

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

Sofia Cardoso¹ · Luis F. Martinez¹ 

Published online: 1 March 2018

© Springer Science+Business Media, LLC, part of Springer Nature 2018

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 impact consumer trust and online payment perceived risk. Four randomized experimental setups were used to manipulate the independent variables, on a sample size of 324 valid responses. The majority of participants were between 18 and 35 years old. The study results demonstrate that new online vendors could 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.

Keywords Consumer behavior · Online transactions · Payments strategy · Reputation · Digital marketing · Millennials

1 Introduction

The continuous growth of online transactions—via credit card and other emerging non-bank payment methods [20]—is leading to the increase of consumer concerns for personal and financial data privacy. Actions such as the Electronic Identification Service (eiDAS)—an example of the Key Regulatory and Industry Initiatives

✉ Luis F. Martinez
luis.martinez@novasbe.pt

¹ Nova School of Business and Economics, Universidade Nova de Lisboa, Campus de Campolide, 1099-032 Lisbon, Portugal

(KRII)—have been created with the intent of reducing consumers' perception of risk, and increase the trustworthiness on the online vendor, with the ultimate objective of positively influencing the purchase decision. The consumers' trustworthiness level acts as a significant aspect to build business to consumer relationships [3]. This aspect is especially relevant when the consumer is unfamiliar with the online vendor, and the consumer's trust levels are influenced by the dispositional trust and the broad evaluation of the second-hand information [22, 23]. The way to achieve consumer acceptance and reduce uncertainty is by manipulating favorable consumer attitudes and influencing transaction intention, thus trust-building mechanisms must be employed [29].

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 [24]. 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 [11]. The 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 [27]. Through his study, Parkinson [27], 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 [24]. As mentioned by Head and Hassanein [13], vendors displaying a privacy seal are ultimately conveying a message of disclosure of privacy standards assured by a third-party regulator.

One survey was conducted to understand the impact of the self-regulatory actions mentioned above. This survey was performed by the Baynard Institute [14] 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 [14] 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,¹ but the

¹ 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.

perceived security of the internet seals. Head and Hassanein [13] mentions how seals of approval aim to assure consumers that the online vendors' site is reliable by placing the logo or seal of a trusted third-party on their website. 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 [14].

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 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 [32].² When the online vendor has a direct connection with the acquiring bank, we can infer that there is a dyadic relationship between online vendor and consumer [17, 19], as the online vendor is the one obtaining the financial and personal data from the consumer, thus redirecting it to the acquiring bank. As this direct connection requires more technical expertise and effort from the online vendor side [31], smaller online vendors with fewer resources often engage with third-party payment providers [31]. These payment providers work as intermediaries between online vendors and consumers, to collect the consumer data, process and approve the transaction [31], and are usually non-banking payment systems (Non-Banks PSPs) which have made inroads into the immediate payments space [20]. By engaging with payment providers, a triadic relationship emerges [19, 31], in which this study will be based upon.

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. We intend to present a unique environment to test the hypotheses, namely by presenting four randomized experimental setups which will allow us to understand how the combination of the independent variables influence the consumers' trust levels and perceived risk. The results of this study will ultimately provide online vendors, the consumers' perspective regarding the trust and risk variables, and will influence future investment decisions regarding online payments security.

Additionally, this study underlines the online vendors' intention to convert visitors into buyers, as online vendors following this intention still face the challenge of establishing consumers' trust online [33]. Thus, it is important to understand how companies can communicate their trustworthiness to consumers [33]. Therefore, the main contribution of this study is to provide online vendors with various consumer perspectives, to ultimately choose the combination of internet seal of approval and third-party payment provider that best reduces consumer's trust and risk perception.

To accomplish the research purpose, the following research question was established: Does the presence of one or more logos of internet seals of approval,

² The Issuing Bank is the Bank or Financial Institution which grants Credit or Debit cards to the consumer [32].

and the presence of a reputable payment provider influence the level of consumers' trust and online payment perceived risk over the transaction?

Overall, this paper main contribution is to provide insights for new—or yet unestablished—online vendors who consider investing on payment providers and online security seals. We assume the presence of one or more logos on the checkout page significantly reduces the consumers' perceived risk, thus positively influencing their purchase decisions. This paper also provides a strong contribution to the research community, as it presents the results of an experimental setup study that focuses on understanding the impact of the combination between the presence of internet seals of approval logos and the reputation of the payment provider on consumer trust and perceived risk. While other studies have provided a strong contribution on the effect of seals of approval on online vendors' websites, this paper provides a more accurate testing of the impact of the presence of logos and the effect of the reputation of the payment provider specifically on the checkout page. To our best knowledge, this study is the first testing an experimental setup based on the relationship between vendor reputation and privacy seals tested on the checkout page. Moreover, the present study should be of interest for researchers working to improve the e-commerce environment, develop new security and privacy policies, and also for developing the customer relationship management strategies.

The remainder of this paper is structured as follows: the Sect. 1.1 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 Sect. 2, the method will be described, followed by the Sect. 3 with the study results and the Sect. 4 with the study discussion. In the Sect. 5 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 et al. [6] and Martinez and Zeelenberg [21], 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 et al. [34] 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 involves the willingness to take risks [34].

In the e-commerce environment it is necessary to take into account 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 [6]. Nonetheless, in the context of e-commerce, trust is founded by the relationship exchange given the

impersonal nature of the internet infrastructure [15], and therefore, the consumer trusts that the online vendor will behave in a favorable manner [22, 23]. 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 [29].

Throughout their studies, Chang et al. [6] 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 because risk cannot be totally eliminated in the online shopping environment [6]. Moreover, third-party assurance seals contribute to the institutional infrastructure of the e-commerce marketplace, as online vendors who agree to meet third-party standards and display the seal on their website are communicating to the consumers that the e-retailer is complying with the third-party requirements and can, therefore, be trusted [18].

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 [24]. 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 [24]. 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 consumer's perceived trust. Consequently, the following hypothesis was postulated:

Hypothesis 1 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. [31] state how intermediation can be used to overcome the shortfall of consumer trust, and how the use of a payment provider, namely a highly reputable one, 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, as the intermediary is able to overcome security and privacy concerns [31].

Hence, another possible strategy which new online vendors may employ to increase consumers' trust is to engage with a highly reputable payment provider as a third-party intermediary for payment processing. Accordingly, 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 2 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 [15] 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” [15]. Moreover, the consumer trusts and acts upon the belief that the e-commerce environment is secure to provide risk-free transactions [15].

Certain factors can act as ‘risk relievers’ and boost customers’ confidence, namely security, privacy, brand name, word-of-mouth, good online experience, and quality of information [12]. Pavlou [29] 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.³

Therefore, it is necessary to take into consideration that consumers’ online experience entails a higher risk perception when compared to shopping in physical stores [16] namely because: [1] the consumer is not able to physically 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; and, [4] the fact that transactions are remote and do not involve face-to-face contact between the vendor and consumer [5]. Thus, a consumer who perceives a very high risk regarding an online transaction is more likely to foresee a great loss potential [15].

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 Europe and USA, is still credit card in spite of the new, upcoming, alternative payment methods, such as digital wallets and prepaid cards [1]. Considering the information provided by Adyen [1], Visa and MasterCard still represent the highest percentage for online purchases in major European countries such as France and UK (80 and 87% respectively). Also, credit card payments for

³ *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 [38].

online purchases dominate in the US market, 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 because, when considering credit card payment method, it is necessary to provide important personal and financial information to the online vendor [15] and to the third-party payment provider [19]. Köster et al. [19] 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. Contrarily to previous research, which focuses on trust as a dyadic relationship [17], 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 [19]. Therefore, the payment provider also acts as an influencer to consumer perceptions and purchase behavior. As proposed by Köster et al. [19], the present paper proposes an adapted view of the triadic relationship between consumer, online vendor and payment provider—as presented in Fig. 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

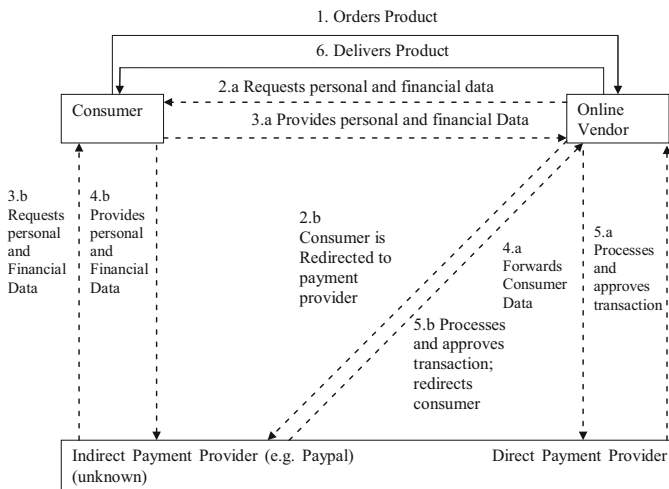


Fig. 1 Triadic relationship between consumer, online vendor and payment provider. Adapted from Köster et al. [19]

only one party, with whom the consumer has already developed familiarity and trust.

Furthermore, and notwithstanding of security measures, namely encryption and authentication, the insecurity regarding the leakage of information during the online transaction [15], and of privacy loss [19], reflect the consumer's fear that the transaction partner will act opportunistically [19]. 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 [26]. According to Vos et al. [37], this strategy can be successful as 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 this evidence, the presence of a logo of the internet seal of approval is expected to reflect a lower perceived risk, at the purchase moment.

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 [19]. Specifically, Köster et al. [19] were 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 vendors' website. The author concluded that the actual choice of a good and reputable payment provider works as an efficient trust-building mechanism.

The conclusions retrieved from the study performed by Köster et al. [19] imply that the presence of a high reputation payment provider has an influence in decreasing the consumers' perceived risk. However, deriving from the insights previously presented, we believe that the presence of logos of internet seals of approval on the checkout page of a low reputation online vendor may act as an important factor in the reduction of risk, regardless of the reputation levels of the third-party payment provider. Therefore, this study seeks to understand whether a combination of the presence of internet seals of approval logos on the checkout page as well as the presence of third-party low reputation payment provider (unknown for the consumers), is able to mitigate the perceived online payment risk over the transaction. Thus, the final hypothesis was postulated:

Hypothesis 3 The presence of one or more logos leads consumers to perceive less online payment risk, when in the presence of low reputation payment provider.

2 Method

2.1 Sample

In total, 331 responses were collected throughout the study, and after excluding incomplete responses, 324 were considered valid. Through the demographic data retrieved from the questionnaire, we found that 67.9% of the respondents were

females, and 92.6% were aged between 18 and 35 years old (i.e., Millennials or generation Y). According to Valentine and Powers [36], Millennials represent an important consumer group to determine the success of online retailers, as they are considered digital natives. Millennials also tend to frequently use online research in order to minimize purchase risk by reading other consumer reviews [36].

Demographic data and other important data characterization can be found in Table 1.

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,

Table 1 Demographic data

	Total	Exp. setup 1 L × P	Exp. setup 2 L × A	Exp. setup 3 H × P	Exp. setup 4 H × A	Statistic
Age (%)						
18–25	60.8	67.2	54.0	62.5	58.5	χ^2 (9) = 13.030, $p = .161$
25–30	25.9	23.4	34.9	20.3	24.6	
30–35	5.9	1.6	3.2	6.3	12.3	
35 +	7.4	7.8	7.9	10.9	4.6	
Gender (%)						
Male	32.1	37.5	31.7	39.1	36.9	χ^2 (3) = .827, $p = .843$
Female	67.9	62.5	68.3	60.9	63.1	
Academic degree (%)						
High School Graduate	10.5	6.3	14.3	9.4	12.3	χ^2 (12) = 9.277, $p = .679$
Bachelor Degree	33.6	40.6	30.2	29.7	33.8	
Master's Degree	51.2	46.9	50.8	56.3	52.3	
Ph.D.	3.1	4.7	4.8	4.7	.0	
Other	1.5	1.6	.0	.0	1.5	
Past experience of online shopping (%)						
Positive experience	77.2	24.1	24.6	24.6	26.6	χ^2 (6) = 1.113, $p = .981$
Negative experience	3.2	28.6	28.6	28.6	14.3	
Neutral experience	19.6	28.3	23.9	26.1	21.7	
Past experience of online shopping using a credit card (%)						
Positive experience	63.7	65.6	58.7	71.9	69.2	χ^2 (6) = 6.095, $p = .413$
Negative experience	3.9	3.1	1.6	3.1	6.2	
Neutral experience	32.4	31.3	39.7	25.0	24.6	

once a month, over the last 6 months. The data retrieved regarding internet usage was relevant to guarantee that the majority of the respondents were familiar with the environment presented for testing.

The past experience of respondents regarding online shopping was also assessed—67% agreed or strongly agreed that their past experience when purchasing online was positive, and 55.3% agreed or strongly agreed that their past experience when purchasing a product or service online using a credit card was positive. This aspect is noteworthy, since a sample with a strong representation of respondents that have experienced a negative past experience when purchasing online would have discredited the results of this study.

Moreover, we found no significant differences related to the demographic characteristics among the experimental groups, as the vast majority of respondents belonged to the Millennial generation. We also found no gender effects for the analyzed variables.

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 hypotheses. 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](#)” 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](#)” 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](#)” for examples on the scenario 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 [5, 6, 16]. 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 [25]. 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,⁴ which still represents one of the most popular alternatives to direct credit card processing, together with Amazon payments and Google wallet [35], and is considered the most pervasive online payment provider [31]. Furthermore, the good reputation internet seal of approval logos were chosen based on the study performed by the Baymard Institute [14], 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.

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].

The research method was tested using a 2×2 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 depicts the experimental setup design and sample sizes in each experimental group.

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.

⁴ Paypal provides funds transfers and acts as an e-wallet solution for consumers, with a global offer [20].

Table 2 Measurement and sources

Constructs	Adapted items	Sources
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. [2]
	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	Pavlou and Gefen [30]
	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. [4]
	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	
	Ebooks.pt is an online vendor who has more to lose than to gain by not delivering their promises	
	Ebooks.pt behavior meets my expectations	
Online payment perceived risk	The Ebooks.pt online vendor wants to be known as one who keeps promises and commitments	Jarvenpaa et al. [17], Doney and Cannon [7]
	Purchasing online involves the risk of private information loss when compared with more traditional ways of shopping	
	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	
	I would be concerned as to whether Ebooks.pt properly manages customers' private information	
	I would be concerned as to whether Ebooks.pt properly manages customers' private information	
Intended transaction	I would use my credit card to purchase from this online vendor	Gefen et al. [10]
	I am very likely to provide the online vendor with the information it needs to better serve my needs	

Table 3 Experimental setup

Internet seals of approval logos	Payment provider	
	Low reputation (L)	High reputation (H)
Presence (P)	L × P (n = 81)	H × P (n = 81)
Absence (A)	L × A (n = 80)	H × A (n = 82)

Table 4 Operationalization of constructs and measurement characteristics

Constructs	Adapted items	Loadings	Measures
Trust in the online vendor			
T1	I can count on this online Ebook store (Ebooks.pt) to be trustworthy	.765	CA = .765 AVE = .432 CR = .837
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	CA = .928 AVE = .924 CR = .961
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	CA = .783 AVE = .790 CR = .883
IT2	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 hypotheses 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.

Next, a one-way MANOVA was performed. The multivariate analysis of variance is used when there is the presence of more than one independent variable [9]. 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 [9]. There are several assumptions underlying this analysis, specifically random sampling, homogeneity of covariance of matrices, and multivariate normality [9]. 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. 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

Table 5 Means and standard deviations of dependent variables

Reputation of the payment provider	Low (L)		High (H)	
	Presence (P)	Absence (A)	Presence (P)	Absence (A)
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)

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 1 and 2 not to 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).

Hypothesis 3 postulated that the presence of one or more logos of internet seals of approval leads consumers to perceive less online payment risk, when in the presence of a low reputation payment provider (unknown for the consumer). In line with this hypothesis, there was a significant reduction in perceived risk, associated with the presence of the logos, when the low reputation payment provider was involved, $L \times A$ versus $L \times P$, $\Delta = 1.27$ $p = .008$. When the high reputation payment provider is involved, the results indicated no significant difference in perceived risk, $H \times A$ versus $H \times P$, $\Delta = 1.84$ $p = .988$. Hence, Hypothesis 3 was confirmed for low reputation online vendors.

Table 6 Pairwise comparisons for the online payment perceived risk variable

Mean differences (I-J)		Perceived risk
	L \times A (J)	- 1.2739*
L \times P (I)	H \times P (J)	- 1.1875*
	H \times A (J)	- 1.3713*
L \times A (I)	H \times P (J)	.0864
	H \times A (J)	- .0975
H \times P (I)	H \times A (J)	- .1838

* $p < .05$

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 combinations of internet seals of approval and payment providers. Four combinations were considered and manipulated in this study to understand changes in trust and perceived risk over the transaction. The first and second combination 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 combination, 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 combination 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.

This belief was confirmed, 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 combination 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, leading to the confirmation of the belief that the present of internet seals of approval, on the checkout page, is by itself a strong aspect to reduce trust.

There is a 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. [6], 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. [31], 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 to consider the combination of a lower reputation payment provider, but at the same time consider the 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. Additionally, another limitation of this study is that we did not conduct an ad-hoc analysis on logo versus no logo. Therefore, future research could seek to examine additional scenarios in order to test whether the mere absence or presence of logos, the number of logos, and the type of logos, could have an effect on the dependent variables.

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. Future research could entail testing consumer risk perceptions when in the presence of internet certifications which are associated with anti-virus brands, and how different types of payment providers have an influence on the same variables. Moreover, the testing of more experimental setups which include different types of logos and how the number of logos present on the check-out page may influence trust and perceived risk.

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

5 Conclusion

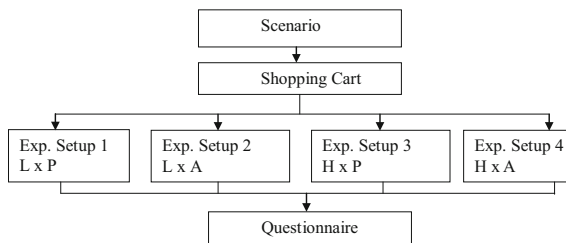
The present study investigated how consumers behave in the transaction moment, and how the partnership between online vendors, third-party certifiers and payment providers can contribute to enhance trust and reduce online payment perceived risk,

in an attempt to increase the possibility of converting online visitors into online buyers. 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 internet seals of approval logos on the checkout page, the unknown online vendor will be able to reduce perceived online payment risk by the consumer, and therefore enhance the possibility visitor conversion.

Acknowledgements This work was funded by National Funds through FCT—Fundação para a Ciência e Tecnologia under the project Ref. UID/ECO/00124/2013 and by POR Lisboa under the project LISBOA-01-0145-FEDER-007722. We thank Jorge Velosa for his comments on an earlier version of this manuscript.

Appendix

Experimental setup flowchart



Scenario introduction

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

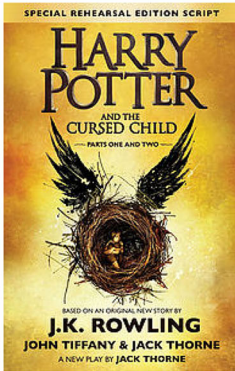
Imagine that you are a book lover and that you currently have a special preference to read your books in an electronic format (Ebooks), rather than the hardcopy of a book. After some online browsing research, you have chosen Ebooks.pt to purchase the new Harry Potter and the Cursed Child novel. This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

Scenarios on the experimental setup

Experimental setup, shopping cart

EBooks.pt 

Welcome, Maria Silva [My Account](#) [Membership](#) [Gift Cards](#) [Help](#)




Harry Potter and the Cursed Child

The Official Script Book of the Original West End Production
de J. K. Rowling, John Tiffany e Jack Thorne

Editor: Little Brown
Edição ou reimpressão: 2016
ISBN: 9780751565355

25,50€

First experimental setup: low reputation payment provider, with logos

EBooks.pt 

Welcome, Maria Silva [My Account](#) [Membership](#) [Gift Cards](#) [Help](#)

Order Summary


Subtotal (1 item) <u>Harry Potter and the Cursed Child - Parts I & II</u> by J. K. Rowling, John Tiffany, Jack Thorne NOOK Book (eBook)	25,50€
Estimated Shipping Available Immediately	0,00€
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	
<input type="text" value="**** * 4242"/>	<input type="text" value="Maria Silva"/>	
Expiration Date	Expiration Year	Security Code
<input type="text" value="01 - January"/>	<input type="text" value="2020"/>	<input type="text" value="123"/>


powered by VeriSign


CERTIFIED PRIVACY



Third experimental setup: good reputation payment provider, with logos

The screenshot displays the EBooks.pt website interface. At the top, there is a search bar for 'Search Ebooks' and a shopping cart icon. The user is logged in as 'Maria Silva', with links for 'My Account', 'Membership', 'Gift Cards', and 'Help'. The main content is divided into two panels. The left panel, titled 'Order Summary', lists the following items and prices:

Subtotal (1 item)	25,50€
<u>Harry Potter and the Cursed Child - Parts I & II</u>	
by J. K. Rowling, John Tiffany, Jack Thorne	
NOOK Book (eBook)	
Estimated Shipping	0,00€
Available Immediately	
Order Total:	25,50€

Below the order summary are security logos for Norton Secured, TRUSTe, and Secured by Trustwave. The right panel shows the PayPal login interface. It includes the PayPal logo, the text 'Pay with PayPal', and a language dropdown set to 'English'. The email field contains 'maria.silva@gmail.com' and the password field is masked with dots. There is a checkbox for 'From now on, skip login with One Touch™' and a note: 'For your security, we'll always ask you to log in to update your PayPal personal or financial info.' A blue 'Log In' button is present, along with a link for 'Having trouble logging in?'. Below this is an 'or' separator and a grey 'Create an Account' button.

References

1. Adyen. (2015). *The global e-commerce payments guide*. San Francisco. Retrieved from <https://www.adyen.com/de/business-intelligence/global-e-commerce-payments-guide>.
2. Benlian, A., Titah, R., & Hess, T. (2012). Differential effects of provider recommendations and consumer reviews in e-commerce transactions: An experimental study. *Journal of Management Information Systems*, 29(1), 237–272.
3. 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. <https://doi.org/10.1016/j.chb.2016.03.014>.
4. Butler, J. K., Jr. (1991). Toward understanding and measuring conditions of trust: Evolution of a conditions of trust inventory. *Journal of Management*, 17, 643–663.
5. 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. <https://doi.org/10.1080/09593960210151162>.
6. Chang, M. K., Cheung, W., & Tang, M. (2013). Building trust online: Interactions among trust building mechanisms. *Information & Management*, 50(7), 439–445. <https://doi.org/10.1016/j.im.2013.06.003>.
7. Doney, P. M., & Cannon, J. P. (1997). An examination of the nature of trust in buyer–seller relationships. *Journal of Marketing*, 61(2), 35–51.
8. Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: A perceived risk facets perspective. *International Journal of Human–Computer Studies*, 59, 451–474.
9. Field, A. (2009). *Discovering statistics using IBM SPSS statistics* (3rd ed.). London: SAGE Publications.
10. Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly*, 27(1), 51–90.
11. Gordon, L., & Lee, S. (1967). *Economics for Consumers*. New York: The American Book Company.

12. Ha, H. (2004). Factors influencing consumer perceptions of brand trust online. *Journal of Product & Brand Management*, 13(5), 329–342. <https://doi.org/10.1108/10610420410554412>.
13. Head, M., & Hassanein, K. (2002). Trust in e-commerce: Evaluating the impact of third-party seals. *Quarterly Journal of Electronic Commerce*, 3(3), 307–325.
14. Holst, C. (2013). Which site seal do people trust the most? Retrieved from <http://baymard.com/blog/site-seal-trust>.
15. 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. <https://doi.org/10.1016/j.ijinfomgt.2013.08.007>.
16. Hong, Z., & Yi, L. (2012). Research on the influence of perceived risk in consumer on-line purchasing decision. *Physics Procedia*, 24, 1304–1310. <https://doi.org/10.1016/j.phpro.2012.02.195>.
17. Jarvenpaa, S. L., Tractinsky, N., & Vitale, M. (2000). Consumer trust in an internet store. *Information Technology and Management*, 1(2), 45–71.
18. Kimery, K. M., & McCord, M. (2002). Third-party assurances: Mapping the road to trust in e-retailing. *Journal of Information Technology Theory and Application*, 4(2), 63–82.
19. 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. <https://doi.org/10.1016/j.elerap.2015.11.002>.
20. Lees, A., & King, M. (2015). *World payment Report*. Capgemini Consulting and Royal Bank of Scotland. London. Retrieved from <https://www.worldpaymentsreport.com/>.
21. Martinez, L. F., & Zeelenberg, M. (2015). Trust me (or not): Regret and disappointment in experimental economic games. *Decision*, 2(2), 118–126. <https://doi.org/10.1037/dec0000025>.
22. McKnight, D. H., Kacmar, C. J., & Choudhury, V. (2004). Shifting factors and the ineffectiveness of third party assurance seals: A two-stage model of initial trust in a web business. *Electronic Markets*, 14(3), 252–266. <https://doi.org/10.1080/1019678042000245263>.
23. 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. <https://doi.org/10.2979/ESJ.2004.3.2.35>.
24. 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. <https://doi.org/10.1111/j.1745-6606.2002.tb00419.x>.
25. Nicholas, A. J., & Lewis, J. K. (2008). Millennial attitudes toward books and e-Books. *The International Journal of the Book*, 5(2), 81–92. <https://doi.org/10.2139/ssrn.2684872>.
26. Palmer, J. W., Bailey, J. P., & Faraj, S. (2000). 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*. <https://doi.org/10.1111/j.1083-6101.2000.tb00342.x>.
27. Parkinson, T. L. (1975). The role of seals and certifications of approval in consumer decision-making. *Journal of Consumer Affairs*, 9, 1–13. <https://doi.org/10.1111/j.1745-6606.1975.tb00545.x>.
28. Pappas, I. A., Kourouthanassis, P. E., Giannakos, M. N., & Chrissikopoulos, V. (2016). Explaining online shopping behavior with fsQCA: The role of cognitive and affective perceptions. *Journal of Business Research*, 69(2), 794–803. <https://doi.org/10.1016/j.jbusres.2015.07.010>.
29. 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), 69–103.
30. Pavlou, P. A., & Gefen, D. (2004). Building effective online marketplaces with institution-based trust. *Information Systems Research*, 15(1), 37–59.
31. Preibusch, S., Peetz, T., Acar, G., & Berendt, B. (2016). Shopping for privacy: Purchase details linked to PayPal. *Electronic Commerce Research and Applications*, 15, 52–64. <https://doi.org/10.1016/j.elerap.2015.11.004>.
32. 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.
33. Schlosser, A. E., White, T. B., & Lloyd, S. M. (2006). Converting web site visitors into buyers: how web site investment increases consumer trusting beliefs and online purchase intentions. *Journal of Marketing*, 70(2), 133–148.
34. Schoorman, F. D., Mayer, R. C., & Davis, J. H. (2007). An integrative model of organizational trust: Past, present, and future. *Academy of Management Review*, 32(2), 344–354.

35. Schuh, S., & Stavins, J. (2015). The 2013 survey of consumer payment choice: Summary results. *Federal Reserve Bank of Boston Research Data Reports*, 15(4), 1–64.
36. Valentine, D. B., & Powers, T. L. (2013). Online product search and purchase behavior of generation Y. *Atlantic Marketing Journal*, 2(1), 76–91.
37. 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. <https://doi.org/10.1016/j.sbspro.2014.07.122>.
38. Wikipedia. (2016). *Hacker*. Retrieved from <https://en.wikipedia.org/wiki/Hacker>.