

GLOBAL BUSINESS DIALOGUE ON ELECTRONIC COMMERCE



TRUSTMARK

SEPTEMBER 26, 2000

Issue Chair: Michio Naruto
Special Representative and Chairman
Fujitsu Research Institute

Issue Sherpa: Shinnosuke Date
Fujitsu, Ltd.
Tel: + 81-3-3215-5067
Fax: + 81-3-3215 5068
email: date@eag.fujitsu.co.jp

Contact Point:
(Americas): Jean Monty
President and CEO
BCE, Inc.

Contact Point:
(Europe/Africa) Rijkman W.J. Groenink
Chairman of the Managing Board
ABN AMRO Bank, N.V.

Introduction

The GBDe endorses the use of Trustmark programs in order to encourage good online business practices by merchants and to assist consumers in identifying merchants they can trust. To help avoid confusion for consumers among different trustmark programs offering different levels of protection, the GBDe has thus developed guidelines, to help ensure greater transparency, minimum voluntary standards and comparable levels of protection among competing trustmark programs. These guidelines have been developed based on initial consultations with all stakeholders. They will be developed further in response to comments received from business and consumer groups.

The GBDe believes that trustmark programs should be developed and operate in accordance with some minimum, voluntary guidelines. In particular, they must:

- be affordable, in particular to SMEs;
- be enforced rigorously, by providing clear monitoring and reporting mechanisms and guaranteeing neutrality of their enforcement decisions;
- be easily accessible to consumers when entering the merchants' web site and broadly disseminated;
- be developed in consultation with all stakeholders;
- use appropriate security measures to prevent misuse of the trustmark;
- offer a mechanism for consumer redress along the lines of the GBDe ADR recommendations;
- require minimum standards of behavior by merchants in the areas of online business practices, privacy protection and complaints handling, in line with GBDe recommendations.

Recommendations

Business should support and participate in such programs to ensure greater transparency and to encourage comparable levels of protection for consumers across national boundaries. Further, companies and organizations developing trustmark programs are encouraged to develop mutual recognition or other arrangements with programs in other countries or regions that meet the GBDe guidelines, to assist consumers in identifying foreign trustmark programs that offer equivalent protections.

These Guidelines are divided into two sections. The first sets out general guidelines for companies or organizations that develop trustmark programs. The second sets out general guidelines for merchants that establish best business practices governing commercial relations between merchants and consumers that should be required by trustmark programs. The paper also includes Recommendations to governments relating to the development and promotion of such programs.

DEFINITIONS

In order to ascertain the scope of these Guidelines and Recommendations, the GBDe has agreed to use the following working definitions:

“trustmark”: “a label indicating that a merchant commits to complying with a number of best business practices, including redress mechanisms”.

“certifier”: “company/organization that develops, manages the trustmark program and attributes the trustmark”.

“commercial relations”: “any transaction or agreement relating to the provision of a good or service, including commercial communications, between a merchant and a consumer conducted online, including through the Internet”.

“consumer”: “any natural person acting for purposes which are outside his or her trade, business or profession”.

“merchant”: “company/organization offering a good or service to consumers and accepting orders directly from consumers that receives, uses the trustmark and commits to complying with the trustmark specifications”.

“personal data”: “of a consumer means data that identifies the consumer or that can easily be combined with other available data to identify the consumer”.

GUIDELINES FOR CERTIFIERS

1. Accessibility

- 1.1. Trustmark programs should accommodate different business models and regulatory regimes to ensure that trustmarks do not erect barriers to competition.
- 1.2. Participation in a trustmark program should be open to any organization that agrees to abide by the entry conditions, consistent with the legitimate business objectives of the certifier. The criteria for participation in a trustmark program should be transparent to applicants and to consumers.
- 1.3. Subscription fees should not constitute an insurmountable obstacle to join a trustmark program. This should not discourage the setting up of additional fees for specific value-added services.
- 1.4. Certifiers are encouraged to offer specific conditions for SMEs in order to facilitate the participation of SMEs in a trustmark program.

Enforcement Mechanisms

The certifier should put in place effective mechanisms to establish and monitor compliance by the merchant of the trustmark program specifications. These may include random checks by the certifier, independent verification, and/or regular reporting requirements by the merchant.

The certifier should clearly include in the contract with the merchant the type of actions that will be undertaken if the merchant does not comply with the program requirements.

The type of actions that the certifier can undertake could include:

withdrawal of the trustmark;
public warning about misuse of the trustmark;
referral to governmental authorities;
legal action against a merchant in breach of the program's requirements, but who displays the trustmark.

- 2.4. The certifier should disclose publicly and prominently the type of actions that it will undertake in order to ensure compliance with the program.
- 2.5. The certifier should take all measures to seek impartiality and objective enforcement. This may include appointing independent persons or balanced business and consumer representation to the respective accreditation and enforcement bodies.

Visibility

3.1. The certifier should advise the merchant about suitable locations for the trustmark.

The trustmark should be prominently visible to the consumer in any of the following locations:

on the welcome page of the merchant's web site;

in case of privacy trustmarks, at a stage in the transaction prior to the collection of personal data from consumers;

on the page where vendors or consumers initiate a transaction by making a clear offer.

Certifiers should ensure that it is clear to consumers what the trustmark certifies (for example, by using a "pop up" screen that briefly describes the program) and that the code of conduct, principles, or best business practices which are the basis of the granting of the trustmark seal are accessible to the consumer, preferably by clicking on the trustmark seal.

4. Stakeholders Participation

Consumer, industry or professional organizations should ensure that they consult each other when developing trustmark programs.

The most important elements in which dialogue among the different stakeholders is essential are the content of codes of conduct, enforcement mechanisms and redress measures.

5. Security

The certifier should take appropriate measures to ensure that consumers can easily distinguish between real and counterfeit trustmarks. This may include technology to guarantee that unauthorized parties cannot copy the trustmark, secure links to a database accessible on the merchant's website, or technology to monitor web pages that are displaying the trustmark.

The certifier should take appropriate measures to maintain confidentiality of commercially sensitive information exchanged with the merchants it certifies.

6. Redress

- 6.1. Access to the certifier must be readily available to consumers and others to accept complaints and to act on them.
- 6.2. The certifier should ensure that the merchant has in place an internal complaint resolution system to which the consumer can have on-line access.
- 6.3. The certifier should offer or, under certain circumstances, as determined in the contract between the certifier and the merchant, require the merchant to offer an alternative dispute resolution (ADR) procedure. ADR systems may be offered by the certifier, the merchant itself or may be outsourced by the merchant.
- 6.4. In any case, the certifier should respond to consumers' complaints either by directing consumers to the appropriate mechanism or by contacting the merchant.
- 6.5. Certifiers should follow the GBDe Recommendations on ADR.

7. Flexibility and Mutual Recognition

The certifier should include an on-line mechanism to allow interested parties to give input on the performance of the system or any other related element of the trustmark program. The certifier should undertake continuous monitoring on consumers' satisfaction with the use of the trustmark program by merchants and should take due notice of the surveys' results.

The certifier should have all the necessary information about the requirements to join the program available on-line or in an electronic version. This information should be provided in a simple manner to ensure easy comprehension of the terms of participation.

The certifier should take all reasonable steps to ensure a speedy decision on participation in the program by the applicant organization. It is desirable that all steps to join a trustmark program can be conducted on-line. This does not preclude the necessity to undertake physical checks (e.g. about the real existence of the organization).

The certifier should put in place all appropriate mechanisms to ensure public dissemination of the trustmark program (e.g. links with Internet portals, consumers' organizations, etc). The certifier must include a list of all certified merchants that must be prominently shown in the trustmark program web page.

The certifier should consider developing mutual recognition or similar arrangements with trustmark programs in other countries or regions, such that merchants certified under one program that complies with these guidelines can be identified by consumers in other jurisdictions as offering equivalent protection.

Guidelines for Merchants

The trustmark programs certified by the Certifier must ensure minimum standards of behavior by merchants in accordance with the following Guidelines, which apply to commercial relations between certified merchants and consumers. These Guidelines would not alter or replace other obligations that a merchant may have as a result of consumer protection, privacy or other laws and regulation or any other voluntary codes of conduct to which a merchant may subscribe.

1. Accuracy and Accessibility of Information

All information required to be disclosed by the merchant shall be clear, accurate, and easily accessible online. The information shall either be posted on or accessible through a hyperlink from the merchant's homepage or entry point of the online site or at a place where the transaction is offered.

Merchants shall not make any representation or omission or engage in any practice that is likely to be deceptive, misleading, fraudulent or unfair to consumers.

Marketing Practices

Merchants should take the necessary steps to ensure that any representation about a good or service is current, accurate, and not deceptive or misleading to consumers and that the truthfulness of objective claims be substantiated.

- 1.1. If marketing or other online activities are directed at children, or where the website knows the visitor is a child, merchants shall take special care to protect children by recognizing their vulnerabilities. In particular, a merchant shall seek to ensure parental permission is obtained before collecting, using or disclosing the child's personal data or completing a transaction.

Information About the Merchant

Merchants should provide, at a minimum, the following contact information online:

legal name;

the name(s) under which it conducts business;

the principal physical address, addresses of representative offices in other countries or other information sufficient to ensure the customer can locate the business offline;

an online method of contact such as e-mail;

a point of contact within the organization that is responsible for customer inquiries; and

a telephone number, unless to do so would be disruptive to the operation of the business given its size and resources and then the merchant should maintain a working listed phone number, the time zone in which it operates, and the hours when contact may be made.

Information About the Goods and Services

Merchants shall provide enough information about the goods or services available online so that consumers can make an informed choice about whether to engage in a transaction online.

5. Information About the Transaction

5.1. Material information about the transaction shall be provided in the same language in which the good or service is offered. The use of automatic language programs for translation purposes should be encouraged. As set out below, merchants shall:
make available to consumers all relevant information relating to the terms and conditions, costs, shipping and charging and cancellation/return/refund policies applicable to a transaction before it is entered into;
provide consumers with an opportunity to review the transaction before it is completed and becomes a binding obligation; and
shall maintain a record of the transaction after it has been completed.

5.2. Merchants shall make available to consumers the terms and conditions applicable to the transaction. Such information should include:
any restrictions or limitations (for example, time or geographic) they impose on the commercial offer and/ or the sale of the goods or services;
easy-to-use payment mechanisms and in the case of credit or debit cards, the expected time when the card will be charged;
for goods, any warranties, guarantees, escrow programs or other offered terms, including limitations, conditions;
for services, any standards, schedules, fees, or other offered terms, including limitation and conditions; and
information about any self-regulatory programs to which the merchant adheres, and how to access those rules, and notice on the law applicable to the commercial relation.

For ongoing transactions or subscriptions:

information about how the transaction will appear on the bill so that the customer will be able determine to which transaction and which company the bill relates;
minimum duration of the contract and easy-to-understand cancellation information, an easy to use means to cancel an ongoing subscription, and timely confirmation of such cancellation.

5.3. Merchants shall disclose the entire price of the goods and services and any other charges to be collected by the merchant. Such information should be provided in a specified currency and should include:

price or license fee to be charged, including all taxes, or in the case of a barter trade, the items that will be exchanged for goods or services purchased or licensed;
shipping and handling charges.

Merchants shall honor the amount authorized by the customer in any subsequent bills to the customer.

Merchants shall disclose to consumers when they will be able to ship the goods or provide services, and the expected time when a consumer's credit card will be charged for a transaction. A consumer shall not be charged for a product or service unless shipment of such product or service is expected within a reasonable period of time. In particular, merchants should:

state which products or services are temporarily unavailable and if an expected availability date is provided, have a reasonable basis for such date;
have a reasonable basis for, and provide consumers with, estimated shipping times (or in the case of online delivery, delivery times);
have a reasonable basis for stated delivery claims when made; and
disclose any shipping, performance, or delivery limitations they impose (age, geographic).

If a material delay in shipping or performance occurs, the merchant shall provide the consumer with information about the delay and the opportunity to cancel the transaction.

5.5. Merchants shall provide consumers with an opportunity to review the transaction and to confirm their intent to enter into the transaction and shall disclose to consumers at what point the transaction will be final and become a binding obligation. Prior to a transaction becoming a binding obligation, merchants should provide consumers with a summary that includes:

the terms and conditions of the transaction;
the selected payment method; and
the option to cancel or affirmatively complete the transaction.

Merchants shall maintain, and make it possible for consumers to access, an appropriate record of information about a transaction for a reasonable period of time after it has been completed. Such information should include:

a statement of what was ordered, the price, and any other known charges such as shipping/handling and taxes;
sufficient contact information to enable purchasers to obtain order status updates; and
the anticipated date of shipment.

6. CANCELLATION/RETURN/REFUND POLICIES

6.1 Merchants shall provide information to consumers about their cancellation, return, and refund policies, including: the length of time after entering into a binding obligation which an available cancellation, return, or refund may be made; the process that should be followed; and any costs that may be incurred. If there is no cancellation, return or refund right, this should be stated.

Security

7.1 For information that is transferred from a consumer to a merchant, merchants shall take reasonable steps ensure the security of a consumer's confidential commercial and personal information. These security efforts shall be consistent with best industry practices and shall be appropriate for the type of information collected, maintained or transferred to third parties. In particular, merchants should:

have in place encryption measures that reflect best industry practices for the transfer or receipt of sensitive information, such as personal financial information or health care records;

- have in place appropriate levels of security to protect data being maintained by computers;
- take reasonable steps to require third parties involved in fulfilling a customer transaction to also maintain appropriate levels of security; and
- not retain any information from which a consumer may be identified if the consumer does not complete a transaction, without the consumer's consent.

8. Customer Service and/or Support

8.1. Merchants shall comply with all commitments, representations, and other promises made to consumers. They shall disclose to consumers information regarding customer service and/or support of the goods and services that consumers purchase online. Such information should include the length of time the customer service and/or support is available, the costs associated with obtaining the customer service and/or support, and how customers can successfully and meaningfully contact the business to get answers to their questions.

If no customer service and/or support are available from the merchant, this should be stated.

9. Warranty

Merchants shall disclose to consumers applicable warranties or limited warranties that they offer regarding the goods or services sold or made available to consumers. Such information should include the scope, duration, and means of exercising rights made available in the warranty or limited warranty.

Privacy

Merchants shall post and adhere to a privacy policy that is open, transparent, and consistent with the following personal data protection practices:

Notice /Awareness: Merchants that collect personal data shall reasonably explain what personal data they collect, use, and disclose to third parties, and for what purposes;

Choice/Consent: Merchants that collect personal data shall reasonably explain what choices they provide consumers about the collection, use and disclosure of such information. At a minimum, Merchants should provide consumers with the choice to opt out of having their personal data used or disclosed for any new purpose not explained at the time the personal data was collected and should obtain the consumer's unambiguous consent to the collection or use of sensitive personal information, such as medical records.

Accuracy: Merchants that collect personal data shall reasonably explain the methods by which the consumer can correct or update personal data and shall adopt procedures to respond to reasonable consumers' requests for such corrections or updates.

Integrity/Security: Merchants that collect personal data shall reasonably explain the steps taken to protect the quality and integrity of the personal data collected as well as the confidentiality of that personal data from unauthorized access.

Redress/Internal Rules : Merchants shall reasonably explain the means of communicating with the merchant's contact point to which the consumer can direct questions, express preferences concerning the handling of personal data or lodge complaints. Merchants shall establish and maintain a system to implement the provisions of these guidelines within the company.

10.2. When transferring personal data to a third party for processing on its behalf, a merchant should ascertain the adequacy of the personal data practices of the third party.

11. Unsolicited E-mail

11.1. Merchants shall accurately describe their business practices with regard to their use of unsolicited e-mail to consumers.

11.2. Merchants that engage in unsolicited email marketing should adhere to a policy that, at a minimum, enables those consumers who do not wish to be contacted online to "opt out" online from future solicitations. This policy should be available both on the web site and in any e-mails, other than those relating to a particular order.

11.3. Merchants that engage in unsolicited e-mail marketing should also subscribe to a bona-fide e-mail suppression list.

12. *Dispute Resolution*

12.1. Merchants shall provide consumers with fair, timely, and affordable means to settle disputes and obtain redress.

12.2. Merchants should provide an easy-to-find and understandable notice on how a consumer can successfully and meaningfully contact the merchant to solve problems related to a transaction. They should have effective “customer satisfaction systems”, encourage consumers to take advantage of such internal mechanisms and make a good faith effort to resolve any disputes relating to a transaction in a fair and equitable manner, for example, by providing money-back satisfaction guarantees or exchange policies. Complaints should be directed in the first instance to the merchant.

12.3. Unless full customer satisfaction is guaranteed by an internal customer satisfaction system, merchants should notify consumers that they are ready to submit disputes resulting from a transaction to one or more specified ADR systems. Information about the ADR offered should be provided as a part of the notice on how consumers can contact the merchant to resolve problems related to a transaction and access to an ADR system normally should be available only after a consumer has sought redress through a merchant's internal complaints mechanism.

12.4. Such ADR systems would not affect the consumer's right to seek remedies through the court system. However, the consumer and the merchant could agree that prior to proceeding in the court of any local jurisdiction, the consumer would submit a claim to an ADR system. ADR systems should function according to published rules of procedure that describe unambiguously all relevant elements necessary to enable consumers seeking redress to take fully informed decisions on whether they wish to use the ADR offered or to address themselves to a court of law.

12.5. ADR systems should provide for impartial, accessible, transparent, and timely conciliation/negotiation, mediation and/or arbitration at no or only moderate cost for the consumer.

12.6. Consumers should be informed about the conditions of access (online or other), the cost, the legal nature of the ADR (arbitration, mediation, conciliation/negotiation, etc.) and of its outcome (binding/not binding/binding for the merchant; enforceable), and recourse to other instances, notably to law courts.

GBDE RECOMMENDATIONS TO GOVERNMENTS

BACKGROUND

Trustmark programs are initiatives developed privately by consumer organizations, major accountancy organizations, professional organizations such as Chambers of Commerce and companies. All of them have emerged to respond to consumers' concerns on trust and confidence on electronic commerce in different areas such as privacy, childrens' advertising, security, product delivery, etc.

Some governments are tempted to regulate this new way of providing consumer trust for fear that consumers will be confused by different programs offering different levels of protection. To avoid possible confusion, the GBDe has developed these guidelines to help ensure greater transparency, minimum voluntary standards and comparable levels of protection for consumers among competing trustmark programs.

RECOMMENDATIONS

1. Further trustmark development by market participants and promotion by stakeholders

- 1.1 At present, only a few trustmarks programs are being used and are widely known. It is essential that trustmark programs are further developed and broadly disseminated to enhance global consumer trust in e-commerce.
- 1.2 Governments should play an active in promoting and disseminating trustmarks programs.

2. Government intervention is premature





- 2.1 For trustmarks to enhance consumer trust, they should remain a private-based initiative.
- 2.2 Harmonization of trustmarks by means of government recommendations or compulsory government accreditation is a disincentive for innovation and competition to the detriment of consumer confidence and choice.
- 2.3 The existence of different levels of trust (e.g. by sector/issue specific programs) or regional/local initiatives should be acknowledged and encouraged.

3. Active stakeholders dialogue




All stakeholders should seek to co-ordinate actions in order to contribute to trustmarks development and encourage competitiveness between programs.

ANNEX 1





Global Trustmark Programs

					
		AOL CERTIFIED MERCHANT PROGRAM http://shopping.aol.com/custserv/merchants.adp#standards	BBBONLINE PRIVACY www.bbbonline.org	BBBONLINE RELIABILITY www.bbbonline.org	BETTERWEB www.pwcbetterweb.com
description		AOL Service AOL Merchant Criteria cover fulfillment, privacy and security. 310 users	US initiative managed by BBBOnline, (private non-profit organisations) Code of conduct covers mainly privacy, but also children's privacy, security & ADR. Over 150 users (almost exclusively in the US, e.g. MCI, HP).	Managed by BBBOnline. Based on compliance with BBB standards on honest advertising, customers fair treatment, & participation in BBB ADR program. Over 4,500 users (almost exclusively in US & Canada).	Global Program from PwC Covers Sales Terms, Privacy, Security and Customer Complaints. 100 applicants (retail, financial services & other services)
Main elements	Fee	Rates are negotiated	\$225 to \$3075 – depends on size of company.	\$400–\$5000 depends on size of company	Annual license fee of \$15,000 US
	Redress & enforcement	Customer contacts first merchant. If no solution, customer can go directly to AOL. If a merchant does not comply with its posted return policy, AOL will provide customer with refund for full purchase price.	Consumer can complain directly to the BBB, if this fails, use of ADR. If business does not participate in the ADR, fails to comply with ADR resolution, seal can be withdrawn publicly. Possible referral to authorities.	Merchant must have satisfactory complaint handling record; agree to BBB's advertising program; agree to respond promptly to consumer complaints, and agree to ADR at consumers' request. Plus enforcement as BBB Privacy.	Seal may be revoked by PwC at any time if concerns arise related to Participant's compliance with Program and/or business practices disclosed. Upon annual renewal, PwC performs comparison of Web site's published policies to the BetterWeb Standards

Consumer input	AOL pays close attention to customer feedback in determining whether merchants are fulfilling their certified merchants obligations.	No official consumer input.	No official consumer input.	No official consumer input.
Security	The transactions of certified merchants are secured via a secure commerce server & encryption technology.	Code has security provisions		Integrated set of security disclosure requirements covering site certificate information, user identification, protection of information being transmitted & protection of stored information, through use of accepted protocols.
Issues covered	AOL Merchant criteria cover privacy, fulfillment & security. All certified merchants must post a privacy policy consistent with Merchant Criteria.	Code mainly focus on privacy which is largely based on the OECD principles.	Code Coverage includes advertising/marketing, contract fulfillment and sales to children.	Standards focus Sales Terms, Privacy, Security and Customer Complaints. Consultants may visit & confirm existence of applicant.






					
		casetrust www.casetrust.com.sg	Clicksure www.clicksure.com	Cpa webtrust www.cpawebtrust.org	Labelsite www.labelsite.org
description		Joint project of Consumers Association of Singapore (CASE), CommerceNet Singapore (CNSG) and Retail Promotion Centre (RPC) Code of conduct covers privacy, fair business practices etc.	UK initiative with international outreach managed by a private company (on the basis of venture capital). • Business practices cover privacy, security & transaction. Independent audit random checks on compliance 100 users	US-origin initiative expanding in Europe and managed by public accountants. Code of conduct covers various issues (transaction, privacy). Independent audit report conducted before seal granted Expect 100-200 users in Europe. Used by Bell Canada	French initiative managed by two business associations (retailers & distance sellers). Code of conduct covers transaction, privacy, marketing. An independent audit report is conducted before the seal is granted No users yet
Main elements	& Fee	Varies from \$ 300 to \$ 1500 p.a. depending on n° outlets.	250-500 Euros certification fee + 960-1920 Euros p.a.	1400 Euros p.a.	250 Euros p.a.
	Redress enforcement	Only enforcement is withdrawal of the mark.	Use of standard is overseen by an independent advisory board. Users to have an internal complaint mechanism & accept arbitration.	Every 3 months there is a re-certification to verify that the site continues to meet standards	Multidisciplinary Certification Committee. Requires that company develops internal complaint-handling mechanisms.
	Consumer input	Consumers association involved	No consumer input but independent advisory board composed by prominent e-commerce experts.	No consumer input.	The Certification Committee is only made of business.
	Security	Minimum standard set by Casetrust.	Clicksure audits its practices against British Standard on Information Security Management.	The transactions are secured by Verisign technology.	The seal will be secured but there are no security provisions in the code.

	issues covered	Governed by Singapore Law	The standard focus on a broad range of issues (quality, privacy, transaction management, information on trading status).	Criteria focus on: business & information practices; transaction integrity & information protection.	Reference in the certification requirements to the need to comply with French law.
--	----------------	---------------------------	--------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------

				
	ONLINE SHOPPING TRUST JAPAN DMA & CHAMBER OF COMMERCE www.jadma.org http://mark.cin.or.jp	Safemall www.trust.kait.kr	SELLO DE GARANTÍA - GUARANTEE SEAL www.aece.org/corporativo/sello.htm	SquareTrade Seal Membership www.squaretrade.com
DESCRIPTION	Japanese initiative by direct marketing industry association & largest retailers association Code of conduct covers , Fair Business Practices.) 300 (JADMA) and 1,600,000 (JCCI) members	The seal is granted by the Korea Association of Information & Telecommunication.	Spanish initiative managed by a Electronic Commerce Business Association. Code of conduct covers privacy (with provisions on children, spamming & cookies) 120 users (e.g. BBVA & Telefónica)	Global initiative; private venture-backed company. Membership granted to online sellers screened by identity verification, reference checks and pledge to use SquareTrade's Online Dispute Resolution \$500 fraud protection guarantee for purchases from Seal Members.
Main elements	From ¥15,000 p.a. to ¥60,000, depends on business size. Application fee ¥10,000	Certification process costs \$500.	100 Euros p.a.	Scaled annual fee based on revenues. Ranges from \$100 US for <\$50,000 to \$6400 for >\$1 Billion.
Fee				

Redress & enforcement	Withdrawal of mark or indication of unlawful use of the mark.	Company contracts to affirm commitment to the Code. The seal programme reserves the right to withdraw the logo upon investigation of a compliant.	A Compliance Committee is in charge of controlling use of seal & adherence to Code & impose sanctions (e.g. withdrawal of seal, publicity of sanction)	Instant Seal removal technology for non-participating Seal Members, fraud protection guarantee and Website seller “watchlist” protect consumers. SquareTrade collaborates with partner marketplaces for enforcement. SquareTrade compliance audits can lead to Seal revocation.
Consumer input	No official consumer input.	The Code was reviewed by consumer organizations.	Code of Conduct developed with consumer assoc. & Compliance Committee made of business & consumers	Feedback from consumer organizations, FTC and Department of Commerce. Consumers filing cases against Seal Members know Members have pledged to respond.
Security	There are 2 options regarding security features: (1)Clicking on the approval mark displays the approval information issued by the approval server; and (2) Anti-copying mechanism using electronic watermark. Security in communication is left to users.	There are no specific undertaking mentioned on the site for confidentiality of customer and data transaction.	No sound security provisions (companies with no secure server must warn the customer) or measures.	All Seal Members are verified. Digital watermark on Seal eliminates fraudulent use. All sensitive data is protected during communication and in storage by a public key infrastructure and JCE using PKCS #5 standard.

	Issues covered	The organization actually visits and confirms the existence of the retailer	The code contains various privacy-related & consumer protection rules.	Sound Code but exclusively focused on privacy. Requires the establishment of a privacy policy (helps companies to develop one)	Based on international standards for good selling & customer service. Seal Members commit to ADR participation up front.
--	----------------	-----------------------------------------------------------------------------	------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------

						
	Truste www.truste.org	Trusted Shops www.trustedshops.de	TrustUK www.trustuk.org.uk	WEBASSURED www.webassured.com	WEBTRADER www.dedigitaleconsument.nl	
<i>DESCRIPTION</i>	US initiative Covers only privacy 1500 licensees (e.g. Disney)	German initiative, subsidiary of Gerling Insurance group. It will be expanded to France, UK & Benelux by mid-2000 Guarantees online consumers a money back guarantee 18 users (e.g. BOL), since 18/01/00	UK initiative, supported by government, & managed by an e-commerce business alliance & consumer body. Grants the seal to associations that abide to certain “accreditation criteria” (transaction, privacy, marketing provisions).	Global initiative founded in 1995 Members agree to a Universal Standard of Ethics, and to be bound by on-line ADR process Affiliated with Dun & Bradstreet and Lloyds 4,000 current licensees, approx. 500,000 applications in process	Dutch initiative managed by consumer body. Code of conduct covers transaction, privacy, marketing. Forms part of a developing network of consumer-based trustmarks in other EU countries 50 users	
Main elements	<i>Fee</i>	Annual licence fee depends on company’s revenue (\$0-\$1M=\$299).	Depend on turnover & volume. Min. Euro 2550	6.400 Euros p.a. (per assoc)	\$180 per year minimum, increases with sales volume	The service is free.
	<i>Redress & enforcement</i>	Trustmark may be revoked, contract terminated, or referral to governmental agencies. Merchants must have internal complaint system. Consumer may contact TRUSTe, but no other formal procedure is set forth.	Companies must have an internal complaints system. If company does not deliver the product in time (30 days), Trusted Shops gives the money back.	Enforcement is done by the assoc that is accredited by TrustUK. Only enforcement by TrustUK is withdrawal of seal.	Due diligence performed by internal staff, by D&B, and the collective Internet community through ongoing feedback on business practices (i.e. complaints/ praise, etc...)	Webtrader can withdraw the logo upon investigation of a complaint. The Code has stringent dispute resolution provisions.

Consumer input	No official consumer participation. TRUSTe relies on users to report violations of posted privacy policies, misuse of trustmark, etc.	Feedback from consumer assoc. & follows Consumer Assoc. E-Com Code of Conduct	Joint venture between e-commerce business alliance & main consumer association.	Universal Standard of Ethics has evolved from 5 years of actual public use and continuous feedback	The Code was written and is implemented by consumer organizations. No input from business
Security	Use of accepted protocols, such as encryption, is necessary if the licensee collects, uses, sensitive information, such as credit card or social security numbers, over Internet.	Oblige to use encrypted technology & secure servers. Transfer of payment info should be encrypted & should tell consumer type of encryption & degree of safety.	Security is left to users with a recommendation to use a British Standard, have a security officer & authenticate transactions.	Licensees must employ industry standard security protocols and disclose the procedures being utilised	Confidentiality guaranteed. No clear security provisions or measures.
Issues covered	Principles focus on privacy: notice & disclosure, choice & consent, data security, quality & access. Users must post a privacy policy.	Code covers privacy, transparency, transaction information. All transaction details of customer are transmitted to Trusted Shops.	The accreditation criteria has sound provisions on on-line advertising, transactions, fulfillment, privacy, security & children.	Seal is backed by Lloyd's guarantee on all purchases from a WebAssured licensee. If a buyer relies on seal & gets burned, WebAssured will refund losses.	The Code includes detailed privacy requirements.

