study, Artificial intelligence, vol. 165, no. 1, pp. 91134, 2005".
- [17] N. Z. T. D. B. A. I. A. J. C. L. M. a. J. M. N. Kiyavitskaya, " "Automating the extraction of rights and obligations for regulatory compliance," i," in n ER'08: Proceedings of the 27th International Conference on Conceptual Modeling.
- [18] M. W. V. a. A. I. A. T. D. Breaux, " "Towards regulatory compliance: Extracting rights and obligations to align requirements with regulations," ," in in RE'06: Proceedings of the 14th IEEE International Requirements Engineering Conference (RE'06), IE.
- [19] L. & F. T. Kagal, "Modeling conversation policies using permissions and obligations," Auton Agent Multi-Agent Syst (2007) 14: 187. doi:10.1007/s10458-006-0013-z".
- [20] L. K. a. T. Finin, " Agent Communication: International Workshop on Agent Communication, AC 2004, New York, NY, USA, July 19, 2004, Revised Selected and Invited

Papers. Springer Berlin Heidelberg, 2005, ch. Modeling Communicative Behavior Using Permission and Obligations".

[21] S. Congdon, "WHAT'S IN YOUR WALLET? ADDRESSING THE REGULATORY GREY AREA SURROUNDING MOBILE PAYMENTS".

[22] "<https://www.fdic.gov/regulations/examinations/supervisory/insights/siwin12/siwinter12-article1.pdf>".

[23] P. C. I. S. S. Council, https://www.pcisecuritystandards.org/document_library, April 2016.

[24] "ElementTree XML API," [Online]. Available: <https://docs.python.org/2/library/xml.etree.elementtree.html>.

[25] "TF-IDF," [Online]. Available: <https://en.wikipedia.org/wiki/Tf%E2%80%93idf>.

[26] "Modal Logic," [Online]. Available: <http://plato.stanford.edu/entries/logic-modal/>.

[27] "NLTK Documentation," [Online]. Available: <https://www.nltk.org/>.

[28] "Protege," [Online]. Available: <https://protege.stanford.edu/>.

[29] "SWRL," [Online]. Available: https://en.wikipedia.org/wiki/Semantic_Web_Rule_Language

[30] "SPARQL," [Online]. Available: <https://en.wikipedia.org/wiki/SPARQL>.

[31] M. R. Overly, "Legal compliance challenges of Big Data: Seeing the forest for the trees".

[32] Brank, J., Grobelnik, M., & Mladenic, D. (2005, October). A survey of ontology evaluation techniques. In Proceedings of the conference on data mining and data warehouses (SiKDD 2005) (pp. 166-170). Citeseer Ljubljana, Slovenia

[33] https://en.wikipedia.org/wiki/Truth_table

[34] http://flask.pocoo.org/docs/1.0/deploying/mod_wsgi/

[35] <https://pypi.org/project/SPARQLWrapper/>

