ROLE OF TRUSTMARK IN E-COMMERCE

Dr. Sandeep Nath Modi

#1 Assistant Professor, National Institute of Financial Management, Government of India
#1sandeepnathmodi@rediffmail.com

Abstract

E-commerce trust marks are used as a way for online shoppers or users to be protected by online service providers who ensure that websites are securely processing information that could be used to share their persona, financial transactions or cause any harm through hacking, sharing of data, viruses or other intervention related to data exchange such as denial of service etc. The trust mark shows that the website being visited offers consumer protection of data and privacy of interaction so that their online shopping may be made safely and their personal information only ever shared with authorized recipients. Trust marks confirm that a business has been accredited by another organization who may or may not be of importance. Accreditations from well-known organizations such as the Better Business Bureau (BBB), TRUSTe, Verisign, McAfee Secure and Comodo Hacker Proof are usually of more value from a customer confidence viewpoint. This Research Paper studies the Behavioural aspects of online users to assess impact of Trust Marks on Online service providers. Secondary data has been used for analysing the role of Trust Marks in E-Commerce. Findings of this Paper is that Tools like Secure Sockets Layer (SSL), BBonline, Security Certificate, Service Level Agreement (SLA) increases trust level of Online Shoppers and in turn enhances business opportunities for Service Providers on Virtual Platform. This in turn reduces Grievances among consumers and reduction in Cyber Crimes. Suggestions include use of recognizable trust badges, include different kinds of trust badges to influence trust on multiple levels, look out for niche trust badges that are relevant to business, place payment related trust badges closer to critical page components like credit card information fields, if there is a small brand, trust badges are likely to yield major dividends, focus should be on quality and quantity of reviews, feature both negative and positive reviews; consumers find it authentic and therefore more trustworthy, generate reviews from actual users of the product rather than from associations or professional reviewers.

Key Words: E-Commerce, Trust Marks, Trust, Trust Badges, Security, Cyber Laws.

1. INTRODUCTION

E-commerce trust mark is an electronic commerce badge, image or logo displayed on a website to indicate that the online business sites are trustful by the issuing organization. A trust mark gives confidence to end users and indicates to them that it is safe to do business with the web site displaying it[1]. For doing business with someone trust is the most important element that has to be considered. Although online shopping is rapidly picking up speed all around the world, many people are not so comfortable with online purchases. And even the existing online buyers hesitate to purchase from new online websites. The thing that is crucial for any website is to assure the visitors that it is safe, secure and reliable. Trustmark logos are one such trust symbol that certify the security and reliability of a website.
Trust marks or trust logos are images of third-parties which test the website for various security and privacy requirements, fair dealings in business transactions, good business practices and a carbon neutral certification badge[2]. Credibility of business is symbolised by certification badge of a third party. Although a person has so many options to choose from, it is really important to judge which trust mark should be put on the website. Business Owners must spend money on those Trust marks which gets recognition from customer. Also, along with user recognisability, one should check for the type of certifications that comes with the logo. For instance McAfee Secure is against hacking and vulnerabilities, PayPal Verified signifies protection against fraud and the VeriSign Trust Seal, which is now the Symantec is for Security and Encryption, which provides Secure Sockets Level (SSL) certificates to websites. SSL is used for exchange of credit card, tax, banking, or personal information to a business server somewhere. Examples of trust mark service providers are:

1. The Better Business Bureau (BBB): The BBB maintains the BBB Online that confirms the business has been accredited by the BBB.
2. TRUSTe: This is a website privacy service provider for hosting online privacy policy.
3. VeriSign: In this websites are secured by VeriSign SSL certificates which indicate the website is using the latest traffic encryption protocols.
4. McAfee Secure: This advises visitors that a site uses McAfee security scanning services on its ecommerce pages to protect from hackers and their vulnerabilities.
5. Comodo HackerProof: This is a trust mark for 24 X 7 scanning service that checks for security issues and reminds visitors of their security at the site bearing the logo.
6. CompTIA: This is a trust mark being given to IT Companies which provide services to their clients as per standard operating procedures, best practices and the right systems and tools.
7. Trust Mark Model: Gems and Jewellery Federation (GJF) came out with Trust Mark Model (TMM) for Gems and Jewellery members to grow their business and achieve Efficiency. TMM works on unique Business Excellence Model initiative developed by ISOQAR for GJF.

2. E-COMMERCE IN INDIA

India's e-commerce market share was worth about $13.6 billion in 2014, it went up to $23.0 billion in 2015 which is expected to touch $119.0 billion in 2020. In 2015, the e-retail segment was worth US$6.0 billion. About 70% of India's e-commerce market is related to tours and travel transactions. According to Google India, there were 35 million online shoppers in India in First Quarter of 2014 and is expected to cross 100 million mark by end of year 2016. CAGR is around 8–10%. Electronics and Readymade Garments are the biggest categories in terms of sales [3].

By 2020, India is expected to generate $119.0 billion online retail revenue out of which $35 billion will be through fashion e-commerce. Online electronics and apparel sales are set to grow five times in coming years [4].

Key drivers in Indian e-commerce are:

- Increasing rate of Internet Users and a recent introduction of 4G across the country.
- High growth in smartphone users India is world's second largest smartphone user base.
- Rising standards of living due to increase in per capita income of population.
• Availability of much wider product range compared to what is available at brick and mortar retailers.
• Competitive prices in comparison to retailers due to reduced inventory and real estate costs.
• Sale and Purchase of Second hand goods on online classified sites.
• Evolution of Million-Dollar start-ups like Jabong.com, Saavn, Make my Trip, Book my show, Zomato Etc.

India's retail market was at $600 billion in 2015 and is expected to grow to $1300 Bn by 2020, estimated CAGR of 10%. According to Forrester, the e-commerce market in India is set to grow the fastest in the Asia-Pacific Region at a CAGR of over 57% between 2012 –16[5].

In India, popular Trust Mark certificate companies include Symantec, Comodo, McAfee, RapidSSL among others. These badges/certificates can be purchased from various certificate companies, like Trustico from domain vendors like GoDaddy and BigRock. It is essential to have online store verified by at least one of the above mentioned third-parties, as it will enhance trust and credibility in front of the visitors. In a retail store, a customer is more trusting as he/she can have a face to face interaction with the seller. Online retailers have their hands tied in this regard. In order to increase customers’ confidence level regarding security of the website and their money isn’t getting involved in a retail fraud, website owners need to have a standardized assurance[6]. Consumers have growing concerns about fraud and identity theft when doing business or shopping online. Online retailers secure online transactions with data security. However, consumers need assurance regarding their personal information being secure and will not be breached by hacker attempts. This has created a demand for e-commerce trust marks to reduce consumer privacy and address security fears.

3. ROLE OF TRUST MARK IN E-COMMERCE

When clicking an e-commerce trust mark, a browser will usually display the company’s website information as well as the validity period of the certificate. The trust mark certificate is used to secure communication from user computers to the company’s website. Having a valid certificate ensures that all information and communications are secure and protected. Trust marks can easily be faked and there is software that will create dummy graphics to produce one. The only way to tell is to visit the issuing website to ascertain how genuine the issuer of the trust mark is. The widely known ones are easy to check out online with a link from the logo. If there is no hyperlink, there is little reason to afford any trust.

Comodo had conducted a survey in 2005 where 78 percent of the online shoppers said that a seal indicates that their information is safe and secure. Till today this holds true, besides a secure https connection, a sceptical customer is more likely to make a purchase if the web store has a security badge. These badges and certificates cost money, annual fees costing a minimum of around INR 16K and going upto almost a lakh. It is possible for many e-tailers to wonder if they actually need to have a paid certification to attract more customers[7]. The answer is yes they do. In a case study couple of years back, it was found that trust badges on websites lead to 32% increase in online business. No online service provider would want to let go of that much of a consumer base. However, a well visible certificate of trust mark need not be the sole criteria for the success of an online store. We took a look at the three well-known names in the Indian e-Commerce industry – Myntra, Jabong and Flipkart. The first two offer 256-bit SSL security only,
whereas Flipkart has its own security seal with a green padlock in the address bar. A retailer, particularly a new one, cannot take the risk with its credibility among its customers. Bob Angus, Partner Marketing Manager at PayPal, wrote in a blog, e-Commerce merchants need to establish trust and secure their customers confidential data with the best. The good news is that SSL investment usually pays off with a bump in sales and loyal customers.

4. TYPES OF TRUST MARK

- Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL) is a standard protocol used for the secure encryption or transmission of documents over a network. It is developed by Netscape. SSL technology creates a secure link between a Web server and browser to ensure private and integral data transmission. SSL uses Transport Control Protocol (TCP) for encryption or communication. The word socket means the mechanism of transferring data between a client and server over a network. For secure Internet transactions, a Web server needs an SSL certificate to establish a secure connection. SSL encrypts network connection above the transport layer, which is a network connection above the program layer. SSL uses an asymmetric cryptographic mechanism, in which a Web browser creates a public key and a private (secret) key. The public key is placed in a data file known as a certificate signing request[3]. The private key is issued to the recipient only. The objectives of SSL are:

- Data integrity: Data is protected from tampered with or altered with.
- Data privacy: Data privacy is ensured through a series of protocols, including the SSL Record Protocol, SSL Handshake Protocol, SSL Change Cipher Spec Protocol and SSL Alert Protocol.
- Client-server authentication: The SSL protocol uses standard cryptographic techniques to authenticate the client and server. SSL is the predecessor of Transport Layer Security (TLS), which is a cryptographic protocol for secure Internet data transmission.

- Bbb online

BBB online is a component of the Better Business Bureau that brings that organization’s power online. Through the BBB online program, users can evaluate businesses to see whether they stand up to the test of Web legitimacy. This service is in addition to work that its offices do with brick-and-mortar stores and enterprises. There are two parts to the BBB online evaluation and standards certification program: a BBB online reliability seal and a BBB online privacy seal [1]. The BBB online reliability seal shows that a website meets legitimate standards. This clarifies as to whether the business has provided accurate and trustworthy information, terms of sale are properly disclosed and security checks are in place on the business’s website. The BBB online seal reveals that shows privacy standards have been applied to website operations. Websites have to apply though filling web form, although some accredited businesses may be able to skip this process.

- Security Certificate

Security certificates are data file used as an Internet security technique through which the identity, authenticity, safety and reliability of a website or Web application is established. A security certificate is useful in providing the level of security of a website to general visitors, Internet service providers (ISPs) and Web servers. A security certificate is a digital certificate and works as a Secure Socket Layer (SSL) certificate. A security certificate is allotted to a website by a third-party certification authority (CA). Typically, the CA examines the specific security requirement of the website requesting the security certificate. Certificate is given on testing the authenticity, legitimacy and security of the website. This security certificate is embedded in the website
and is provided to servers, browsers, firewall and security applications, and ISPs when the website is requested. Updation of certificate is done on an annual basis or in a predefined time period [5]. On expiry of time period of certificate, a user will see a notification in browser of website stating that the security certificate is expired and the user may deal with the website at his own risk.

- **Service Level Agreement (SLA)**
A Service Level Agreement (SLA) is the contract of service between a service provider and customer. A SLA provides specific and measurable service offerings. SLAs are often included in signed agreements between Internet service providers (ISP) and customers. It is an operating level agreement (OLA) when used in an organization without a formal provider-customer link. Adopted in the late 1980s, SLAs are currently used by most industries. SLAs define output of service but defer methodology to the service provider's discretion. Specific requirements vary by industry and purpose of SLA. SLAs features include:

- Specific details and scope of provided services including responsibilities, priorities and guarantees.
- Specific, expected and measurable services at minimum or set levels.
- Whether formal and legally binding or informal.
- Detail tracking and reporting guidelines.
- Detailed problem management procedures.
- Structure of fees and expenses.
- Customer duties and responsibilities.
- Disaster recovery procedures.
- Terms of Agreement termination.

A customer transfers partial business responsibilities to an external service provider. The SLA serves as an effective tool for current and continuous provider-customer work phases.

5. **CRITICISM**
Third party verification from a reliable source and a strategically placed trust seal may assure customers about the safety and security. Some trust seals, such as McAfee Hacker Safe, however, have been criticized for not securing the interest of users of websites such as because they intentionally mark as 'Hacker Safe' websites like McAfee is having Cross-site Scripting or XSS vulnerability. Most seals are a simple image that can be copied and pasted into their sites by hackers. Such lapses highlight the importance of anti-XSS protection security measures. If the Trust seals are not updated or scanned on a daily basis these sites can give an illusionary picture of security as they are awarded at a certain point of time and the scan date must be displayed. When a site is not scanned daily, hackers can take advantage of change in technology and loopholes of websites resulting websites will not show any flaw or weaknesses in technology. The iconographical value is too high to mislead customers unaware about these changes.

6. **CONCLUSION**
The future of Trustmark in E-Commerce is difficult to predict. There are various segments that would grow in E-Commerce in the future like: Travel and Tourism, apparels, electronic appliances and hardware products. There are also some essential factors which will contribute to the boom of the Trustmark in India i.e. safety, security, reliability, Trust Level, Policy of website, Commitment of Trust mark certificate provider, attitude of company in website designing, locational services, right content, quick Service, T & C should be clear & realistic. We found various types of opportunities for online service providers like retailers, wholesalers/distributors, producers and also for people. Retailers get e-orders and should be in constant touch with the consumers all the time. Wholesalers can take advantage of ECommerce who are capable of establishing
contacts with reputed manufacturers and linking their business with the on-line trust mark certification companies. Producers can also linking themselves with on-line, by giving better information about their trust marks reliability to other links in the business chain and by a having a unique brand identity. Hence, the people who wish to take advantage of it can establish cyber and have their benefits. People could found various opportunities of employment. On the behalf of above said reports and experts view showed that the future of trust marks would be bright in the upcoming years if all essential factors would be implemented. Make trust mark companies address and phone number visible at all times, web design matters, make it very easy to contact you, message relevance and tailoring, simple language, correct spelling, link to external websites that reference trust mark organisation, provide staff detail and photos, photos of trust mark office, Email policy. All statements and claims should be backed up by expert evidence, neutral experts or scientific studies. List sources. Avoid superlatives. Detailed product information. Show prices. Show client list. Mention the number of clients. Show a link with a reputable organization. Use testimonials. Use case studies to prove the benefits of trust mark services and to show off your expertise. Both make trust mark websites more trustworthy. Put customer reviews. If websites take credit cards online, is it safe? Provide the information about secure channels, 256-bit encryption and what not. Take credit card payments? Prove the customer its safe (256-bit SSL encryption etc.). Use various Trustmark, Have people opt-in to your email list? Put a privacy seal on your site. And so on. Find out what’s a known trust mark on among your customers, and use it. Maintain a blog. When Oprah recommends a website, it’s instantly credible. Users of trust marks must know the trust end users enjoy while using trust marks. Have a social media outlet. If websites have an active Twitter account or Facebook page, it furthermore shows there are real and genuine people behind the organization. What does WOT say about trust mark certificates? WOT user community has rated over 42 million websites. Some people might check you out there. Keep ads to a minimum, Be a good and honest person. If websites are not having good intentions and treat their customers bad, it will come out eventually. Be friendly, generous and honest – always.

REFERENCES


[4] Sharma Shweta, Mittal,Sugandha, “Prospects of E-Commerce in India”

