

**Self-Regulatory Approaches
to Cross-Border Transfers
of Personal Data:
The APEC Experience**

The Privacy Symposium

August 2007

Fran Maier

Executive Director, TRUSTe

Self-Regulatory Approaches to Cross-Border Transfers of Personal Data: The APEC Experience



The Privacy Symposium
August 2007
Fran Maier
Executive Director, TRUSTe



About TRUSTe

- Independent, non-profit headquartered in San Francisco
 - Washington, DC gov't affairs office
- Web Privacy Seal Program
 - Anti-spam and email standards
 - Trusted Download Program for legitimate (spyware-free) downloads
- Celebrating 10 Year Anniversary

1997



2007



Mission

Advancing Privacy and Trust for the Networked World

- Widely accepted privacy best practices
- Elevate responsible players
- Help consumers identify who they can trust
- Supplement legislation and regulation
- Address emerging privacy vulnerabilities and threats

TRUSTe: 10 Years of Impact

- **Web Privacy Seal**
 - 2,400 Websites
 - 1,500 companies
 - 22 of Top 50 most visited websites
 - 1 Million “click-to-verify” pageviews monthly
 - Thousands of consumer complaints resolved annually
- **EU Safe Harbor Seal** by authority of the US Department of Commerce
- **Children’s Online Privacy Protection Act Safe Harbor** by authority of the US Federal Trade Association
- **Email Privacy Seal** beyond legal requirements for legitimate mail
- **Trusted Download Program** (beta)
 - Certifying consumer downloadable software (not Spyware)



Our Sealholders

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.



H&R BLOCK®



Today

- Certification Process
 - Complete, Rigorous, Beyond simple Self-Assessment
- Compliance and Enforcement Toolbox
 - Aimed at improvement
 - Thorough, Regular, and Action-Oriented
 - Dispute Resolution, Monitoring, and Enforcement
- Building toward Common Criteria

Today's Agenda

- Part One: APEC Cross-Border Privacy Rules and Trustmarks
- Part Two: Model Trustmark Elements: the TRUSTe Experience

Part One

APEC: Cross-Border Privacy Rules

APEC: Cross-Border Privacy Rules

- 1999: Electronic Commerce Steering Group (ECSG) established
 - Purpose: coordinate e-commerce activities in APEC
 - Structure: works through subgroups
- 2000-2001: ECSG surveys of APEC economies
 - approaches to consumer protection
 - legal recognition of electronic documents and signatures
- 2002: Data Privacy Subgroup established
 - Purpose: develop APEC-wide privacy framework
- 2004: APEC Member Economies endorse *Privacy Framework*
 - 9 Guiding Principles
 - Goal: maximize privacy protection *and* continuity of cross-border data flows

APEC: Cross-Border Privacy Rules

- Privacy Framework Principles
 - Preventing Harm
 - Notice
 - Collection Limitations
 - Uses of Personal Information
 - Choice
 - Integrity of Personal Information
 - Security Safeguards
 - Access and Correction
 - Accountability

APEC: Cross-Border Privacy Rules

- Privacy Framework Implementation Guidance
 - Support development and recognition of organizations' cross-border privacy rules that adhere to APEC Privacy Principles
 - Work with stakeholders to develop mechanisms for the mutual recognition or acceptance of cross-border privacy rules between and among economies
 - Ensure that rules and recognition mechanisms facilitate accountable cross-border data transfers and privacy protections, without unnecessary burdens on data flows, businesses, or consumers

APEC: Cross-Border Privacy Rules

- 2005: Cross-Border Privacy Rules Study Group established
 - Purpose: examine implementation options
 - Activities: Technical Assistance Seminars on International and Domestic Implementation of Privacy Framework held in Korea and China, respectively
- 2006-Present
 - “*Four Step Approach to Cross Border Privacy Rules*” questionnaire distributed to economies
 - Asks how each economy would implement Privacy Framework for cross-border context, including recognition of Trustmark organizations
 - Second Technical Assistance Seminar on International Implementation held in Australia, June 2007 showcases the role of Trustmarks as “accountability agents”
 - 12 economies agree to participate in ‘Data Privacy Pathfinder’ pilot project in 2008, to implement voluntary cross-border privacy rules system within APEC

TRUSTe Collaboration with Trustmarks in APEC

- Member of Asia Trustmark Alliance (ATA) Task Force
- Project: Common Criteria for Cross-Recognition of Trustmarks under APEC Privacy Framework
 - Standards for Comparing Trustmarks
 - Standards for Certification of Merchants by Trustmarks
 - Essential for implementation of cross-border privacy rules
- First draft presented at May 2007 Trustmark Conference, Mexico City
- Now under consideration by ATA membership
- Paradigm for accountability agent structure in APEC

Example Principle and Criteria

4 Privacy

4.9. Accountability

A personal information controller should be accountable for complying with measures that give effect to the Principles stated above. When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles.

4.9.1 Accountability of merchant: How does certifier require that merchant be accountable for complying with these measures?

___ Certifier requires that merchant establish and maintain a system to implement the provisions of its website privacy statement and practices.

___ Certifier requires that merchant assign individual(s) to be responsible for the accuracy of website privacy statement and for receiving and processing user questions or complaints.

___ Certifier requires that merchant periodically or regularly undertake an audit of its privacy policy compliance, either through self-assessment or by a third party.

___ Other (please specify): _____

Part Two

Model Trustmark Elements: The TRUSTe Experience

TRUSTe Certification Process

1. Web Site Privacy Assessment

- Application/Contract
- Self-Assessment

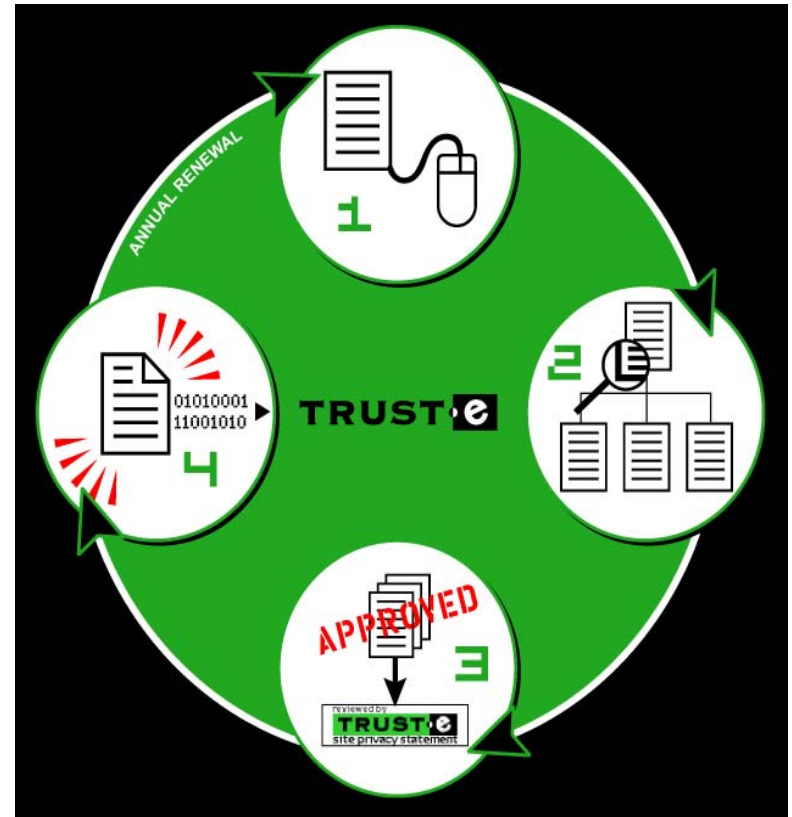
2. Web Site Audit

- TRUSTe expert
- Access Reputation and other Data
- Revision of policy and practice

3. Seals Awarded and Displayed

4. Ongoing Monitoring & Dispute Resolution

- Watchdog Dispute Resolution
- Scanning/Seeding



TRUSTe Certification Process: Improve Licensee Practices

CERTIFICATION CENTER

Welcome, Darth!
[Logout](#)

Sales Representative:
Heather Dorso
415-520-3405
hdorso@truste.org

User Profile:
Darth
The Empire
[Update User Account](#)

User Administration:
[Manage Other Users](#)

What's Next?

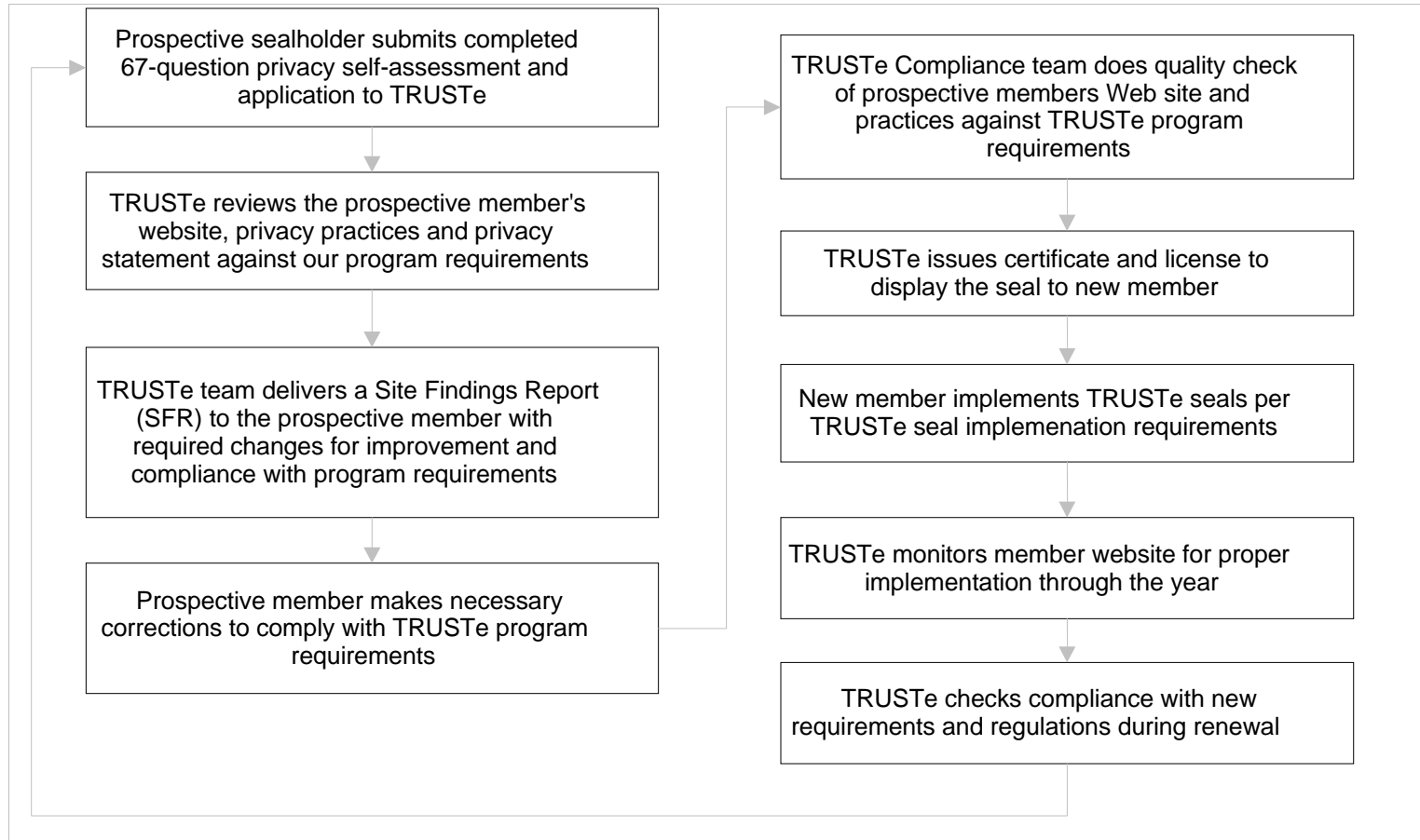
[Work on Your Self Assessment](#)
or
[Invite Other Users](#)
([Learn More](#))
[Self Assessment Glossary](#)

1	Create Profile	Completed	Review
2	Sign License Agreement	Completed	Review
3	Submit Payment	Completed	Review
4	Submit Self-Assessment	Not Started	Begin
<p>The self-assessment must be signed by an authorized representative. If you are not the authorized representative please invite the appropriate person to participate</p> <ul style="list-style-type: none"> → Invite another participant to complete the Self-Assessment → Continue Self-Assessment In Progress → Review Self-Assessment Instructions → Submit Authorized Signature Not Started 			
5	Submit Privacy Statement	Completed	Review
6	Submit Application	Not Started	Begin

- Over 90% required to make changes to business practices
 - Notice at Point of Collection
 - Privacy Policy disclosures esp. cookies and third-party sharing
 - HTTPS for sensitive data (e.g. credit card)

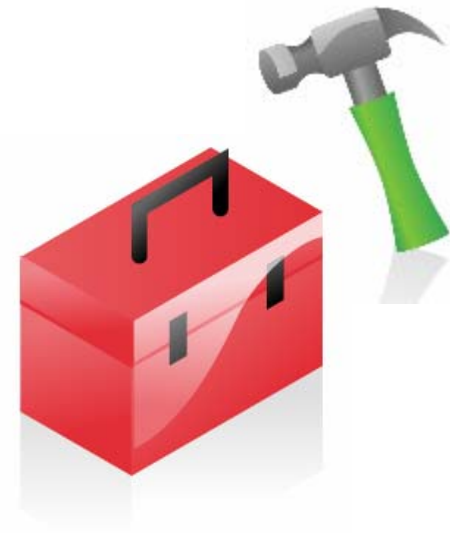
✉ [Click here](#) to have a TRUSTe representative contact you.

TRUSTe Privacy Seal Certification



Compliance and Enforcement Toolbox

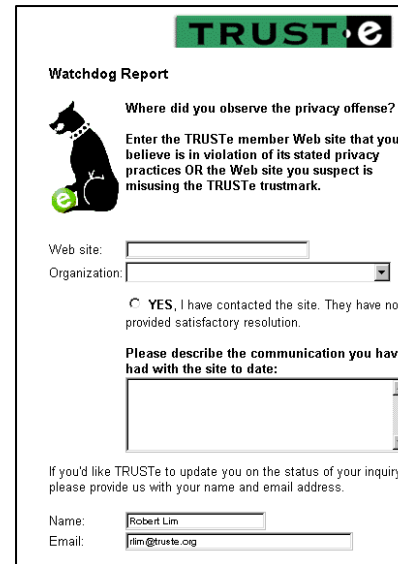
- Certification:
 - 90% improve practices
- Watchdog Dispute Resolution
 - 100% resolution
 - Small # of terminations
- Proactively monitor
 - Scanning: 50% fail and then fix
 - Email Seeding
- Enforcement Options
 - Non Renew
 - Suspend
 - Terminate



Watchdog Online Dispute Resolution


- Online independent recourse mechanism for consumers to report
- Goal is to augment Sealholder's privacy program, escalate and resolve complaints quickly
- 86% would recommend using Watchdog to a friend

"I loved Adobe beforehand and I love it now. TRUSTe facilitated getting me to the right person to talk to."



TRUSTe

Watchdog Report

 **Where did you observe the privacy offense?**

Enter the TRUSTe member Web site that you believe is in violation of its stated privacy practices OR the Web site you suspect is misusing the TRUSTe trustmark.

Web site:

Organization:

YES, I have contacted the site. They have not provided satisfactory resolution.

Please describe the communication you have had with the site to date:

If you'd like TRUSTe to update you on the status of your inquiry, please provide us with your name and email address.

Name:

Email:



[Logout: chodge](#)

Date: 2002-11-07 01:42:02

User name: wendy myers

User email:

Release info: Yes

Contact OK: Yes

Seeking: <http://www.freechinaspages.com/grant/shellyme/index.asp?cvn=> Full website address. I have returned emails asking them not to email my in future but all these are returned as undeliverable. Rayetadn@eszett.de Miriamin@surfnet.net.il Just two of many email addresses from where this same cash grant offer is received. [View history](#)

[Return to complaint list](#)



TRUSTe Watchdog Complaints

- Resolve 5000+ per year directly
 - Also offer “self help” through web site
- TRUSTe works with consumer and the sealholder to resolve issues
- Critical input to monitoring process
- Goal: Improve Consumer

Note: for all TRUSTe Watchdog Complaints

TRUSTe Watchdog Report

April 2007

Watchdog Privacy Complaints:
103

Number of Trademark Violation
Reports: 384

Unable to unsubscribe:

█ 16%

Shared personal info.:

█ 19%

Unable to close account:

█ 20%

Email sent without permission:

█ 18%

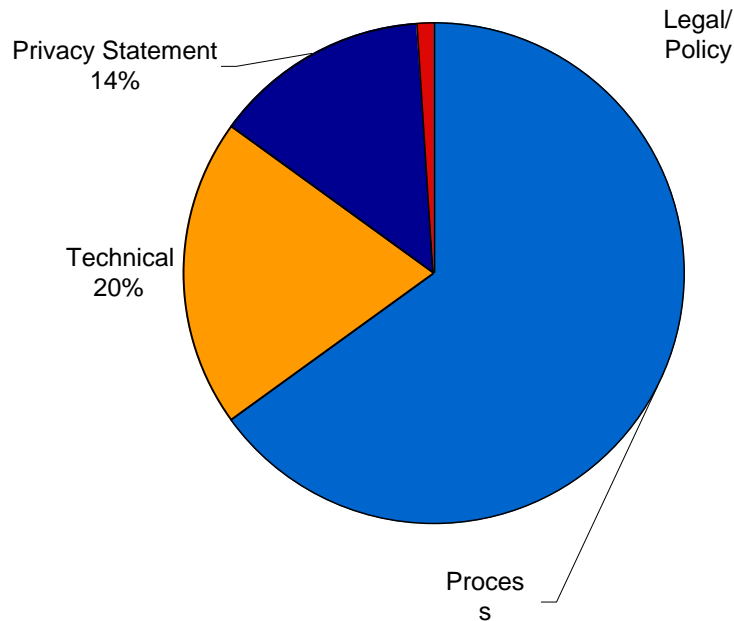
Unauthorized profile with my
information:

█ 20%

Unable to contact licensee:

█ 7%

Types of Investigations: Primarily Customer Care



- **Process (65%):**
 - Unsubscribe me
 - Close account
 - Can't reach licensee
- **Technical (20%):**
 - Interface disclosures
 - TRUSTe seeding of client lists to check unsub link, unauthorized third-party mail
- **Privacy Statement Analysis (14%):**
 - Notice about data sharing, cookies etc.
- **Legal/Policy Analysis:**
 - Legal status of unusual business models or practices
 - Potentially deceptive notice

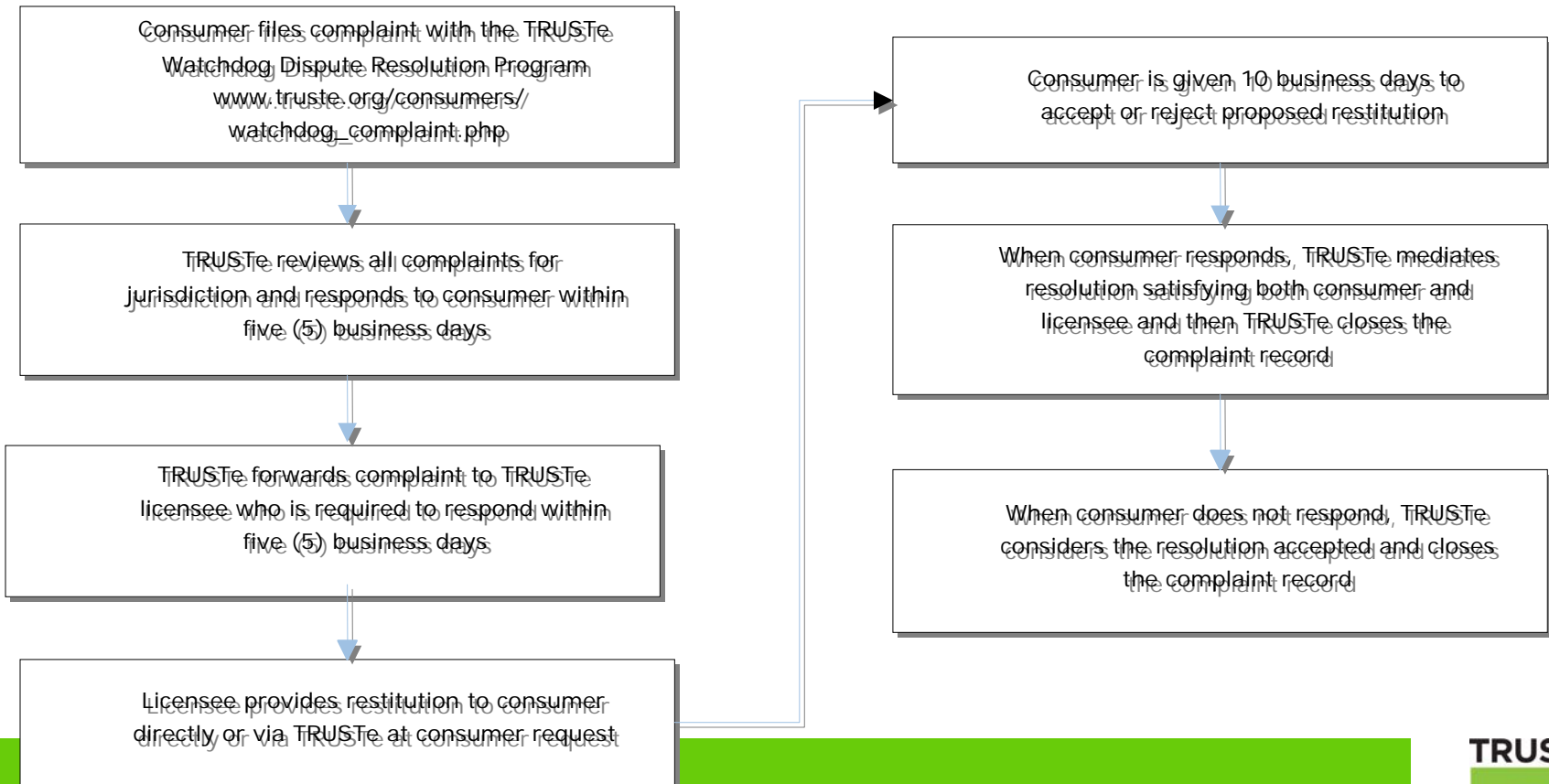
Severity Scorecard: Early Warning System

- Used to analyze Watchdog complaints by company and provide early warning
- Weighting helps assess:
 - severity of complaint(s)
 - trends in complaint type
 - Trends in complaint volume
- Color/letter process map reflect: type of follow-up and sealholder changes required:
 - type of investigation
 - privacy policy change
 - notice at opt-in
 - type of information collected
 - data spill assistance to Licensee
 - level of escalation within TRUSTe

TRUSTe Watchdog Diagnosis (Complaints per Month)	Increasing Offenses			weight ed score
	1	2	3+	
Unable to unsubscribe	D	E	G	
Unauthorized profile with my information	D	E	G	
Unwanted email	D	E	G	
Excessive email	D	E	G	
Email sent without permission	D	E	G	
Unable to close account	D	E	G	
Unable to change/delete personal information	D	E	G	
Shared personal information	A	B	C	
Violated privacy policy	A	B	C	
Unable to contact licensee	A	B	C	
Children's information (under 13)	A	B	C	
Inconsistent Unsubscribe Instructions	A	B	C	
Inaccurate Disclosure: POC	A	B	C	
Inaccurate Disclosure: PS	A	B	C	

Steps to Resolve a Watchdog Complaint

- Working with Consumer and Sealholder to reach satisfactory resolution




Ongoing Monitoring

Evaluate websites from many angles: proactive and reactive approach

- Technological scans
- Email “seeding”
- Reputation monitoring
- Ongoing reviews
- Watchdog monitoring
- Other reviews of blogs, press, consumer postings

- Approximately 50% of scans discover problems

MAXAMINE™
TRUSTe Scorecard Report
Scan Date: August 23, 2006

TRUSTe Compliance
TRUSTe Scorecard 81.0%
Measures TRUSTe requirements of the site. 
[Show Scorecard](#) [Legend](#)
[Expand All](#)

Report Date: August 23, 2006
Site: www. .com
File: /user/mx-www. .com/www. .com_2006-08-23_2133.max

Checkpoint	Description	Compliance
1	Is the TRUSTe trustmark ("TM"/"finalmark.gif") on the licensee's home page?	Yes
1a	Does TRUSTe TM link to the privacy statement?	Yes
2	What pages of the Web site contain the TM logo?	1 Page
2a	Does TRUSTe TM link to the privacy statement wherever it is present?	Yes
3	Is the name of the TM logo "finalmark.gif"?	Yes
4	Is the privacy statement present?	Yes
4a	Is a link to the privacy statement on the licensee's home page?	Yes



Enforcement Options

- **Suspend Certification**
 - Notified on Verification Page
 - Seal still on Website
 - Timeframe for Resolution
- **Terminate**
 - Termination for Convenience (non-public) - other issues not directly related to contract and/or reputation issues
 - Terminate and Rehabilitate – Batteries.com
 - Termination for Cause (Publish on website) – Gratis/FreeIPods.com
 - Terminate and refer case to law enforcement/regulators – ToySmart.com
- Process must be **Transparent, Consistent, Fair**, and Lead to Positive Consumer Outcomes
 - Usually result in company coming back into compliance

Independent Non-Profit Status Important

Termination Case Study Gratis Internet

Timeline

9.14.2004: Gratis Internet, freeipods.com certified by TRUSTe

10.4.2004: TRUSTe investigates complaints about freeipods sharing email addresses with 3rd parties

1.14.2005: TRUSTe issues (private) Notice of Termination unless Gratis remedies all violations within 20 days

1.14.2005: Seals are deactivated and Gratis removes TRUSTe seals from Website,

2.9.2005: TRUSTe issues (public) Notice of Termination

3/14/2006: New York Attorney General sues Gratis for breach of privacy policy after lengthy investigation

- Gratis Internet violated its stated policy to not sell or rent personal information to third parties
- TRUSTe investigated Watchdog reports of sharing by seeding email accounts
- TRUSTe required Gratis to change privacy practices
- Gratis complied but could not offer any remedy for consumer complaints, and refused privacy training
- TRUSTe publicly terminated Gratis Internet gaining the attention of the NY Attorney General
- Gratis was sued by the Attorney general for violating its privacy policy

Enforcement Action Case Study:

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

Timeline

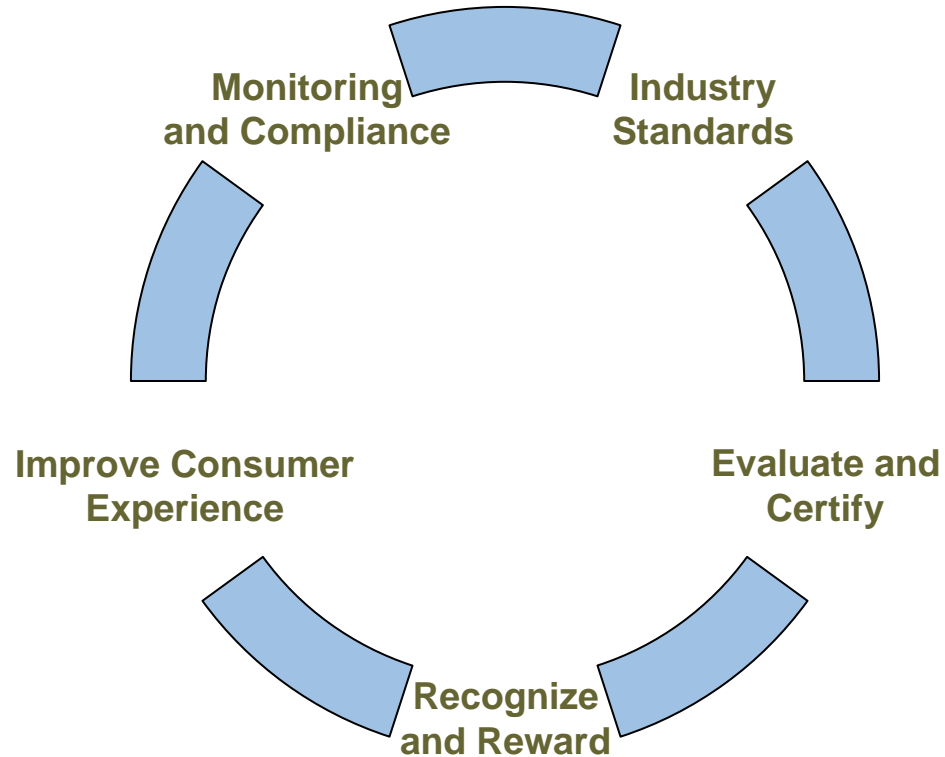
- 4.24.2002: Batteries.com signs license agreement 7.0
- 4.4.2003: Sungifts.com sends out email promotion offering free subscription to *Men's Journal*
- 5.28.2003: CNet writer Berlind exposes breach of privacy policy in *ZDNet*.
- 6.13.2003: TRUSTe issues Notice of Termination unless Batteries.com remedies all violations.

- Batteries.com violated privacy policy when it changed it shared PII with a 3rd Party without gaining prior consent
- TRUSTe responded immediately and took swift corrective/enforcement action including notice of termination
- Fortunately Batteries.com agreed to the remedial steps
 - Apology sent to affected customers
 - In-house audit of privacy practices by TRUSTe
 - On-site privacy training
- Benefit to licensee and consumer by improving privacy practices and avoiding future breaches

Building Blocks for Effective Programs

1. **Strong Program/Certification Requirements**
2. **Thorough and impartial audit**, more than self assessment
3. **Accountability and Enforcement**
4. **Credible oversight** from multiple parties
5. **Evolving** standards and accountability, ability to address new issues

Mutually Reinforcing Activities



Contact Information

Fran Maier
Executive Director & President

TRUSTe
685 Market Street, Suite 270
San Francisco, CA 94105

+1.415.520.3418

fran@truste.org

www.truste.org