Ontological Constructs to Create Money Laundering Schemes

Murad Mehmet and Duminda Wijesekera
George Mason University Fairfax, VA 22030
mmehmet@gmu.edu, dwijesek@gmu.edu

Abstract. There is an increasing tendency in the money laundering sector to utilize electronic commerce and web services. Misuse of web services and electronic money transfers occurs at many points in complex trading schemes. We provide ontological components that can be combined to construct some of these money laundering schemes. These constructs can be helpful for investigators, in order to decompose suspected financial schemes and recognize financial misuses.

Keywords: money laundering, money laundering ontology.

1 Introduction

Money Laundering Schemes (MLS) have evolved in order to take advantage of internet based financial transactions and web services. To date, regulations alone have not been able to deter such schemes, as seen in recent examples of long running money laundering schemes [1], [2], [3], [4]. Digital currencies (E-Money) are particularly suitable for money laundering schemes because of their global usability, anonymity, ease of use, and instantaneous transferability. It is becoming increasingly difficult to differentiate between legitimate and fraudulent transactions because of their complexity and evolving nature, as described in recent publications [3], [4], [9].

In order to decompose this complexity we provide some basic ontological constructs that can be used to create known money laundering schemes. These basic ontological constructs can be integrated with financial transaction specification languages to provide further forensic analysis, particularly with XBRL, the de-facto standard for reporting in the financial industry, in order to recognize financial misuses.

The rest of the paper is organized as follows: Section 2 discusses the well known money laundering schemes. Section 3 defines the proposed money laundering ontological constructs. Section 4 presents an example of constructing a money laundering scheme using the proposed ontological constructs. Section 5 presents a discussion on related work in the area of money laundering ontologies. Finally, section 6 presents the conclusion.

2 Known Money Laundering Schemes

In order to identify the basic components of existing money laundering schemes, we list some well known money laundering schemes as follows:

1. Structured Transfer Scheme: This method involves splitting a transfer of funds into multiple fund transfers involving smaller amounts that are below the threshold of suspicion.
2. Alternative Remittance Systems Scheme: In this method, all transactions are done in cash involving parties (two or more) that calculate the difference of their balances, and make quick payments in their own countries without involving any electronic wire transfer.
3. Loan Back Scheme: In this method, a shell company (a fictitious company created merely to transfer money without raising suspicion) transfers funds allocated as credit from the money launderer in the form of a loan. The loan is then repaid with laundered money, thereby legitimizing the laundered money.
4. Low Invoicing Scheme: In this method, the seller lowers the invoice to the buyer as payment for an illegal commodity (such as drugs or weapons). The buyer then resells the product for a high profit.
5. High Invoicing Scheme: In this method, high prices for goods are paid by contractors resulting in high profits (laundered money) for the seller. It is characterized by fabricated deliveries of products, transactions carried out by shell companies in offshore territories, and use of electronic payments by anonymous persons.
6. Anonymous Account Holder Services: In this method, accounts are created by E-Money servers for customers who wish to be anonymous during the use of E-Money transactions. These are attractive to money launderers due to the ease and secrecy of fund transfers among the accounts, as well as the accessibility to fund withdrawals at any regular banking locations.

3 Components of Money Laundering Schemes

The four basic entities that we use to construct a money laundering scheme are people, organization, portfolio, and messages. The “people” represents the individuals who participate in a business transaction. This entity can be business related, non-business related, or a money launderer. The “organization” represents any institution or firm that engages in financial operation or business trading. The “portfolio” represents any asset of a person or an organization in a financial institution. “Messages” represents any form of communication exchanged between people and organizations.

We also use three auxiliary entities: communication medium, invoice and identification documents to represent schemes. The “communication medium” represents any environment that allows the delivery of messages. The “invoice”

represents the demand for payment issued in trading schemes. "Identification documents" are used to identify the "people".

There are many relationships amongst the entities. Therefore, we formally define these entities and relationships using the Web Ontology Language (OWL).

3.1 The Ontology of Money Laundering Schemes

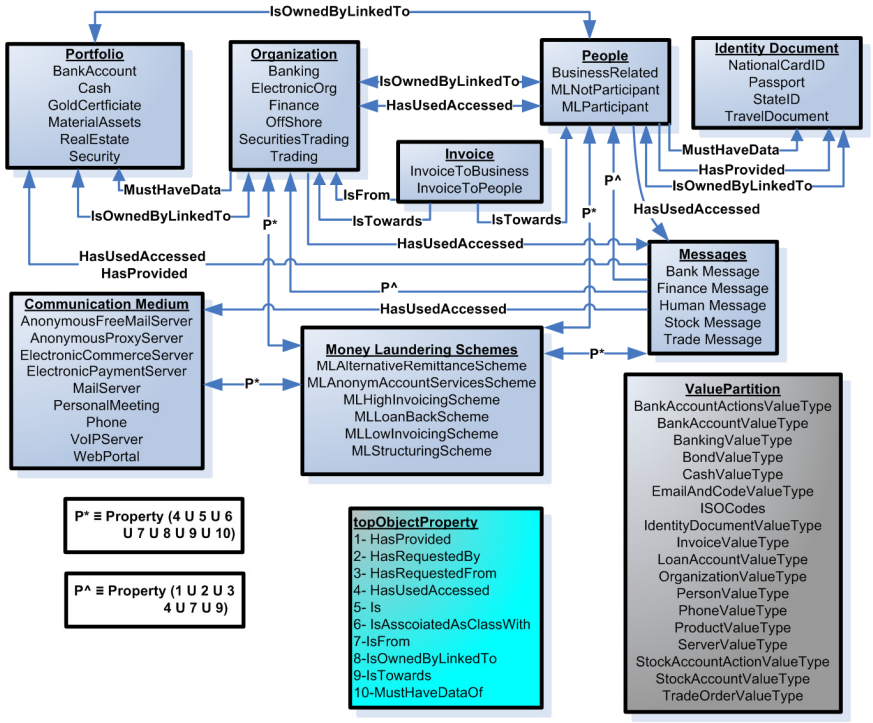

Fig. 1. The ontology class diagram

The ontology class diagram represents the components used in money laundering schemes as described in previous section: people, organization, portfolios, messages, communication medium, invoice and identification documents. We list and describe the entities in the OWL ontology shown in Figure 1 above as follows:

1. People: Represents individuals who participate in a business transaction. It consists of the subclasses "business related", "ML participant", and "ML not participant". This entity is associated with entities: "organization", "portfolio", "messages", "identification document", and "money laundering schemes". For instance, money launderer "people" need "identification documents", to send "messages" to withdraw "portfolio" cash from an "organization" bank, as part of a structuring "money laundering scheme".

2. Portfolio: Represents financial assets and products, it has many subclasses such as “cash”, “security”, and “bank account”. This entity is associated with “organization”, “people” and “messages”. For instance, “people” own accounts linked to a bank “organization”, they access them via bank transaction “messages”.
3. Organization: Represents any business engaged in trading or financial transactions, it has many subclasses such as “banking”, “securities trading”, and “electronic organization”. This entity is associated with entities: “people”, “portfolio”, “messages”, “invoice”, and “money laundering schemes”. For instance, a security trading company sends invest “messages”, or issues an “invoice” from the security account to the account owner.
4. Messages: Represents all messages exchanged in the domain between “people” and “organization”. All the activities in the domain are performed via messages, such as “bank messages”, “trade messages”, and “human messages”. This entity is associated with entities: “people”, “organization”, “portfolio”, “communication medium” and “money laundering schemes”. For instance, to withdraw funds the money launderer “people” send the withdraw “message” to the bank “organization”, and thereby the withdraw “message” accesses the “portfolio” bank account, as part of the structuring “money laundering scheme” using the phone “communication medium”.
5. Communication medium: Represents all methods of standard and encrypted communication. It has many subclasses such as “anonymous proxy server”, “electronic payment server”, and “mail server”. This entity is associated with entities “message” and “money laundering schemes”. For instance, the deposit uses the “electronic payment server” as part of the “money laundering schemes”.
6. Identification document: Represents all documents that can be provided by the person for identification purposes. It has many subclasses such as “national card ID” and “passport”. This entity is only associated with the entity “people”. For instance, money launderer “people” must have an “identification document” passport.
7. Invoices: Represents trading statements. It consists of the subclasses “invoice to business” and “invoice to people”. This entity is associated with entities “organization” and “people”. For instance, an “organization” issues an “invoice” to “people”.
8. Money laundering schemes: Represents the various money laundering techniques, it has many subclasses such as “low invoicing scheme” and “structuring scheme”. The finance industry is very dynamic, as the money laundering techniques continue to evolve they will be added to our ontology. This entity is associated with entities: “people”, “organization”, “message”, and “communication medium”. For instance, money launderer “people” send transfer “message” to bank “organization”, as part of the high invoicing “money laundering schemes”.

We list and describe the object properties in the OWL ontology as follows:

1. HasProvided: For one entity to provide information to another entity. For instance, a person provides his or her bank account number to an organization.

2. HasRequestedBy: An entity makes a request to another entity. For instance, an EFT is requested by an account holder from a bank.
3. HasRequestedFrom: An entity receives a request from another. For instance, an EFT requested from a bank by a person.
4. HasUsedAccessed: An entity uses or accesses another entity.
5. Is: To associate an entity within the MLS with their specific entity. For instance, the entity "EMSS Launderer" is a "MLSParticipant".
6. IsAssociatedAsClassWith: To associate or link an entity "Value Type" with its super class.
7. IsFrom: To associate the source entity of messages that is not in the form of a request. For instance, an electronic fund transfer is from a person.
8. IsOwnedByLinkedTo: An entity that is owned by or linked to another.
9. IsTowards: To associate the target entity of messages that is not in the form of a request. For instance, an electronic fund transfer is towards a shell company.
10. MustHaveDataOf: An entity has data of another. For instance, a bank must have data of the account holder person.

4 Example Construction of Money Laundering Scheme

In this section we create the anonymous account holder services scheme, using the constructs from our OWL ontology. According to our OWL definition, messages are linked to one or more entities. For instance, opening an account is a relation linked to the requester entity and the requested entity, the request message is sent by a person to a bank. Another example can be the relation in electronic fund transfer (EFT), where there is a receiver entity and a sender entity. Owning an account, however, is linked to only one entity.

We list the message sequence of the example scheme in Table 1.

Table 1. Choreographies of Anonymous Account Holder Services Scheme

Step	Entity	Message (Linked Entity)
1st	AnonySession	HasRequestedFrom(ProxyServer), HasRequestedBy(MLaunderer)
2nd	AnonySession	IsFrom(ProxyServer), IsTowards(MLaunderer)
3rd	EMAccount-1	HasRequestedFrom(EMoneyServer), HasRequestedBy(MLaunderer)
4th	EMAccount-1	IsFrom(EMoneyServer), IsTowards(MLaunderer)
5th	MLaunderer	HasProvided(ShellComp)
6th	ShellComp	MustHaveDataOf(EMAccount-1)
7th	MLaunderer	HasUsedAccessed (DepositCash)
8th	DepositCash	IsFrom(MLaunderer), IsTowards(ShellComp)
9th	EMAccount-2	HasRequestedFrom(EMoneyServer), HasRequestedBy(ShellComp)
10th	EMAccount-2	IsFrom(EMoneyServer), IsTowards(ShellComp)
11th	E-Deposit	HasRequestedFrom(EMExchange), HasRequestedBy(ShellComp)
12th	EMExchange	HasUsedAccessed(EMAccount-2)
13th	EFT	IsFrom(EMAccount-2), IsTowards(EMAccount-1)

14th	EFT	IsFrom(ShellComp), IsTowards(MLaunderer)
15th	Withdraw	HasRequestedFrom(EMExchange), HasRequestedBy(MLaunderer)
16th	Withdraw	HasUsedAccessed(EMoneyServer)
17th	Withdraw	IsFrom (EMAccount-1), IsTowards(MLaunderer)

We briefly describe the choreographies of Table 1 as follows:

Steps 1 and 2 are the request for an anonymous session by the money launderer and the opening of the session by the proxy server. Steps 3 and 4 are the request for an electronic currency account by the money launderer and the opening of the account by the electronic payment server. In steps 5 and 6 the money launderer passes the account information to the shell company. In steps 7 and 8 the money launderer transfers cash funds to the shell company. Steps 9 and 10 are the request for an electronic currency account by the shell company and the opening of the account by the electronic payment server. Steps 11 and 12 represent the cash deposit of the shell company to the electronic currency exchange and provision of account information. Steps 13 and 14 are the transfer of funds from the shell company to the money launderer using electronic currency accounts. Steps 15, 16, and 17 represent the withdrawal of funds from the electronic currency account of the money launderer, using the electronic currency exchange office.

Figure 2 represents the sequence diagram of the choreographies, using the relation and constructs from the OWL ontology. Figure 3 depicts the objects properties used in the ontology, linking the entities of the choreographies of anonymous account holder services scheme.

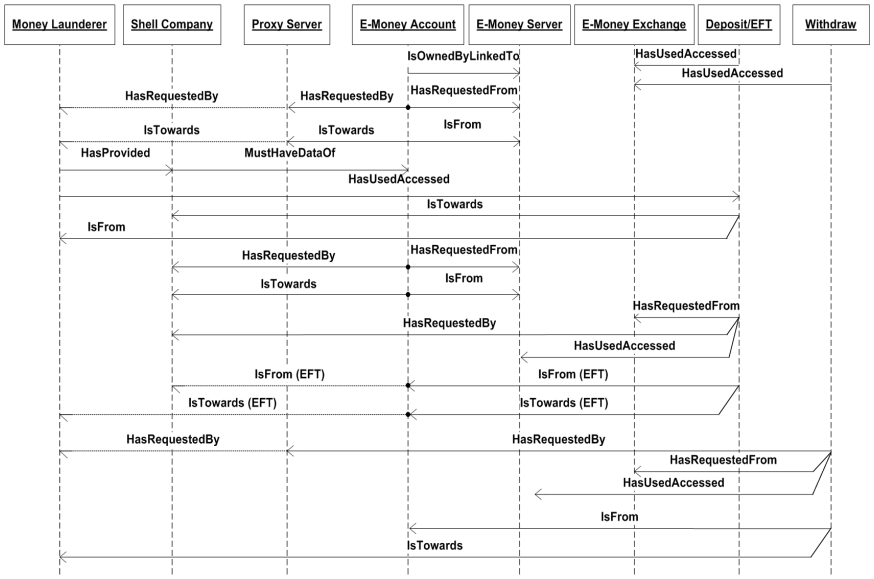

Fig. 2. The equence diagram of the anonymous account holder services scheme

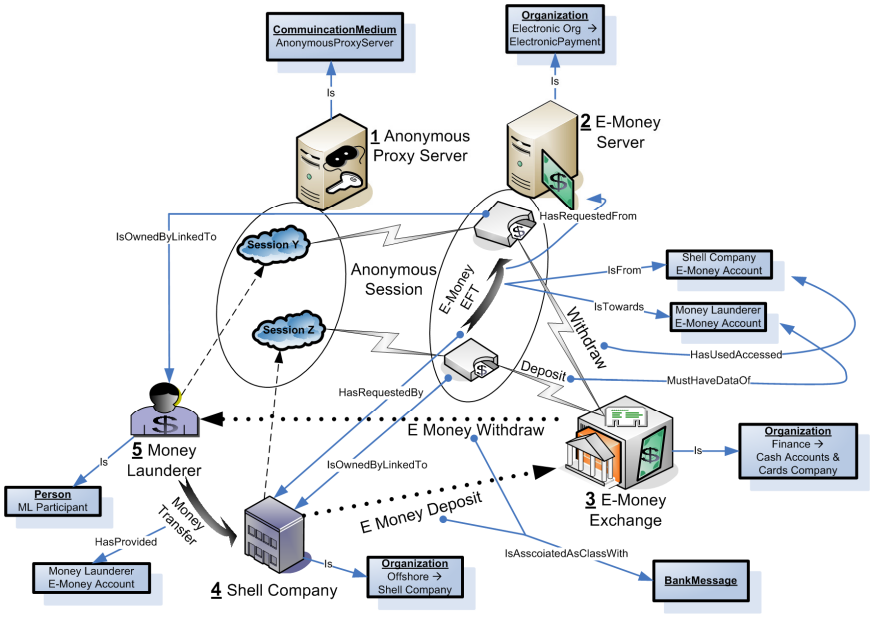

Fig. 3. The objects represented in the anonymous account holder services scheme

5 Related Work

International organizations such as The Financial Action Task Force on Money Laundering and National Drug Intelligence Center publish annual reports and statistics of money laundering trends, including ongoing investigation of cyber laundering cases [1], [2], [3], [4]. FF-POIROT [5], [6], [7], [8] is a project which builds a detailed ontology of European law on the preventive practices of financial fraud. The project is focused on sales tax fraud and online investment solicitation, and it does not go into details of money laundering ontologies and schemes. Woda [9] extensively describes money laundering techniques, but does not include any formal specification or ontology definition of the MLS. Vanderlinden [12] produced a comprehensive OWL ontology for financial systems, and covers legitimate transactions. The emphasis of the work done is to produce the OWL, and no detail is provided about the formal definition and methodological background.

Several publications study deficiencies of the languages used in the financial industry, with a particular focus on the taxonomy and the specification of the reporting languages. None of these studies cover the MLS with the exception of Viveo [20] and SEPBLAC [21].

As part of their consulting work for large global financial enterprises, Viveo released their product “QUALIFY-IT- XBRL Reporting” to provide bankers with uniform message content (e.g. Fraud detection, Risk control, Money laundering)

before anyone else can get it. The Viveo [20] product is tailored to the retail banking industry and heavily depends on XBRL [13], and thus lacks the capability to be used in web services transaction languages such as IFX [22]. The taxonomy project of SEPBLAC [21] entitled "Telematic Reporting Project" automates the reporting process of suspicious transactions, improve efficiency with fewer tasks and errors, and ensure scalability. Chen et al. [13] assess different taxonomies used for financial reporting in different countries, based on data samples selected from the Shanghai Stock Exchange. They explore if the current XBRL can apply to real life scenarios, and conclude the need to improve XBRL. Nicola et al. [14] developed an application-oriented, domain-specific benchmark "Transaction Processing over XML", which simulates multi-user financial workloads with data based on the FIXML standard. Carrillo et al. [15], [16] propose creating middleware to reduce the incompatibility from multiple implementations of XBRL in an enterprise. This is based on their developing an XBRL taxonomy for public institutions in Colombia.

Several efforts are underway in developing taxonomies for financial and investment organizations. Progress is being made on preparing taxonomy for the financial industry and investment organizations. Lara et al. [17] introduce a generic translation process of XBRL taxonomies of investment funds into OWL ontologies. They suggest that extensions to OWL are required to fulfill all the requirements of financial information reporting. An improved XBRL can be achieved by adding formal semantics. Castells et al. [18] developed an ontology-based platform that provides the integration of contents and semantics in a knowledge base that provides a conceptual view of low-level contents and semantic search facilities. Dui et al. [19] demonstrate that configuration management for XML languages is more complicated than traditional software engineering artifacts, they propose to evaluate XML by using different versions of the Financial Products Markup Language (FpML). They conclude that designers of FpML, and of many other complex XML languages, may need to make changes to the language while retaining overall compatibility. None of these works mentioned above analyze the semantics of money laundering, nor propose a model that can used to detect the schemes within the available financial reporting languages such as IFX [22], a language the financial industry heavily depends upon for web-based transaction and business-to-business banking.

We have used Methontology [10] to develop this ontology because Protégé [11] uses it.

6 Conclusions

In this paper we describe a preliminary OWL ontology to build money laundering schemes. Our ontology provides components that can be used to construct MLS. Our work creating money laundering ontologies is aimed at providing formal semantics for financial transaction data, and facilitating detection of illegal financial schemes. Currently, we are working on developing algorithms to detect each of the schemes from a sequence of financial transaction records, where the objective is to capture and identify the transactions that match constructs from our OWL ontology.

References

1. The Financial Action Task Force on Money Laundering: Annual Review of Non-Cooperative Countries or Territories. http://www.fatfgafi.org/dataoecd/3/52/33922473.pdf (2004)
2. The Financial Action Task Force on Money Laundering: Financial Action Task Force Annual Report 2008-2009. http://www.fatf-gafi.org/dataoecd/11/58/43384540.pdf (2009)
3. The Financial Action Task Force on Money Laundering: Money Laundering & Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems. http://www.fatf-gafi.org/dataoecd/57/21/40997818.pdf (2008)
4. National Drug Intelligence Center: Money Laundering in Digital Currencies. http://www.justice.gov/ndic/pubs28/28675/index.htm (2008)
5. Zhao G., Kingston J., Kerremans K., Coppens F., Verlinden R.: Engineering an Ontology of Financial Securities Fraud. In: Workshop of Regulatory Ontology (2004)
6. Kerremans K., Tang Y., Temmerman R., Zhao G.: Towards Ontology-based E-mail Fraud Detection. In: 12th Portuguese Conference on Artificial Intelligence (2005)
7. Project Financial Fraud Prevention Oriented Information Resources Using Ontology Technology, http://www.ffpoirot.org (2010)
8. Leary R.M., Vandenberghe W., Zeleznikow J.: Towards a Financial Fraud Ontology: A Legal Modelling Approach. In : Workshop on Legal Ontologies, ICAIL (2003)
9. Woda, K.: Money Laundering Techniques with Electronic Payment Systems. In: Information & Security International Journal, vol .18, pp. 27--47 (2006)
10. Lopez M.F., Perez, A.G. : METHONTOLOGY: From Ontological Art Towards Ontological Engineering. In: Symposium on Ontological Engineering of AAAI, pp. 33--40 (1997)
11. Horridge M., Jupp, S., Moulton G.: A Practical Guide To Building OWL Ontologies Using Protégé 4 and CO-ODE Tools. http://owl.cs.manchester.ac.uk/tutorials/protegeowltutorial (2009)
12. Vanderlinden, E.: Finance Ontology and Semantic Technologies. http://www.fadyart.com/financeV4.owl (2010)
13. Chen, H.: Application and Neediness of Extensible Business Reporting Language. In: International Forum on Information Technology and Applications (2009)
14. Nicola, M. Kogan, I.: An XML transaction processing benchmark. In: 2007 ACM SIGMOD International Conference on Management of Data (2007)
15. Carrillo, E., Chaparro F., Santoyo, J.: XBRL and Financial Information Standards: a Case Success: University – Enterprise. In: Euro American Conference on Telematics and Information Systems (2008)
16. Carrillo E.: XBRL: From Common Financial Vocabularies to Intelligent Decision Making. In: Euro-American Conference on Telematics and Information Systems (2007)
17. Lara R., Cantador I., Castells P.: XBRL Taxonomies and OWL Ontologies for Investment Funds. In: 1st International Workshop on Ontologizing Industrial Standards (2006)
18. Castells, P., Foncillas B., Lara R., Rico M., Alonso, J.L. :Semantic Web Technologies for Economic and Financial Information Management. In: ESWS, pp. 473--487 (2004)
19. Dui D., Emmerich W.: Compatibility of XML Language Versions. In: Lecture Notes in Computer Science, pp. 148--162 (2003)
20. Viveo Systems: QUALIFY-IT- XBRL Reporting. In: XBRL-CEBS Workshop (2005)
21. SEPBLAC: Anti-Money-Laundering XBRL Taxonomy Project. In: 11th XBRL Conf (2005)
22. IFX Forum: Interactive Financial Exchange Message Specification 1.7.0. http://www.ifxforum.org/standards/standard (2005)