

A Work Project, presented as part of the requirements for the Award of a Master Degree in Management from the NOVA – School of Business and Economics.

Online payments strategy: How third-party internet seals of approval and payment provider reputation influence the millennial consumers' online transactions

SOFIA ANASTÁCIO CARDOSO, 2583

A Project carried out on the Master in Management Program, under the supervision of: Professor Luis F. Martinez

6<sup>th</sup> of January, 2017

## Contents

Acknowledgments .....	1
Abstract.....	2
1 Introduction.....	2
1.1 Literature Review: The perception of trust and perceived risk on online transactions.....	6
2. Method.....	13
2.1 Sample.....	13
2.2. Experimental Setup: scenario method and manipulations .....	14
2.3 Measurement Development .....	16
3. Results .....	17
3.1 Measurement factor structure and reliability .....	17
3.2 Hypotheses testing.....	18
4. Discussion .....	21
5. Conclusion.....	23
References .....	24
Appendices .....	27

## Acknowledgments

I would first like express my gratitude for my thesis advisor Prof. Luis F. Martinez, at Nova School of Business and Education, for the continuous support, guidance and motivation.

I would also like to show my deepest gratitude to Teresa Marques who has dedicated her time to share her scientific knowledge and wisdom, and to support me in throughout this process. Furthermore, I would like to thank the “anonymous” reviewers for their insights.

Finally, I also place on record, my sense of gratitude to my parents for the encouragement, support and attention.

## **Abstract**

With the recent increase in online purchases, organizations have been able to improve their capacity to collect, store and profit from personal and financial data gathering. Online purchases occur in an environment characterized by higher risk levels surrounding the transaction. Several payment strategies can be applied in order to mitigate the consumers' perceived risk and increase trust levels. The present study intends to understand how the presence of internet seals of approval, and the reputation of the payment provider impacts consumer trust and online payment perceived risk. The study uses four randomized experimental setups to manipulate the independent variables, on a sample size of 324 valid responses, the majority of responses are from people between the ages of 18 and 25 years old. The study results demonstrate that new online vendors can mitigate these variables by investing in a payment strategy that combines the presence of internet seals of approval logos together with the presence of payment providers with low reputation.

Key words: Consumer Behavior; Online Transactions; Payments Strategy; Reputation; Digital Marketing; Millennial Consumer.

## **1 Introduction**

The continuous growth of online transactions, via credit card and other emerging non-bank payment methods (Lees & King, 2015), is consequently leading consumer concerns for personal and financial data privacy to emerge. All around the world, actions have arisen to protect consumers' privacy, and Key Regulatory and Industry Initiatives (KRII) have been created for this purpose. Some examples of these initiatives are the Electronic Identification and Trusted Service (eIDAS) by the European Commission, or the Personal Data Notification & Protection Law Act in the United States (Lees & King, 2015). These actions intend to

reduce consumers' perception of risk and increase trustworthiness of the consumer in the online vendor, aspects which will determine the final purchase decision. The consumers' trustworthiness level act as a significant aspect to build business to consumer relationships (Bilgihan, 2016), therefore, the reduction of consumer uncertainty is a crucial component for e-commerce acceptance (Pavlou, 2003). The way to achieve this acceptance is by manipulating favorable consumer attitudes and influencing transaction intention, thus trust-building mechanisms must be employed (Pavlou, 2003). Additionally, online vendors must make an effort to successfully manage key elements of the online business-to-consumer environment, namely information content, design, security and privacy policies (Vos et al., 2014).

Today's technology has increased the capacity to collect, store, analyze and profit from vast amounts of data gathering which raises consumer and governmental concerns about online privacy (Miyazaki & Krishnamurthy, 2002). A solution found to ease concerns regarding quality and security of certain products and services was the use of seals and certifications by third-party agencies designed to provide assurance of quality to the consumer (Gordon & Lee, 1967). These third-party agencies grant their seals of approval to the products, or services, which meet previously determined standards of quality, security and privacy, and firms gain the right to use these symbols on their products and services (Parkinson, 1975). Through his study, Parkinson (1975), was able to demonstrate that, at the retail level, seals and certifications influence the consumer purchase decision significantly. In consequence, several private sector organizations developed self-regulatory actions in the form of internet privacy seals of approval programs, to raise consumer confidence on a particular website (Miyazaki & Krishnamurthy, 2002).

One survey was conducted to understand the impact of the self-regulatory actions mentioned above. This survey was performed by the Baymard Institute (Holst, 2013) and raised the question: “*which site seals are actually the most trusted by users?*”. The survey was conducted with a sample size of 2510 responses, and tested the up-to-date versions of the following site seals, divided into two categories: (1) SSL seals, namely, Norton Secured, Secured by Thawte, Trustwave, Geotrust, Comodo; and (2) TLS or trust seals, namely, BBB Accredited Business, TRUSTe, McAfee Secure. This survey was conducted with a consumer behavior focus in order to comprehend how these internet seals made the consumer feel in terms of perceived security, rather than from a technical perspective to measure the strictest technical and security compliance guidelines. From the first question “*Which badge gives you the best sense of trust when paying online?*”, the survey got the following responses: Norton Secure (35.6%), McAfee Secure (22.9%), TRUSTe (13.2%), BBB Accredited Business (13.2%), Secured by Thawte (6%), Trustwave (3.2%), Geotrust (3.1%), COMODO (2.8%). Holst (2013) demonstrates how it is not the actual security of the online vendor that users give importance to, since users have little to no understanding of the difference between TLS/ SSL encryption<sup>1</sup>, but the perceived security of the internet seals. Through this survey it is also noticeable how the two most trusted site seals are the ones associated with well-known antivirus software brands, which leads to an immediate association with security (Holst, 2013).

Inevitably, whenever an online vendor wants to use his own website to sell products and services, it will be necessary to implement the necessary technology and agreements to

---

<sup>1</sup> Secure Site Seal, or SSL seal certification, certifies the actual technical security of the payment form, whereas the Trust seal or TLS certification, don't always certify any technical security and rather certify the consumer relations of the company.

process payments. There are several ways to perform this implementation, and one way to process payments is through a direct connection with a local credit card acquiring Bank. This acquiring Bank or Financial Institution will process and approve or reject the credit card transaction, by verifying the credit card data and financial availability with the Issuing bank<sup>2</sup> (Rajappa et al., 2012). When the online vendor has a direct connection with the acquiring Bank, we can state that there is a dyadic relationship between online vendor and consumer (Jarvenpaa, Tractinsky, & Vitale, 2000; Köster, Matt, & Hess, 2016), since the online vendor is the one obtaining the financial and personal data from the consumer, and redirecting it to the acquiring Bank. Since this direct connection requires more technical expertise and effort from the online vendor side (Preibusch, Peetz, Acar, & Berendt, 2016), smaller online vendors with fewer resources often engage with third-party payment providers (Preibusch et al., 2016). These payment providers work as intermediaries between online vendors and consumers, to collect the consumer data, process and approve the transaction (Preibusch et al., 2016), and are usually Non-Banking payment systems (Non-Banks PSPs) which have made inroads into the immediate payments space (Lees & King, 2015). By engaging with payment providers, a triadic relationship emerges (Köster et al., 2016; Preibusch et al., 2016) in which this study will be based upon.

To accomplish the research purpose, the following research question was established: Does the presence of one or more logos of internet seals of approval, and the presence of a reputable payment provider influence the level of consumers' trust and online payment perceived risk over the transaction?

---

<sup>2</sup> The Issuing Bank is the Bank or Financial Institution which grants Credit or Debit cards to the consumer (Rajappa et al., 2012)

The remainder of this paper is structured as follows: the first section is the literature review, presenting the theoretical background on consumer trust perception and perceived risk on online transactions. Throughout this section the developed hypotheses will be presented and explained. On the second section, the method will be described, followed by the third section with the study results and the fourth section with the study discussion. In the final section the conclusions will be presented, together with the practical implications, the limitations of the research, and directions for future research.

### ***1.1 Literature Review: The perception of trust and perceived risk on online transactions***

#### *1.1.1 Consumers trust in the online purchase*

According to Chang, Cheung, and Tang (2013) trust acts as a psychological state which allows a person to accept vulnerability based upon positive expectations of the intentions or behavior of others. The definition by Schoorman, Mayer, and Davis (2007) can also be taken into consideration, where trust is defined by the willingness of a party to be vulnerable to the actions of the other party, resting on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control. Thus, trust is the willingness to take risk (Schoorman et al., 2007).

In the e-commerce environment it is necessary to consider that the act of purchasing a product or service online happens in a unique environment, where trust is of the utmost importance, mainly due to the lack of physical presence of the product and the physical distance between buyers and sellers (Chang et al., 2013). Nonetheless, in the context of e-commerce, trust is founded by the relationship exchange given the impersonal nature of the internet infrastructure (Hong & Cha, 2013), and therefore, the consumer trusts that the online vendor will behave in a favorable manner (McKnight, Kacmar, & Choudhury, 2004). Trust

works as a successful mechanism to reduce uncertainty and risks, by creating a sense of safety and playing an important role in consumers' shopping behaviors in e-commerce (Pavlou, 2003).

Throughout their studies, Chang et al. (2013) found that third-party certification and reputation significantly increases consumer trust in the online vendor, and proposes that new online vendors must create opportunities to demonstrate their trustworthiness. Online vendors must, therefore, engage in trust enhancing strategies, mainly since risk cannot be totally eliminated in the online shopping environment (Chang et al., 2013).

One possible strategy, which can be applied by new online vendors in order to enhance consumers' trust, is engaging in third-party certification seals of approval. A key feature of this type of certification is the commitment, from the online vendors' behalf, to abide by the defined standards of these certification entities. Comprehensively, by paying a registration fee, online vendors are authorized to place the logos on their website, and these organizations assure that the online vendors have been audited for their privacy practices (Miyazaki & Krishnamurthy, 2002). Internet seals of approval such as TRUSTe and BBBOnline claim that the consumer will feel an added confidence when seeing the seal of approval logo on the licensee's website (Miyazaki & Krishnamurthy, 2002). Given the previous statements, this study intends to better understand whether the presence of internet seals of approval logos on the checkout page has an impact on the enhancement of consumers perceived trust. Consequently, the following hypothesis was postulated:

**Hypothesis 1a:** The presence of one or more logos of internet seals of approval on the checkout page, leads consumers to perceive higher trust levels on the transaction moment.



Overall, there are other aspects which can be used in the e-commerce environment as trust enhancers. Preibusch et al. (2016) state how intermediation can be used to overcome the shortfall of consumer trust, and how the use of a payment provider, namely highly reputable, can mitigate the consumers' trust deficit. In addition, the payment provider can work as a trust booster if it reflects more trust than the online vendor itself, since the intermediary is able to overcome security and privacy concerns (Preibusch et al., 2016).

Hence, another possible strategy which new online vendors may engage in to increase consumers' trust, is for the online vendor to engage with a highly reputable payment provider as a third-party intermediary for payment processing. Therefore, this study intends to better understand the impact of the presence of a reputable payment provider as an enhancer of the consumers' perceived trust over the transaction, and the following hypothesis was postulated:

**Hypothesis 1b:** The presence of a high reputation payment provider will lead consumers to perceive higher trust levels on the transaction moment.

#### *1.1.2 Online Payment Perceived Risk*

Through their studies, Hong and Cha (2013) distinguish several types of perceived risk, and the most appropriate type of perceived risk for the purpose of this study is the online payment risk, which is defined as “the likelihood that a consumers' private information, including personal and credit card information, may be exposed to potential threats and that such private information may be misused” (Hong & Cha, 2013, p. 929). Moreover, the consumer trusts and acts upon the belief that the e-commerce environment is secure to provide risk-free transactions (Hong & Cha, 2013).

Certain factors can act as “risk relievers” and boost customer's confidence, namely security, privacy, brand name, word-of-mouth, good online experience, and quality of

information (Ha, 2004). Pavlou (2003) distinguishes two sources of uncertainty when it comes to online transactions: the first one, behavioral uncertainty, is mainly based on the possibility of the online vendor (or the payment provider) acting opportunistically upon the consumer, and arises from four major risks: (1) economic risk, due to the possible financial and monetary loss; (2) personal risk, due to the uncertainty related with the purchase of the specific product or service; (3) seller performance risk, due to imperfect monitoring; and finally, (4) privacy risk, related to the risk of private information of the consumer being disclosed. The second source is environmental uncertainty, and it is due to the unpredictability related with the nature of the technology, which can be controlled in part by the online vendor by using encryption, authentication, firewalls and other technologies to protect the consumer and itself. However, there is still a part that cannot be controlled, namely the risk of theft of credit card information and personal information by hackers<sup>3</sup>.

Therefore, it is necessary to take into consideration that online consumers experience a higher risk perception comparing to those shopping in physical stores (Z. Hong & Yi, 2012) namely because, (1) the consumer is not able to examine the product before receiving it; (2) there is a concern regarding after-sales service; (3) consumers may not fully understand the language used in e-sales (Hong & Yi, 2012); and, (4) the fact that transactions are remote and do not involve face-to-face contact between the vendor and consumer (Cases, 2002). Thus, a consumer perceiving very high risk regarding an online transaction is more likely to foresee a great loss potential (Hong & Cha, 2013).

Additionally, it is relevant to bear in mind that consumers will also perceive risk given the fact that the most used payment method for online purchases, considering the reality in

---

<sup>3</sup> *Hacker* is defined as someone who is able to subvert computer security to gain unauthorized access to data, and if doing so for malicious purposes source (Wikipedia, n.d.)

Europe and USA, is still credit card in spite of the new, upcoming, alternative payment methods, such as digital wallets and prepaid cards (Adyen, 2015). Taking the information provided by Adyen (2015), Visa and MasterCard still represent the highest percentage for online purchases in major European countries such as France and UK (80% and 87% respectively). The United States of America is also dominated by credit card payments for online purchases, with the leaders Visa, Mastercard and American Express representing a total of 93% of the total online payment methods.

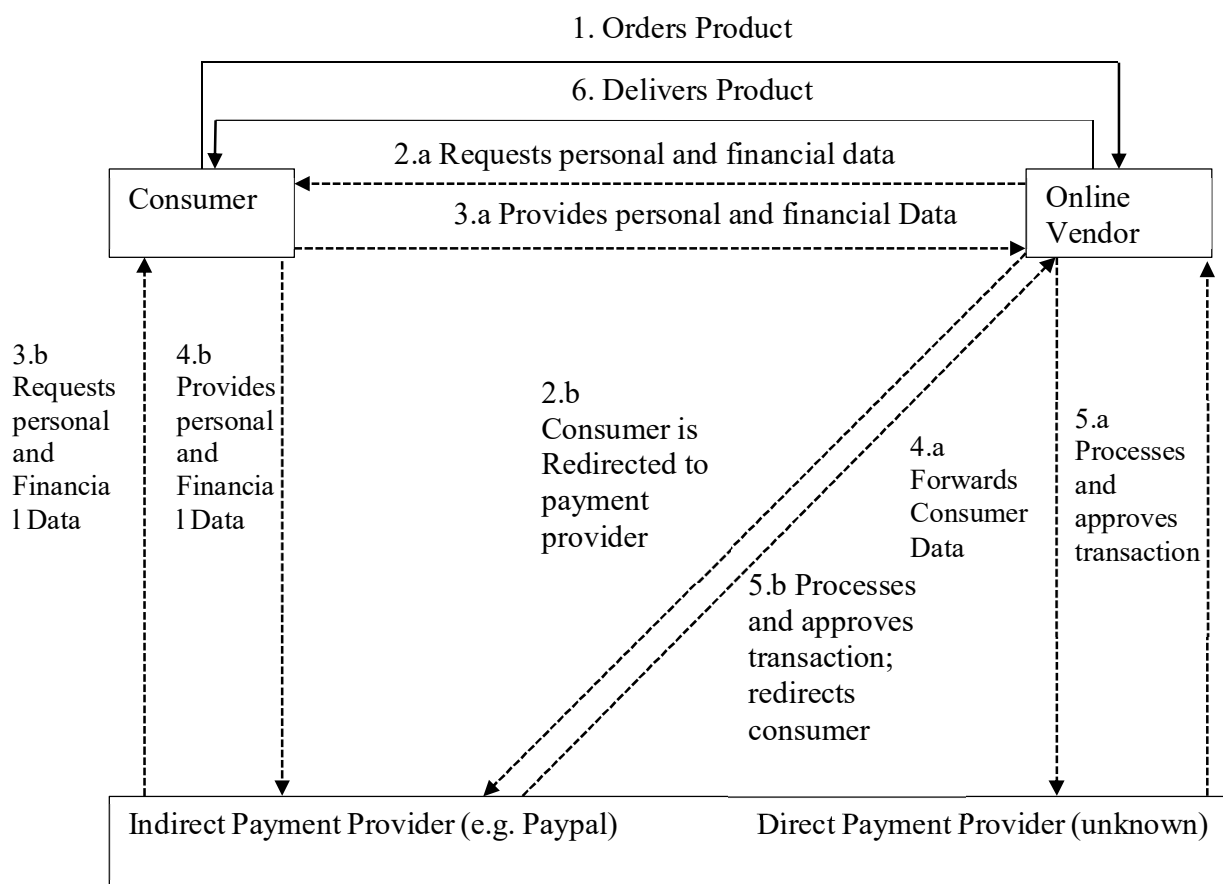
Consequently, consumers may perceive higher risk levels when performing the payment since, for this payment method, it is necessary to provide important personal and financial information to the online vendor (Hong & Cha, 2013) and to the third-party payment provider (Köster et al., 2016). Köster et al. (2016) explain how, in order to complete a transaction, consumers need to rely on two different parties: the online vendor and the payment provider, and therefore, proposes a triadic relationship to the transaction process. On the contrary to previous research, which focuses on trust as a dyadic relationship (Jarvenpaa, Tractinsky & Vitale, 2000), the focus on trust as a triadic relationship notes how consumers are purchasing the products or services from the online vendor and providing their information to both the online vendor and the payment provider (Köster et al., 2016). Therefore, the payment provider also acts as an influencer to consumer perceptions and purchase behavior. As proposed by Köster et al. (2016), the present paper proposes an adapted view of the triadic relationship between consumer, online vendor and payment provider, as presented in Figure 1.

In this adaptation of the triadic relationship, the payment provider is divided into two subsections, the first representing the direct integration, between online vendor and third-party payment provider. In this direct integration the consumer provides its personal and

financial information to the online vendor, which will then forward the data to the back-end payment provider, which is unknown to the consumer. The payment provider will process and approve the transaction, and immediately notify the online vendor. The second subsection represents an indirect integration with the payment provider, in which the consumer is redirected to the respective payment provider web page, and will provide the personal and financial data directly to the payment provider, e.g. Paypal.

When engaging with an indirect payment provider, the online vendor is offering the consumer the possibility of providing the data to only one party, with whom the consumer has already developed familiarity and consumers' trust.

Figure 1: Triadic Relationship between Consumer, Online Vendor and Payment Provider, adapted by Köster et al. 2016.



Furthermore, and notwithstanding of security measures, namely encryption and authentication, the insecurity regarding the leakage of information during the online transaction (Hong & Cha, 2013), and of privacy loss (Köster et al., 2016), reflect the consumer's fear that the transaction partner will act opportunistically (Köster et al., 2016). One possible strategy which can work as an attempt for online vendors to decrease consumers' perceived risk is the use of logos of seals of approval from trusted third parties, which assures consumers that a certain standard of privacy will be upheld (Palmer, Bailey, & Faraj, 2006). This strategy can be successful since, according to Vos et al. (2014), a crucial issue to verify the credibility of the e-commerce platform is the display of policies, namely privacy, refunds and shipping policies, and also the logos of payment methods and communication facilities.

Based on the above evidence, the presence of a logo of the internet seal of approval is expected to reflect a lower perceived risk, at the purchase moment, and therefore the following hypothesis was postulated:

**Hypothesis 2a:** The presence of one or more logos of internet seals of approval leads consumers to perceive less online payment risk over the transaction.

Moreover, it is relevant to mention that less reputable online vendors have more difficulty persuading consumers to perform the online transaction and, on the other hand, highly reputable online vendors do not gain additional trust-building factors when engaging with reputable payment providers (Köster et al., 2016). In reality, Köster et al. (2016) was able to demonstrate that consumers perceive less risk and a higher purchase intention, when there is the combination of the presence of a reputable payment provider on a less reputable online vendor. The author concludes that the actual choice of a good and reputable payment

provider works as an efficient trust-building mechanism. In addition, Köster et al. (2016) state how the consumers' skepticism in the transaction is significantly reduced when online vendors engage with highly reputable payment providers.

Given all of the above, the present study intends to understand whether the presence of a reputable payment provider, versus the presence of an unknown payment provider, is able to mitigate the perceived online payment risk over the transaction, and therefore the following hypothesis was postulated:

**Hypothesis 2b:** The presence of a high reputation payment provider leads consumers to perceive less online payment risk over the transaction.

## 2. Method

### 2.1 Sample

In total, 331 responses were collected throughout the study, and after excluding incomplete responses, 324 were considered valid. From this sample 67.9% of the respondents are from the Female gender, and 60.8% are between 18 and 25 years old, demonstrating a majority of young respondents belonging to the millennial generation. The frequency distributions of the demographic constructs can be found on Table 1.

Table 1: Demographic Data

<i>Age</i>	<i>Freq.</i>	<i>%</i>	<i>Gender</i>	<i>Freq.</i>	<i>%</i>	<i>Academic Degree</i>	<i>Freq.</i>	<i>%</i>
18-25	197	60.8%	Male	104	32.1%	High School	34	10%
25-30	84	25.9%	Female	220	67.9%	Graduate Bachelor Degree	109	34%
30-35	19	5.9%				Master's Degree	166	51%
35+	24	7.4%				PhD	10	3%
						Other	5	2%

Additionally, 65% of the respondents have used the internet for online shopping of products and services once a month, over the last 6 months; and 54% of all respondents have used a credit card as a payment method when shopping online, also once a month, over the last 6 months. Another item of this study analyzed the past experience of respondents regarding online shopping, in which 67% either agree or strongly agree that their past experience purchasing online was positive, and 55.3% also either agree or strongly agree that their past experience purchasing a product or service online using a credit card was positive.

## ***2.2. Experimental Setup: scenario method and manipulations***

A survey questionnaire was developed to measure the research constructs with four experimental conditions, in order to provide the empirical data to test the hypothesis. The survey was distributed through social network sites, such as Facebook and LinkedIn, and through email. Furthermore, the participation on the questionnaire was anonymous and voluntary. The questionnaire consisted of five sections: after a brief introduction, on the first section, the respondents would have to answer three demographic related questions, two questions related to the past experience in online shopping, and two questions which evaluated the general online payment risk perception before the scenarios manipulation. On the second section, the respondents were presented with one of the four randomized scenarios to be analyzed carefully (see Appendix A for experimental Setup Flowchart). After the scenario was presented, the respondents were asked scenario specific questions regarding trust and the perceived risk of the online payment, and finally, two questions regarding the intended purchase of the product.

The scenarios asked the respondents to imagine that they were book lovers, with a special preference for the electronic format (see Appendix B for scenario introduction). The

first part of the experimental setup illustrated the first step of a regular online shopping cart, presenting the purchase details, namely the name and details of the product, an image of the product, and the final price. The second part presented one of the four scenarios (see Appendix C for the scenarios demonstration). For the development of the scenarios, the product chosen was a digital good in order to remove the physical aspect of the purchase, removing the risk perception regarding delivery and return policy (Cases, 2002; Chang et al., 2013; Hong & Yi, 2012). The choice for an ebook, which would be available for download immediately after the transaction is approved, is based on the fact that it is a pure digital product with a concept which is familiar to most millennials (Nicholas & Lewis, 2008). The other key characteristic of an ebook is the fact that it is a low-involvement, low risk product, meant for leisure purposes.

The user interface used for the experimental setup portrayed an unknown online ebook store to illustrate the necessary mechanisms to mitigate the risk perception over a new and less reputable online vendor. Given this, the chosen good reputation, non-banking online payment provider was Paypal<sup>4</sup>, which still represents one of the most popular alternatives to direct credit card processing, together with Amazon payments and Google wallet (Claire Greene, Schuh, & Stavins, 2013), and is considered the most pervasive online payment provider (Preibusch et al., 2016). Furthermore, the good reputation internet seal of approval logos were chosen based on the study performed by the Baymard Institute (Holst, 2013), presented in the Introduction section of this paper. The logos presented in the scenarios were a combination of SSL and TLS logos, namely Norton Secure, TrustE and Secure by Thawte.

---

<sup>4</sup> Paypal provides funds transfers and acts as an e-wallet solution for consumers, with a global offer (Lees & King, 2015)



### 2.3 Measurement Development

The instrument of the questionnaire was developed based on validated constructs which were adapted for the purposes of this study and to the specific scenarios, and can be found on Table 2. A 7-point Likert scale was used, from strongly disagree (1) to strongly agree (7), with a neutral response of neither agree or disagree (4).

Table 2: Measurement and sources

<i>Constructs</i>	<i>Adapted Items</i>	<i>Sources</i>
Internet usage and online shopping habits	I have used the internet for online shopping of products and services in the last 6 months	Benlian et al (2012)
	I have used the internet for online shopping of products and services in the last 6 months, using a Credit card as a payment method	
Positive Past experience	My past experience purchasing online was positive	P.Pavlou, D.Gefen (2004)
	My past experience purchasing products or services using a credit card was positive	
Trust in the Online vendor	I can count on this online Ebook store (Ebooks.pt) to be trustworthy	Butler Jr (1991)
	I feel that this online Ebook store (Ebooks.pt) can be trusted	
	I trust Ebooks.pt to keep my best interests in mind	
	I find it necessary to be cautious with Ebooks.pt	
Online payment Perceived Risk	Ebooks.pt is an online vendor who has more to lose than to gain by not delivering their promises	Jarvenpaa, Tractinsky & Vitale (2000), Doney & Cannon (1997)
	Ebooks.pt behavior meets my expectations	
	The Ebooks.pt online vendor wants to be known as one who keeps promises and commitments	
Online payment Perceived Risk	Purchasing online involves the risk of private information loss when compared with more traditional ways of shopping	Hong and Yi (2012), Pappas (2016)
	Purchasing online involves the risk of fraudulent and opportunistic behavior	
	I would be concerned as to whether Ebooks.pt is equipped with a security monitoring and data protections tools	
Online payment Perceived Risk	I would be concerned as to whether Ebooks.pt properly manages customers' private information	Featherman & Pavlou (2003), I. B. Hong & Cha (2013)

Intended Transaction	I would use my credit card to purchase from this online vendor I am very likely to provide the online vendor with the information it needs to better serve my needs	Gefen et al (2003)
----------------------	--	--------------------

The research method was tested using a 2 x 2 between-subjects design experimental setup. Four different scenarios were developed to manipulate the presence of the internet seal of approval logos (present vs absent), and the level of the payment provider reputation (high vs low). This research method allowed the examination of the main effects of the presence of high reputation logos of internet seals of approval, together with the reputation of the payment provider and their influences on the dependent variables. Table 3 demonstrates the experimental setup design and sample sizes in each experimental group.

Table 3: Experimental Setup

<i>Internet Seals of Approval Logos</i>	<i>Payment Provider</i>	
	Low reputation (L)	High Reputation (H)
Presence (P)	L x P (n = 81)	H x P (n = 81)
Absence (A)	L x A (n = 80)	H x A (n = 82)

### 3. Results

#### 3.1 Measurement factor structure and reliability

The measurement model was tested using exploratory factor analysis. Principal components analysis indicated a three factor solution that accounted for 59.9% of the variance. After a varimax rotation, items loading together indicated factors representing trust in the online vendor, online payment perceived risk and intended transaction. All the items loaded clearly on their designated factor with factor loadings greater than .40 (see Table 4).

Cronbach's alpha was used to evaluate the reliability of the constructs, and demonstrated that all values for Cronbach's alpha were higher than .70, together with the

analysis of the average variance extracted (AVE) and composite reliability (CR), also demonstrated in Table 4.

Table 4: Operationalization of constructs and measurement characteristics.

<i>Constructs</i>	<i>Adapted Items</i>	<i>Loadings</i>	<i>Measures</i>
Trust in the online vendor	T1 I can count on this online Ebook store (Ebooks.pt) to be trustworthy	.765	<b>CA = .765</b> <b>AVE = .432</b> <b>CR = .837</b>
	T2 I feel that this online Ebook store (Ebooks.pt) can be trusted	.758	
	T3 I trust Ebooks.pt to keep my best interests in mind	.724	
	T4 I find it necessary to be cautious with Ebooks.pt	.702	
	T5 Ebooks.pt is an online vendor who has more to lose than to gain by not delivering their promises	.635	
	T6 Ebooks.pt behavior meets my expectations	.514	
	T7 The Ebooks.pt online vendor wants to be known as one who keeps promises and commitments	.421	
Online payment perceived risk	R3 I would be concerned as to whether Ebooks.pt is equipped with a security monitoring and data protections tools	.962	<b>CA = .928</b> <b>AVE = .924</b> <b>CR = .961</b>
	R4 I would be concerned as to whether Ebooks.pt properly manages customers' private information	.961	
Intended transaction	IT1 I would use my credit card to purchase from this online vendor	.902	<b>CA = .783</b> <b>AVE = .790</b> <b>CR = .883</b>
	T2 I am very likely to provide the online vendor with the information it needs to better serve my needs	.876	

### ***3.2 Hypotheses testing***

As a starting point for the hypothesis testing, the means and standard deviation for each of the dependent variables were estimated, namely for the dependent variables trust and online payment perceived risk, for the four different scenarios of high and low reputation payment provider and the presence or absence of the internet seal of approval logo. This estimation is demonstrated in Table 5.

Table 5: Means and Standard Deviation of dependent variables

<i>Reputation of the Payment Provider</i>		Low (L)		High (H)	
		Presence (P)	Absence (A)	Presence (P)	Absence (A)
<i>Internet Seal of Approval Logo</i>					
Trust	Mean	36.83	37.22	37.33	38.21
	SD	(8.38)	(6.76)	(8.67)	(8.33)
Perceived Risk	Mean	9.86	11.14	11.05	11.23
	SD	(3.05)	(1.93)	(2.18)	(2.32)

The next step of this analysis involved performing a one-way MANOVA. The multivariate analysis of variance is used when there is the presence of more than one independent variable (Field, 2009). Through this analysis it is possible to evaluate the interaction between the independent variables and the contrasts of the different groups, how these differ from each other, while looking simultaneously at the dependent variables (Field, 2009). There are several assumptions underlying this analysis, specifically random sampling, homogeneity of covariance of matrices, and multivariate normality (Field, 2009). The underlying assumption that the data is normally distributed has been presumed following the central limit theorem, in which the sampling distribution of the sample mean is considered approximated by a normal distribution as the sample size becomes larger (Anderson, Sweeney, & Williams, 2011). Therefore, given that the sample size is larger than 30, a normal distribution was assumed.

A MANOVA was conducted in order to understand the significance of the multivariate effect for the different experimental setups. This MANOVA analysis was able to demonstrate significance, Wilks lambda  $k = .945$ ,  $F(8,636) = 2.290$ ,  $p = .020$ , partial  $\eta^2 = .028$ , and the univariate main effects were further examined.

Non-significant univariate main effects for the different groups were obtained for trust in the transaction moment,  $F(4, 319) = .317$ ,  $p = .866$ , partial  $\eta^2 = .004$ , leading to

hypothesis 1a and 1b to not be supported and therefore discarded. Significant univariate main effects for the different groups were obtained for online payment perceived risk,  $F(4, 319) = 4.33$ ,  $p = .002$ , partial  $\eta^2 = .052$ . Significant pairwise differences were obtained for this variable on the four experimental setups with post hoc tests. The differences in means for the dependent variables and significances obtained from the least significant difference (LSD) pairwise comparison procedure (see Table 6).

Table 6: Pairwise comparisons for the online payment perceived risk variable

<i>Mean differences (I-J)</i>		<i>Perceived Risk</i>
	L x A (J)	-1.2739*
L x P (I)	H x P (J)	-1.1875*
	H x A (J)	-1.3713*
	H x P (J)	.0864
L x A (I)	H x A (J)	-.0975
	H x P (I)	-.1838

Hypothesis 2a postulated that the presence of one or more logos of internet seals of approval leads consumers to perceive less online payment risk over the transaction. In line with this hypothesis, there was a significant reduction in perceived risk, associated with the presence of the logos, when low reputation payment providers were involved, L x A vs L x P,  $\Delta = 1.27$   $p = .008$ . However, when the high reputation payment provider is involved, the results indicated no significant difference in perceived risk, H x A vs H x P,  $\Delta = 1.84$   $p = .988$ . Hence, Hypothesis 2a was partially supported but only for low reputation online vendors.

Hypothesis 2b postulated that the presence of a reputable payment provider leads consumers to perceive less online payment risk over the transaction. Pairwise comparisons of the mean showed a significant reduction in perceived risk associated with the low reputation payment provider, but it is only apparent in the presence of the logos, H x P vs L

$x P, \Delta = 1.19, p = 0,016$ ;  $H x A$  vs  $L x A, \Delta = 0.0975, p = .999$ , therefore, this hypothesis was not supported.

#### **4. Discussion**

When developing a new online business, with an unknown brand for the consumer, the online vendor should take into consideration that the consumer is taking a large risk by providing personal and financial information to the parties involved in the transaction. In order to reduce this perceived risk underlying the purchase of a product or service, the new online vendor can pursue several strategies. Four strategies were considered and manipulated in this study to understand changes in trust and perceived risk over the transaction. The first and second strategy included a low reputation payment provider, which is unknown to the consumer, and the presence or absence of internet seals of approval logos. In this strategy, there is a direct connection with the payment provider, and the consumer must provide their financial and personal data directly on the online vendor's webpage.

The results of the study have demonstrated that, when considering the investment of a low reputation payment provider and in reputable internet seals of approval certifications, the presence of one or more logos significantly reduces the perceived risk of the consumer. Interestingly, with the presence of a high reputation payment provider (PayPal), there was no significant difference in the groups where the logos are present or absent, leading to believe that the high reputation payment provider is a contributor itself for the reduction of the perceived risk.

However, this belief was not demonstrated, since when isolating the low reputation payment provider and comparing it with the high reputation payment provider (PayPal), the results showed that, in the presence of logos, the low reputation payment provider is

perceived to have lower risk. Therefore, the strategy which demonstrates the most significant reduction on perceived risk is when the payment provider has a low reputation and there is the presence of reputable internet seals of approval logos.

There is reason to believe that these results may have been affected by other aspects of consumer behavior, namely the consumers' perception of PayPal. This perception may be affected by the brand image, the users understanding of the technology, perception of security and privacy, or other aspects. Therefore, further investigation would have to take place to understand if these variables actually had an effect on the present study.

This study further demonstrated that consumers' trust over the online vendor is not significantly affected by the presence of any of the independent variables. These results go against the studies performed by Chang et al. (2013), which stated that the third-party certification of internet seals of approval significantly increases consumer trust in the online vendor, and the study by Preibusch et al. (2016), which states that the use of a high reputation payment provider can mitigate the trust deficit. This leads to the conclusion that further research regarding the trust variable in online purchases needs to be pursued through a confirmatory analysis of the present study.

The results of this study have relevant implications in practice. The main recommendation of this study is for new and unestablished online vendors considering a cost efficient payment strategy, to invest in a lower reputation payment provider which will require lower fees, but at the same time invest in third-party certification, namely on one or more reputable internet seals of approval which are easily recognized by the consumer. It is important to further mention that the consumer demonstrates a lack of understanding of the actual security measures, and technical knowledge of the different types of certifications, leading to believe that investing in certifications associated with well-known brands of anti-

virus products, such as Norton and MacAfee, may provide additional reduction of the perceived risk and therefore higher conversion rates. Overall, the online vendor must manage the necessary investment in third-party certifications and payment providers wisely, and as the business grows, continue to invest in security and encryption measures in order to guarantee data safety. The results of this study can be applied across various industries, namely across all companies and organizations which intend to sell products or services online.

The study presented limitations inherent to the research design, namely given the scenario-based approach. The validity of this research method can be affected by the low perceived realism over the scenarios. In practice, the study is limited in terms of other aspects of consumer decision making, namely the elimination of the aspect of product delivery, by using a digital product for the experimental setup, and the fact that the only payment method used was credit card which involves higher risk levels.

Ultimately, this study contributes to improving management practices by online vendors considering the possible investment in an efficient payments strategy which is able reduce costs while offering the highest conversion rates.

## **5. Conclusion**

The present study investigated how consumers behave in the transaction moment, and how the partnership between online vendors, third-party certifiers and payment providers can contribute to increase conversion rates. This study intends to understand which payment strategy could work most effectively in order to reduce the levels of perceived risk on the transaction moment, and therefore increase in conversion rates. The four strategies presented



were a combination of the presence or absence of reputable payment providers, together with the presence or absence of internet seals of approval logos.

The results have led to the conclusion that by investing in a payments strategy which combines a low reputation payment provider and the presence of the third-party certification in the checkout page, the unknown online vendor will be able to reduce perceived online payment risk by the consumer, and therefore enhance the possibility of purchase. Hopefully, this study will inspire further research in order to better understand how the consumer behaves at the moment of purchase, and how third-party certifications and payment providers are able to influence the transaction decision.

## References

- Adyen. (2015). *The Global E-Commerce Payments Guide*. San Francisco. Retrieved from <https://www.adyen.com/de/business-intelligence/global-ecommerce-payments-guide>
- Anderson, D. R., Sweeney, D. J., & Williams, T. A. (2011). *Statistics for Business and Economics. Statistics for Business and Financial Economics*. <http://doi.org/10.1198/tas.2006.s59>
- Bilgihan, A. (2016). Gen y customer loyalty in online shopping: An integrated model of trust, user experience and branding. *Computers in Human Behavior, 61*, 103–113. <http://doi.org/10.1016/j.chb.2016.03.014>
- Cases, A.-S. (2002). Perceived risk and risk-reduction strategies in Internet shopping. *The International Review of Retail, Distribution and Consumer Research, 12*(4), 375–394. <http://doi.org/10.1080/09593960210151162>
- Chang, M. K., Cheung, W., & Tang, M. (2013). Building trust online: Interactions among trust building mechanisms. *Information and Management, 50*(7), 439–445. <http://doi.org/10.1016/j.im.2013.06.003>
- Claire Greene, Schuh, S., & Stavins, J. (2013). *The 2013 Survey of Consumer Payment Choice : Summary Results*. Retrieved from <http://www.bostonfed.org/economic/rdr/index.htm>.
- Field, A. (2009). *Discovering Statistics using IBM SPSS statistics* (3rd ed.). London: SAGE

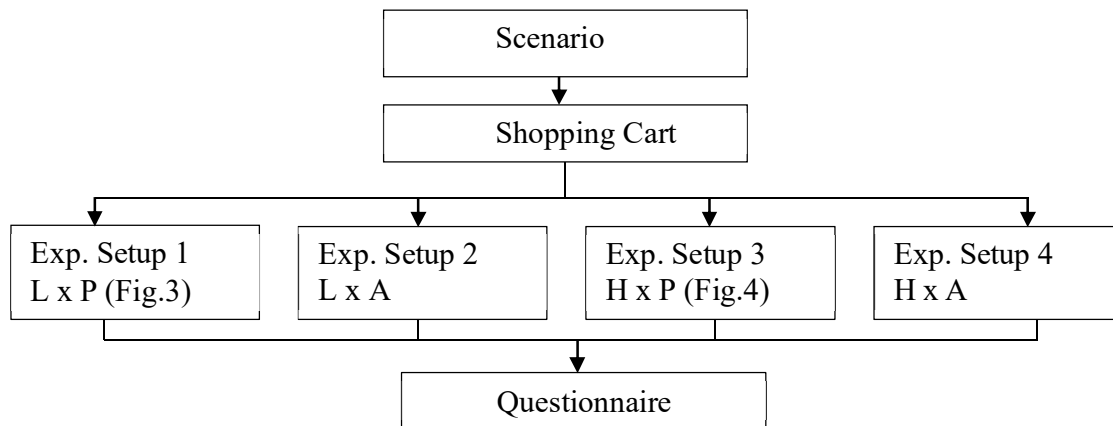
Publications.

- Gordon, L., & Lee, S. (1967). *Economics for Consumers*. New York: The American Book Company.
- Ha, H. (2004). Factors influencing consumer perceptions of brand trust online. *Journal of Product & Brand Management*, 13(5), 329–342. <http://doi.org/10.1108/10610420410554412>
- Holst, C. (2013). Which Site Seal do People Trust the Most? Retrieved from <http://baymard.com/blog/site-seal-trust>
- Hong, I. B., & Cha, H. S. (2013). The mediating role of consumer trust in an online merchant in predicting purchase intention. *International Journal of Information Management*, 33(6), 927–939. <http://doi.org/10.1016/j.ijinfomgt.2013.08.007>
- Hong, Z., & Yi, L. (2012). Research on the Influence of Perceived Risk in Consumer On-line Purchasing Decision. *Physics Procedia*, 24, 1304–1310. <http://doi.org/10.1016/j.phpro.2012.02.195>
- Jarvenpaa, S. L., Tractinsky, N., & Vitale, M. (2000). Consumer Trust in an Internet Store. *Information Technology and Management*, 1(2), 45–71.
- Köster, A., Matt, C., & Hess, T. (2016). Carefully choose your (payment) partner: How payment provider reputation influences m-commerce transactions. *Electronic Commerce Research and Applications*, 15, 26–37. <http://doi.org/10.1016/j.elerap.2015.11.002>
- Lees, A., & King, M. (2015). *World payment Report*. Capgemini Consulting and Royal Bank of Scotland. London. Retrieved from <https://www.worldpaymentsreport.com/>
- McKnight, D. H., Kacmar, C. J., & Choudhury, V. (2004). Dispositional Trust and Distrust Distinctions in Predicting High- and Low-Risk Internet Expert Advice Site Perceptions. *E-Service Journal*, 3(2), 35–58. <http://doi.org/10.2979/ESJ.2004.3.2.35>
- Miyazaki, A. D., & Krishnamurthy, S. (2002). Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions. *Journal of Consumer Affairs*, 36(1), 28–49. <http://doi.org/10.1111/j.1745-6606.2002.tb00419.x>
- Nicholas, A. J., & Lewis, J. K. (2008). Millennial Attitudes Toward Books and E-Books. *The International Journal of the Book*, 5(2).
- Palmer, J. W., Bailey, J. P., & Faraj, S. (2006). The Role of Intermediaries in the

- Development of Trust on the WWW: The Use and Prominence of Trusted Third Parties and Privacy Statements. *Journal of Computer-Mediated Communication*, 5(3), 0–0. <http://doi.org/10.1111/j.1083-6101.2000.tb00342.x>
- Parkinson, T. L. (1975). The Role of Seals and Certifications of Approval in Consumer Decision-Making. *Journal of Consumer Affairs*, 9, 1–13. <http://doi.org/10.1111/j.1745-6606.1975.tb00545.x>
- Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce*, 7(3), 101–134. <http://doi.org/10.1.1.86.7139>
- Preibusch, S., Peetz, T., Acar, G., & Berendt, B. (2016). Shopping for privacy: Purchase details leaked to PayPal. *Electronic Commerce Research and Applications*, 15, 52–64. <http://doi.org/10.1016/j.elerap.2015.11.004>
- Rajappa, K., Perumparambil, P., Baxley, D., PSV, V., Vergne, C., Sullivan, W., ... Thakur, R. (2012). Global Trends In The Payment Card Industry 2013. *Capgemini Consulting and Royal Bank of Scotland*. Retrieved from [https://www.capgemini.com/resource-file-access/resource/pdf/global\\_trends\\_in\\_the\\_payment\\_card\\_industry\\_2013\\_acquirer.pdf](https://www.capgemini.com/resource-file-access/resource/pdf/global_trends_in_the_payment_card_industry_2013_acquirer.pdf)
- Schoorman, F. D., Mayer, R. C., & Davis, J. H. (2007). An integrative model of organizational trust: Past, present, and future. *The Academy of Management Review*, 32(2), 344–354.
- Vos, A., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., & Giannakopoulos, G. (2014). Risk Reduction Strategies in Online Shopping: E-trust Perspective. *Procedia - Social and Behavioral Sciences*, 147, 418–423. <http://doi.org/10.1016/j.sbspro.2014.07.122>
- Wikipedia. (n.d.). Hacker. Retrieved from <https://en.wikipedia.org/wiki/Hacker>

## Appendices

### Appendix A: Experimental Setup Flowchart



### Appendix B: Scenario Introduction

For the next section of this questionnaire, you will be given a scenario regarding which some questions will be required answer.

Imagine that you are a book lover and that you currently have a special preference to read your books in an electronic format (Ebooks), rather than the hardcopy of a book. After some online browsing research, you have chosen Ebooks.pt to purchase the new Harry Potter and the Cursed Child novel. This product will be available for download immediately after the transaction is approved.

### Appendix C: Scenarios on the experimental Setup

Figure 2: Experimental Setup, Shopping Cart

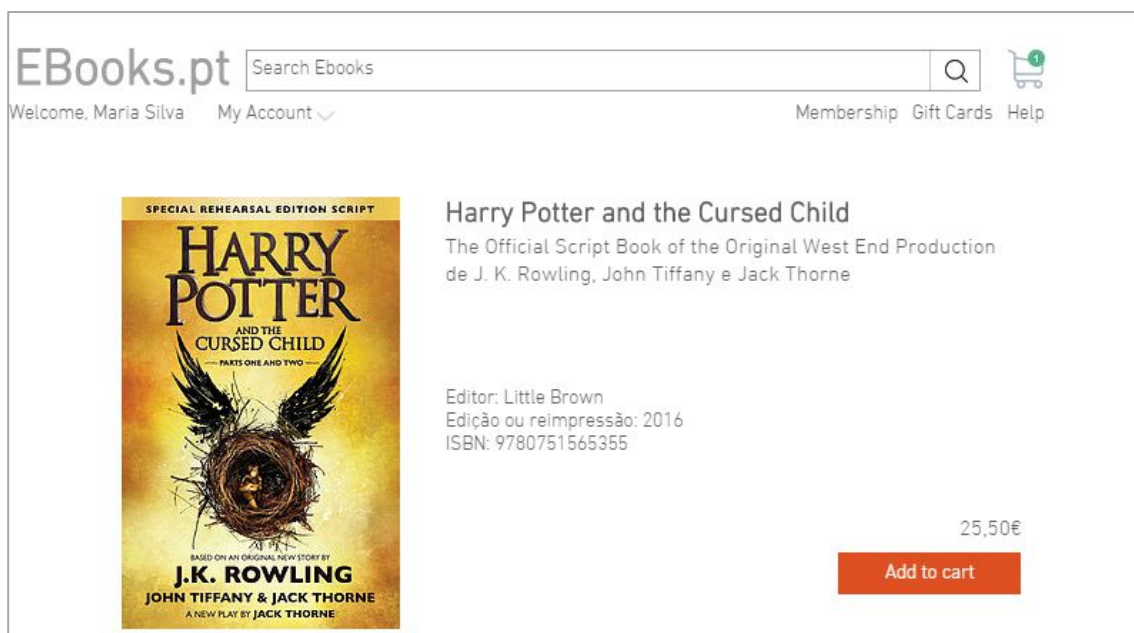





Figure 3: First experimental setup: low reputation payment provider, with logos

**EBooks.pt** Search Ebooks  

Welcome, Maria Silva My Account  Membership Gift Cards Help

## Order Summary

Subtotal (1 item) 25,50€  
Harry Potter and the Cursed Child - Parts I & II  
 by J. K. Rowling, John Tiffany, Jack Thorne  
 NOOK Book (eBook)




Estimated Shipping 0,00€  
 Available Immediately

---




**Order Total:** 25,50€

Please confirm your personal information

Shipping Information	Billing Information
Electronic delivery maria.silva@gmail.com	Maria Silva Rua de cima, nº3, 0000-000 Lisboa Portugal VAT NUMBER: 11111111



Please provide us you payment information   


Card Number	Name on Card	
**** * 4242	Maria Silva	
Expiration Date	Expiration Year	Security Code
01 - January	2020	123

**Confirm payment**

Figure 4: Third experimental setup: good reputation payment provider, with logos

**EBooks.pt** Search Ebooks  

Welcome, Maria Silva My Account  Membership Gift Cards Help


## Order Summary


Subtotal (1 item) 25,50€  
Harry Potter and the Cursed Child - Parts I & II  
 by J. K. Rowling, John Tiffany, Jack Thorne  
 NOOK Book (eBook)

Estimated Shipping 0,00€  
 Available Immediately

---


**Order Total:** 25,50€



Pay with PayPal English 

maria.silva@gmail.com

\*\*\*\*\*

From now on, skip login with One Touch™ 

For your security, we'll always ask you to log in to update your PayPal personal or financial info.

**Log In**

[Having trouble logging in?](#)

or

**Create an Account**

