2011 Email Evolution Conference

The Secrets To Winning the Trust of your users and their inbox

#eec11

eec DMA Direct Marketing Association

Agenda

- Introductions
- Changing interactive Marketing Landscape
- The fundamentals of Compliance
- Lunch with the Experts
- Protecting Integrity of email & Maximizing Deliverability
- Being Prepared – Data Governance & Stewardship
- Review – Q&A

Speakers

- Robert Consoli
  - Silverpop Systems Inc.

    (Director, Deliverability and Provisioning Services)

- 10 years of experience focused in Deliverability

- Email Blogger: http://www.silverpop.com

- Member of:
  - Email Roundtable
  - Certified Senders Alliance
  - APWG

2011 Email Evolution Conference

Speakers

- Dennis Dayman, CIPP
  - Eloqua
    (Chief Security and Privacy Officer)

- Seventeen (17) Years in Email
  - AT&T (Director of Policy and Legal External Affairs)
  - MAPS - Mail Abuse Prevention Systems (Sr. Consultant)
  - Verizon Online (Security and Legal Compliance)
  - StrongMail (Director of Deliverability, Privacy, and Standards)
  - Advisor/Investor to corporate and coalition boards
    - MAAWG, CAUCE, IAPP, Tech Wildcatters
  - Co-chair EEC Deliverability Round Table

- Twitter: ddayman
- Blogs:
  - http://www.deliverability.com
  - http://blog.eloqua.com/
- Columnist: http://www.clickz.com

Speakers

- Michelle Pelletier
  - Return Path, Inc.

  (Senior Director, Professional Services)

- A dozen years in email/CRM
- 4 years specializing in deliverability
- Manages team of email consultants specializing in optimizing all aspects of email lifecycle
- 2nd year co-chair EEC Deliverability Round Table

2011 Email Evolution Conference

Speakers

- Craig Spiezle
  - Online Trust Alliance
    (Executive Director & President)

- Mission: To develop and advocate best practices and public policy which mitigate emerging privacy, identity and security threats to online services, brands, government, organizations and consumers

- Board Member Identity Theft Council
- Member White House Identity Task Force
- Member of IAPP, APWG & InfraGard

Little Known Fact ......

- City Utility Commissioner
- Past member of Ski Patrol, Instructor & College Ski Coach Avid Photographer

2011 Email Evolution Conference

Speakers

- Matthew Vernhout
  - Transcontinental Interactive
    (Director, Delivery and ISP Relations)

- Director at large CAUCE
- CIPP/C
- Email Blogger: http://emailkarma.net
- Moderator at Email Roundtable
- Administrator at Email Marketer's Club

2011 Email Evolution Conference

Lunch Topics

- Email Authentication
- Deliverability
- North American Anti-Spam Legislation
    - CASL, CAN-SPAM
- Regulatory landscape
    - Privacy, Security & Data Governance
- Cloud, Social & Mobile

Changing Marketing Landscape

Individualism & Innovation
vs the Common Good

Craig Spiezle
Executive Director & President
Online Trust Alliance

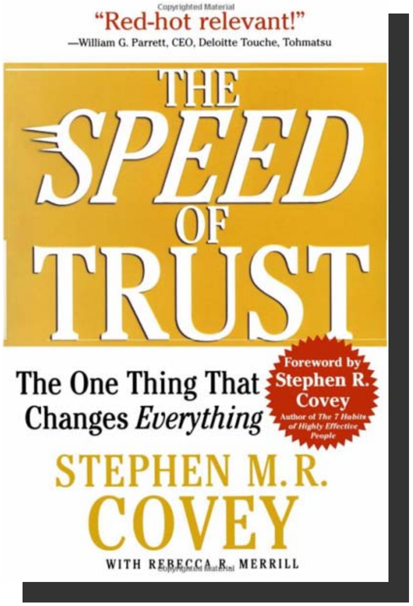
Self-Interests vs Collective Good

- Law of unintended consequences
  - Unanticipated & unintended effects
  - Ignorance, error, immediate self-interests
  - self defeating prophecy
- Interests of individuals vs the community
  - Unknown accountability vs stewardship
  - Unfortunately self-interest trumps collective good, requiring oversight
- “Me mind set to we mindset”
- Risk a tragedy of the trust commons

2011 Email Evolution Conference

“The ability to establish, grow and restore trust with all stakeholders - is the key leadership competency of the new global economy.”

– Steven Covey, *The Speed of Trust*


Copyrighted Material
“Red-hot relevant!”
—William G. Parrett, CEO, Deloitte Touche, Tohmatsu
THE SPEED OF TRUST
The One Thing That Changes Everything
Foreword by Stephen R. Covey
Author of The 7 Habits of Highly Effective People
STEPHEN M.R. COVEY
WITH REBECCA R. MERRILL

2011 Email Evolution Conference

Keys to the Internet's Vitality

- Consumer Control & Choice
- Collaboration
- Willingness to change
- Accountability
- Trust

2011 Email Evolution Conference

2011 Marketing Changes

- Redefinition of PII
- Tracking = Collection, Usage & Sharing
- On-line & Off Line; multi channel
- Beyond the PC; multiple devices
- Location bases services
- Browser enabling controls
- Patience for self-serving self-regulation days may be limited
- Evolve or become extinct

2011 Email Evolution Conference

Legislative Update

- Beyond Can-Spam
- Data governance
- Behavioral Targeting
- Breach Notification
- Privacy Policies
  - Discoverable? Comprehendible?
- Devices & Geo-location
- https://otalliance.org/resources/initiatives.html

Regulatory Landscape

FEDERAL • TRADE • COMMISSION ★ UNITED • STATES • OF • AMERICA ★ MCMXV ★

DEPARTMENT OF COMMERCE ★ UNITED STATES OF AMERICA ★

UNITED STATES ★ CONGRESS ★
E PLURIBUS UNUM

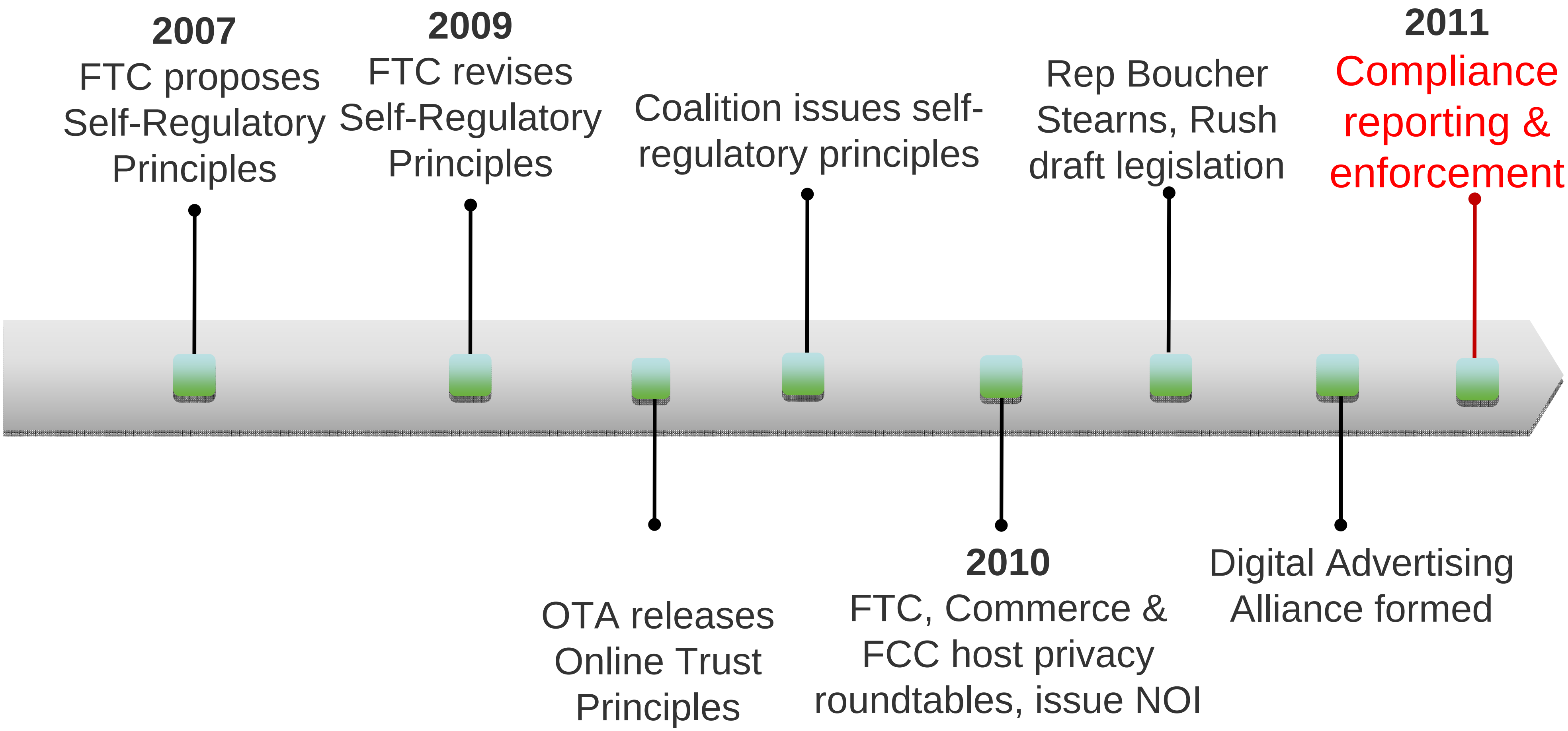
FEDERAL COMMUNICATIONS COMMISSION
★ U ★ S ★

Regulatory Landscape

FEDERAL TRADE COMMISSION ★ UNITED ST

FEDE MUN ATIONS COMMISSION

Evolution of Self-Regulation



2007
FTC proposes Self-Regulatory Principles

2009
FTC revises Self-Regulatory Principles

OTA releases Online Trust Principles

Coalition issues self-regulatory principles

2010
FTC, Commerce & FCC host privacy roundtables, issue NOI

Rep Boucher Stearns, Rush draft legislation

Digital Advertising Alliance formed

2011
Compliance reporting & enforcement

FTC Privacy Report Overview

- **It is not all about "Do No Track"**
- Privacy By Design
- Simplified Choice
- Greater Transparency
- Builds on past focus of:
  - Notice & Choice
  - Access & Security
- Extension to Feb 18 – Comments posted at:

"…a legislative solution will surely be needed if industry does not step up to the plate."

www.ftc.gov/os/comments/privacyreportframework/index.shtm

2011 Email Evolution Conference

Commerce Privacy Green Paper

- Privacy Policy Office (PPO)
- “Will use the office as a bully pulpit …..”
- National data-breach law
- “Privacy Bill of Rights” Fair Information Privacy Principles (FIPPs)
- Comments – 1/28 Deadline

Self-Regulation without strong enforcement is not enough

http://www.ntia.doc.gov/comments/101214614-0614-01/

2011 Email Evolution Conference

Bipartisan Concerns

- Data Collection
- Data Usage
- Data Sharing
- Data Security
- Marketplace innovation
- Online & Off-line
- Consumer and business data

2011 Email Evolution Conference

Top Concepts in FTC Report

- *Privacy by Design*
- *Do Not Track*
- *Simplifying Consumer Choice*
- *Increased Transparency*
- *Future of Self-Regulation*

2011 Email Evolution Conference

Do Not Track

Identified as a candidate for legislation (or self-reg)

- How would a Do Not Track rule work?
- Is technology and self-regulation enough?
- What should companies do today?
- Are the current efforts sufficient?
- What does it mean?
  - Collection of Data
  - Usage of Data
  - Sharing of Data

2011 Email Evolution Conference

Technical Options

- Opt-Out – Cookies
  - In place today, but generally viewed as technically inadequate
  - Does not mean they will not collect or share
- Ad on's

  Ad blockers, impact to ad based services
- Browser Controls
  - Header
  - Integrated solutions (Firefox, IE 9)
  - Distinguish between 1P & 3P

2011 Email Evolution Conference

Distinction - PII & non-PII

- Will PII have relevance as a concept in the future?
- Implications to data providers and email marketers
- Online & off-line

2011 Email Evolution Conference

Privacy Notices

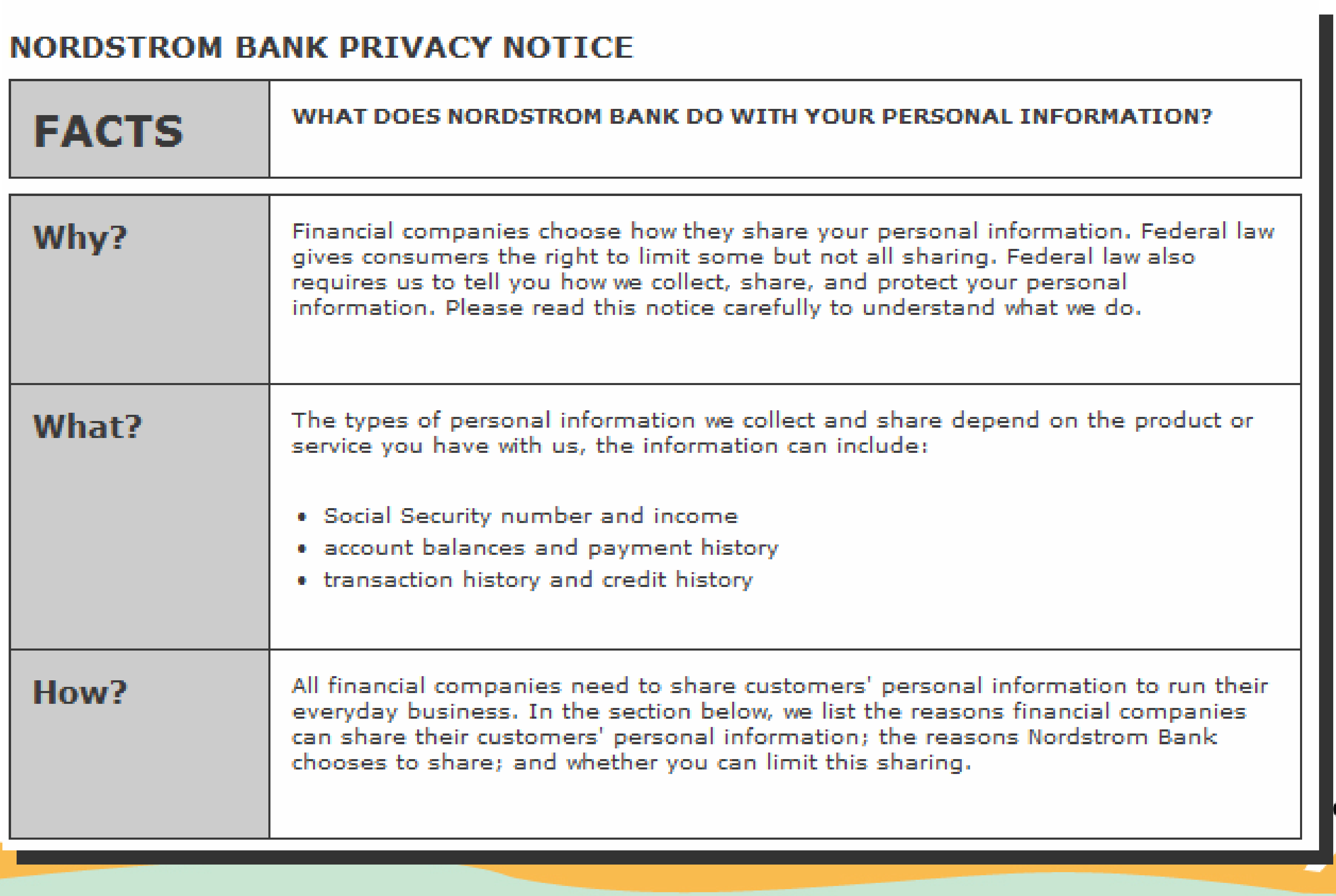
Standardization and Simplification

•A major criticisms was that privacy notices are often very difficult for consumers to understand.

•FTC stressed standardization on two levels:

- o Standardize their policies internally, using similar formats and terminology across all privacy policies.
- o Standardizing privacy notices across companies, pointing to the adoption of standardized, layered privacy notices for financial companies under the Gramm-Leach Bliley Act as a potential model.

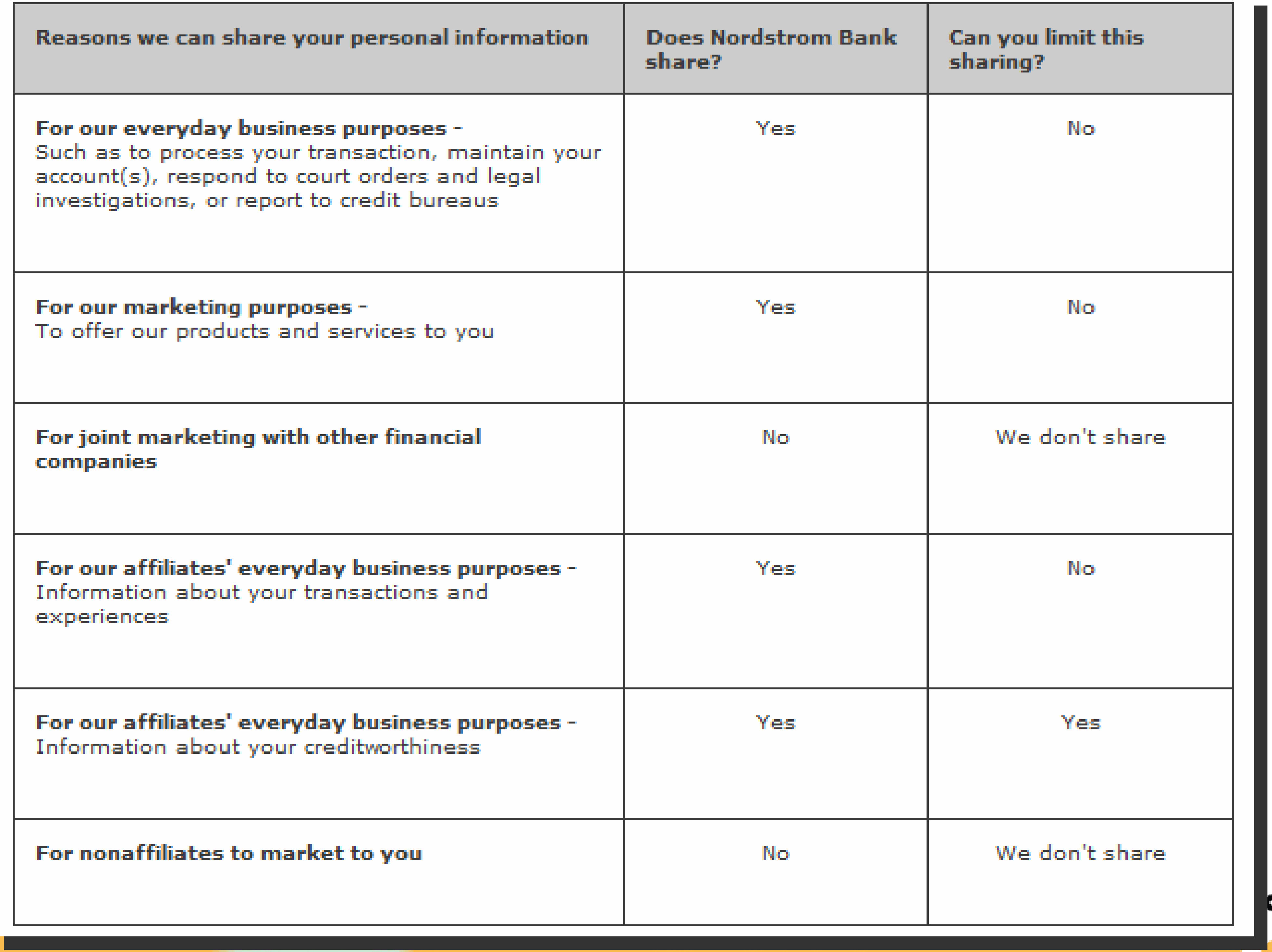
Best Practice



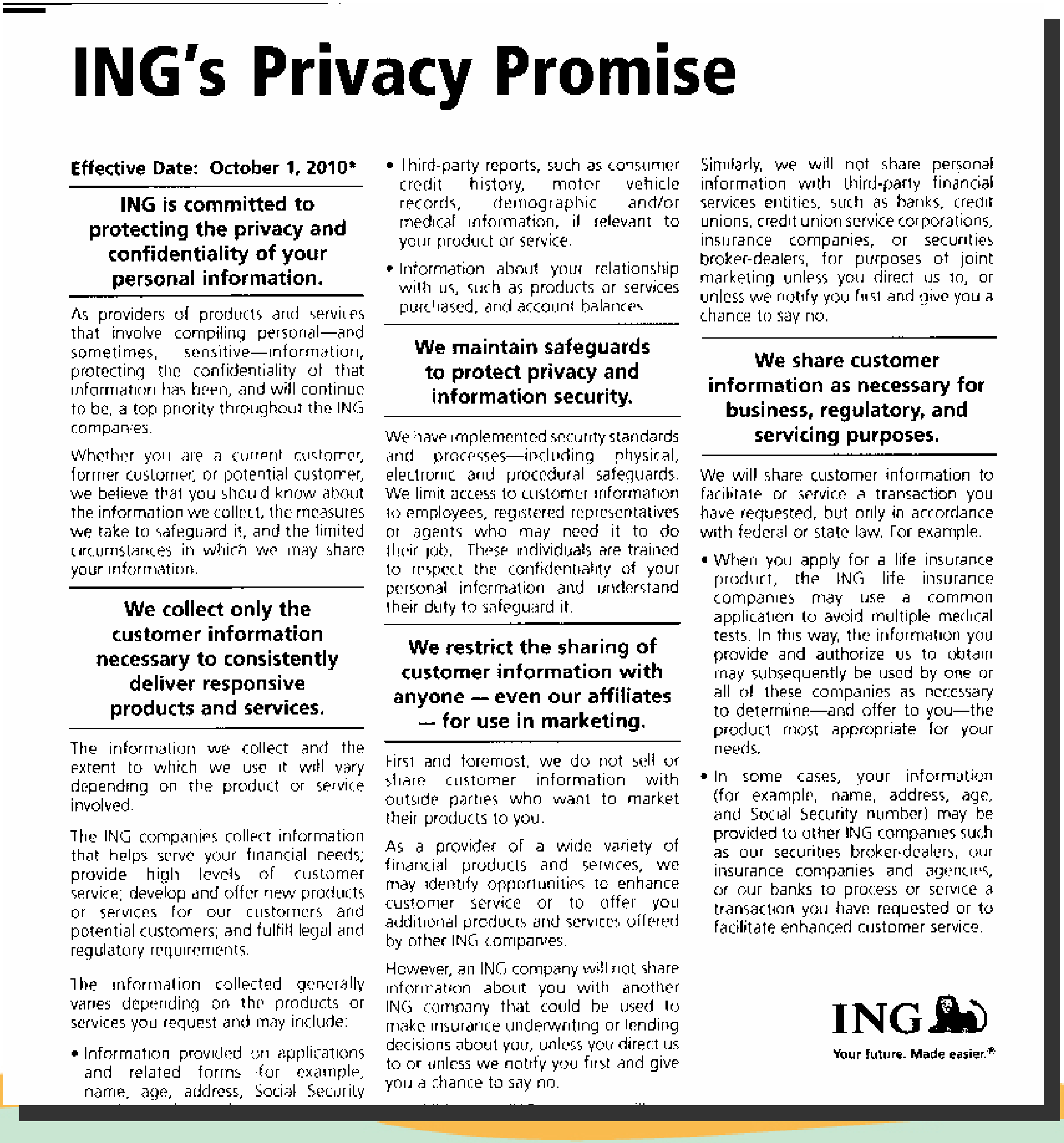
NORDSTROM BANK PRIVACY NOTICE

FACTS	WHAT DOES NORDSTROM BANK DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us, the information can include: • Social Security number and income • account balances and payment history • transaction history and credit history
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons Nordstrom Bank chooses to share; and whether you can limit this sharing.

ce



Reasons we can share your personal information	Does Nordstrom Bank share?	Can you limit this sharing?
For our everyday business purposes - Such as to process your transaction, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus	Yes	No
For our marketing purposes - To offer our products and services to you	Yes	No
For joint marketing with other financial companies	No	We don't share
For our affiliates' everyday business purposes - Information about your transactions and experiences	Yes	No
For our affiliates' everyday business purposes - Information about your creditworthiness	Yes	Yes
For nonaffiliates to market to you	No	We don't share



ING's Privacy Promise

Effective Date: October 1, 2010*

ING is committed to protecting the privacy and confidentiality of your personal information.

As providers of products and services that involve compiling personal—and sometimes, sensitive—information, protecting the confidentiality of that information has been, and will continue to be, a top priority throughout the ING companies.

Whether you are a current customer, former customer, or potential customer, we believe that you should know about the information we collect, the measures we take to safeguard it, and the limited circumstances in which we may share your information.

We collect only the customer information necessary to consistently deliver responsive products and services.

The information we collect and the extent to which we use it will vary depending on the product or service involved.

The ING companies collect information that helps serve your financial needs; provide high levels of customer service; develop and offer new products or services for our customers and potential customers; and fulfill legal and regulatory requirements.

The information collected generally varies depending on the products or services you request and may include:

- Information provided on applications and related forms for example, name, age, address, Social Security
- Third-party reports, such as consumer credit history, motor vehicle records, demographic and/or medical information, if relevant to your product or service.
- Information about your relationship with us, such as products or services purchased, and account balances.

We maintain safeguards to protect privacy and information security.

We have implemented security standards and processes—including physical, electronic and procedural safeguards. We limit access to customer information to employees, registered representatives or agents who may need it to do their job. These individuals are trained to respect the confidentiality of your personal information and understand their duty to safeguard it.

We restrict the sharing of customer information with anyone — even our affiliates — for use in marketing.

First and foremost, we do not sell or share customer information with outside parties who want to market their products to you.

As a provider of a wide variety of financial products and services, we may identify opportunities to enhance customer service or to offer you additional products and services offered by other ING companies.

However, an ING company will not share information about you with another ING company that could be used to make insurance underwriting or lending decisions about you, unless you direct us to or unless we notify you first and give you a chance to say no.

Similarly, we will not share personal information with third-party financial services entities, such as banks, credit unions, credit union service corporations, insurance companies, or securities broker-dealers, for purposes of joint marketing unless you direct us to, or unless we notify you first and give you a chance to say no.

We share customer information as necessary for business, regulatory, and servicing purposes.

We will share customer information to facilitate or service a transaction you have requested, but only in accordance with federal or state law. For example.

- When you apply for a life insurance product, the ING life insurance companies may use a common application to avoid multiple medical tests. In this way, the information you provide and authorize us to obtain may subsequently be used by one or all of these companies as necessary to determine—and offer to you—the product most appropriate for your needs.
- In some cases, your information (for example, name, address, age, and Social Security number) may be provided to other ING companies such as our securities broker-dealers, our insurance companies and agencies, or our banks to process or service a transaction you have requested or to facilitate enhanced customer service.

ING

Your future. Made easier.®

2011 Email Evolution Conference

Future of Self-Regulation

- The Report expresses impatience with self-regulatory progress, as have FTC officials publicly.
- What does that mean for the future of self-regulation?

2011 Email Evolution Conference

Commerce – Green Paper

- Proposes an expanded set of Fair Information Practice Principles (FIPPs).
- Stronger than the FTC Report in raising prospect of baseline privacy legislation.
- Directly raises the question of whether the FTC should be given rulemaking authority to implement privacy principles (which it now lacks under Section 5 of the FTC Act).
- Suggests a safe harbor for companies that adhere to enforceable "codes of conduct."

Commerce – Green Paper

- Cautions any new laws should not preempt strong sectoral laws that already provide important protections, but rather should act in concert.
- Recognizes the role state law has played in building the privacy and data security framework.
- Cautions against impairing states' role as privacy law incubators.
- Role state AG's can play in enforcing privacy rights is expressly recognized.

2011 Email Evolution Conference

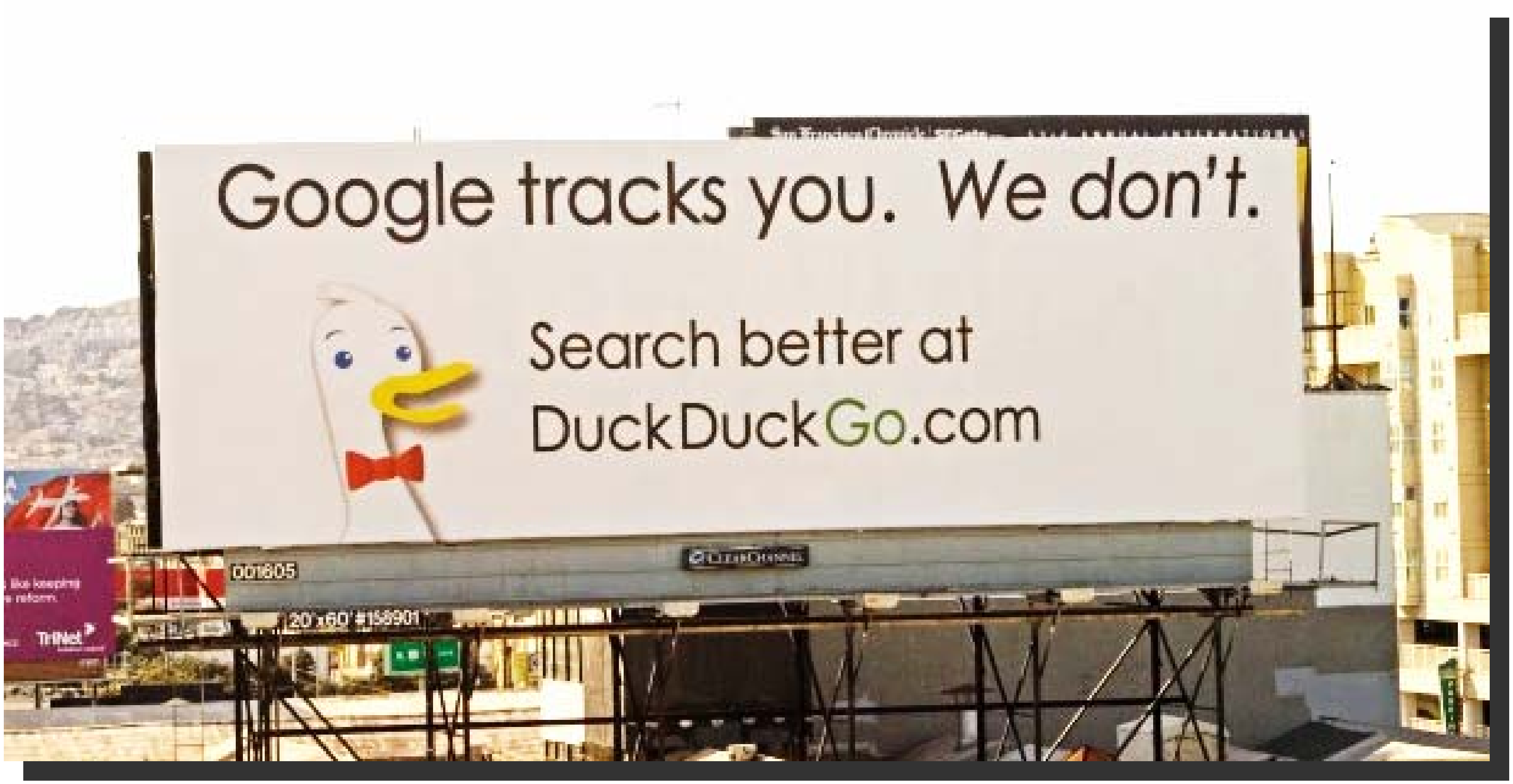
Commerce – Green Paper

- Calls for a federal data security breach notification law for electronic data.
- Call for a Privacy Policy Office (PPO)
  - o Office would not have enforcement authority – the FTC would continue to play the lead privacy enforcement role.

2011 Email Evolution Conference

Competitive Differentiators

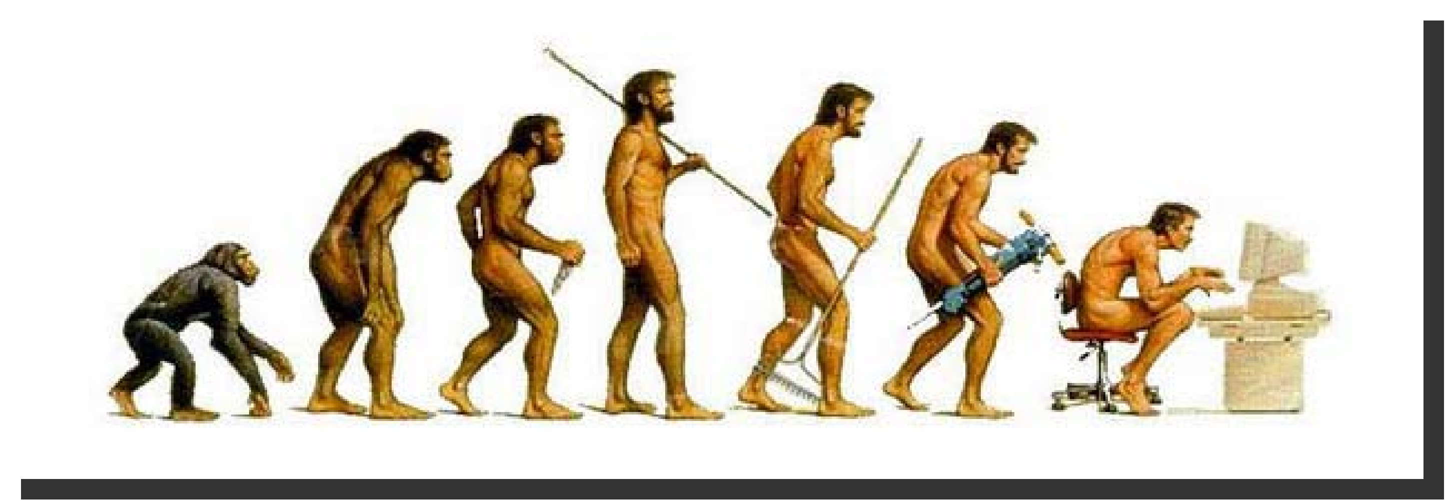
- Security, Privacy & Data Stewardship



Email
Evolution
Conference
2011

Summary

- Times Are Changing
- Evolve & Innovate or Perish



2011 Email Evolution Conference

The Fundamentals Of Compliance

Dennis Dayman
Eloqua
Chief Security and Privacy Officer, CIPP

2011 Email Evolution Conference

Agenda

- Email Overview
  - U.S. – Can-Spam
  - Canada - CASL
- Privacy Overview
  - U.S. Overview
  - E.U. Overview
  - Canada Overview
  - APEC Overview
- Notable differences between U.S. and E.U
- Role of privacy in my email program
- Data Transfers
- U.S. Safe Harbor Program Overview

Can-Spam 2003

- A conspicuous opt-out and/or unsubscribe link (must operate for at least 30-60 days following the campaign) or, alternatively, Reply-To opt-out mechanisms may be used
- Unsubscribes / opt-out requests must be honored within 10 days
- Opt-out / Suppression lists are only used for removals (never for emailing)
- A physical postal address as defined by the USPS postal service
- Subject lines that relate to the body content (and that are not deceptive)
- A SEXUALLY EXPLICIT label in the subject if the content is unsuitable for minors.
- Open relays must not be used to deliver emails

Can-Spam 2003 (cont.)

- Harvested addresses may not be used to send emails
  - Harvested addresses are defined as obtaining addresses through sites that prohibit gathering of email addresses
  - Use of harvested addresses will raise the penalty of any other violations of the CAN-SPAM act
- Automated creation of email addresses through guessing techniques or by using dictionaries to create email addresses is also not permitted.
  - Creation of email addresses and then use of these addresses will also increase penalties for violations of the CAN-SPAM Act
- Religious, Political and National Security messages may be exempt from this Act.

Can-Spam 2008

- The definition of a person has been clarified.
- The definition of a sender has been clarified.
- The definition of a valid physical postal address has been clarified and expanded.
- Opt-Out requests must not cost money and require only one action by the recipient (i.e., click a link, send an opt-out email) and must not request additional information.
  - opt-out requests may not be behind login/password systems
  - opt-out requests may not use persuasive language to keep the recipient
  - opt-out pages may only ask for an email address
  - opt-out links must land directly on an opt-out form

Can-Spam Enforcement

- A individual person or company cannot directly sue another company based on the CAN-SPAM provisions.
- Under CAN-SPAM, only the FTC can enforce these laws.
- Thus, for violations, a complaint must be registered with the FTC who then may choose to investigate such violations and, if necessary, enforce the law.
- Each separate email in violation of the CAN-SPAM Act is subject to penalties of up to $16,000
- Monitor what others are doing on your behalf
  - Can contract away your legal responsibilities
  - Sender and advertiser can be held legally responsible

Electronic Marketing Under Canada’s Anti-Spam Legislation (CASL)

Matthew Vernhout, CIPP/C
Transcontinental Interactive
Director, Delivery and ISP Realtions

2011 Email Evolution Conference

How many of you send email to Canadians?

How many of you don’t know if you send email to Canadians?

Roadmap

- Primary requirements for sending Commercial Electronic Messages (CEM)
- Key differences from CAN-SPAM
- Enforcement
- Jurisdiction
- Next steps: regulations (content, process)

How we got here

- May 2004 - IC establishes Task Force on Spam
- May 2005 – Task Force presents final report to IC
- April 24, 2009 – Bill C-27, the *Electronic Commerce Protection Act* (ECPA) introduced in the HoC
- December 30, 2009: Parliament prorogued
- May 25, 2010 – reintroduced as the *Fighting Internet and Wireless Spam Act* (FISA)
- December 15, 2010 – Royal Assent (with no name!)

CASL: Overview

- CASL will apply to any form of electronic message sent for marketing purposes (referred to as a "Commercial Electronic Message", or "CEM"), including:
    - *Email, SMS, instant messaging and social media/networking.*
- CASL also addresses Internet marketing challenges such as address harvesting, malware, phishing, pharming and other Internet threats

What do I need to do to comply with CASL?

- CASL requires opt-in consent:

    o Explicit opt-in – no expiration, until individual opts-out
    o Deemed or Implied:
        ▪ Where an existing business or non-business relationship with the recipient exists
        ▪ Where the recipient has published their electronic address in a prominent manner*
        ▪ where the recipient has provided their email address directly to the sender

No implied consent for referrals
In most cases implied consent last for 2 years

* And the content of the CME is related to the reason the address was published and they have not indicated that no CEM's can be sent to this address

What do I need to do to comply with CASL?

- CASL requires senders to:
    - Identify themselves
    - Indicate on whose behalf the message is sent
    - Provide up-to-date contact information
    - Include a functional unsubscribe mechanism.

- These rules apply regardless of how many messages are sent

Defining: Business Relationships

- You are considered to have had a *business relationship* when a customer has purchased/leased a product, good or service, bartered or entered a contract with you.
- You are considered to have had a *non-business relationship* when a person donates to, volunteers for, or becomes an official member of, your organization.

Exemptions

- Family or personal relationship (to be defined in regulations)
- Business inquiry

No consent required

- Quotes or estimates, if requested
- Facilitates commercial transaction
- Warranty or safety information
- Information about ongoing subscription, membership, etc.
- Information related to employment relationship or benefit plan
- Delivers good or service

Types of Messages in CASL

- Commercial Electronic Message:
  - “commercial activity” means any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, whether or not the person who carries it out does so in the expectation of profit
  - An electronic message that contains a request for consent to send a message is also considered to be a commercial electronic message.

- Personal Message:
  - sent by or on behalf of an individual to another individual with whom they have a personal or family relationship

Note: No definition of Transactional mail

Unsubscribes

- The unsubscribe mechanism *must:*
  - Be available by the same electronic means by which the message was sent
  - *Specify an electronic address, or link to a* page on the World Wide Web that can be accessed through a web browser, to which the indication may be sent.
  - Valid for a minimum of ***60 days*** after the message has been sent
  - ***Without delay***, and in any event no later than ***10 business days*** after the indication has been sent, without any further action being required on the part of the person who so indicated.

Similarities with CAN-SPAM

- Requirement to accurately identify sender
- Prohibition false and misleading transmission data/subject lines
- Requirement for unsubscribe mechanism
- Liability for brands who knowingly allow spam to be sent on their behalf
    - Beware and police your affiliates

Installation of computer programs

- Computer programs cannot be installed w/o express consent

- Exemptions:
  - Installation of an update or upgrade to a computer program the installation or use of which was expressly consented
  - Cookies and HTML/Scripts are excluded

Oversight & Enforcement

- Three agencies:
  - Canadian Radio-television and Telecommunications Commission (CRTC)
  - Competition Bureau
  - Office of the Privacy Commissioner (OPC)
- Administrative monetary penalties (AMPS):
  - Up to **$1 million** for individuals and **$10 million** in all other cases per violation
- Private Right of Action:
  - Available to any person affected by a violation - actual and statutory damages
- Protection for ‘honest mistakes’ (due diligence is key)

Jurisdiction

- Section 12: “A person contravenes section 6 only if a computer system located in Canada is used to send or access the electronic message.”
- Thus, CASL applies to all messages that leave or enter Canada

Enforcement against U.S. orgs

- PRA: reciprocal enforcement of judgement legislation
  - *Facebook inc. v. Adam Guerbuez* (Quebec)
  - $873 million US enforced by QC Courts
- Enforcement of AMPs more challenging
- Explicit provision for international collaboration

Regulations

- Allow Industry Canada and CRTC to clarify rules
- Likely published for comment in Feb-March 2011
- Issues for clarification:
  - Definition of personal or family relationship
  - Identification information required when obtaining consent
  - Conditions for use of consent on behalf of unknown third parties

Anti-Spam in Canada - Summary

- Canadian Anti-Spam Legislation or CASL:
  - Opt-in
  - Prohibits Unsolicited Commercial Messages
  - Prohibit installation of programs without consent
  - No false information
    - Sender or Subject Lines
  - No harvesting or dictionary attacks
  - More than email:
    - IM; SMS; social media; voice*

* May replace Canadian Do Not Call Registry

Anti-Spam in Canada - Summary

- Other requirements:
  - identification; contact information; unsubscribe mechanism
- Unsubscribe:
  - Without delay, but not longer than 10 business days
  - No longer recommended “no-reply@”
- Certain messages exempted altogether:
  - family or personal relationship; business inquiry/relationship
- Proper identification (Postal Address)

- Private Right of Action Included
- Enforcement cross border - Can’t hide under HQ location
- Protection for “Honest” Mistakes

What is Privacy

- Control
- Secure
- Right

What kind of information can be private?

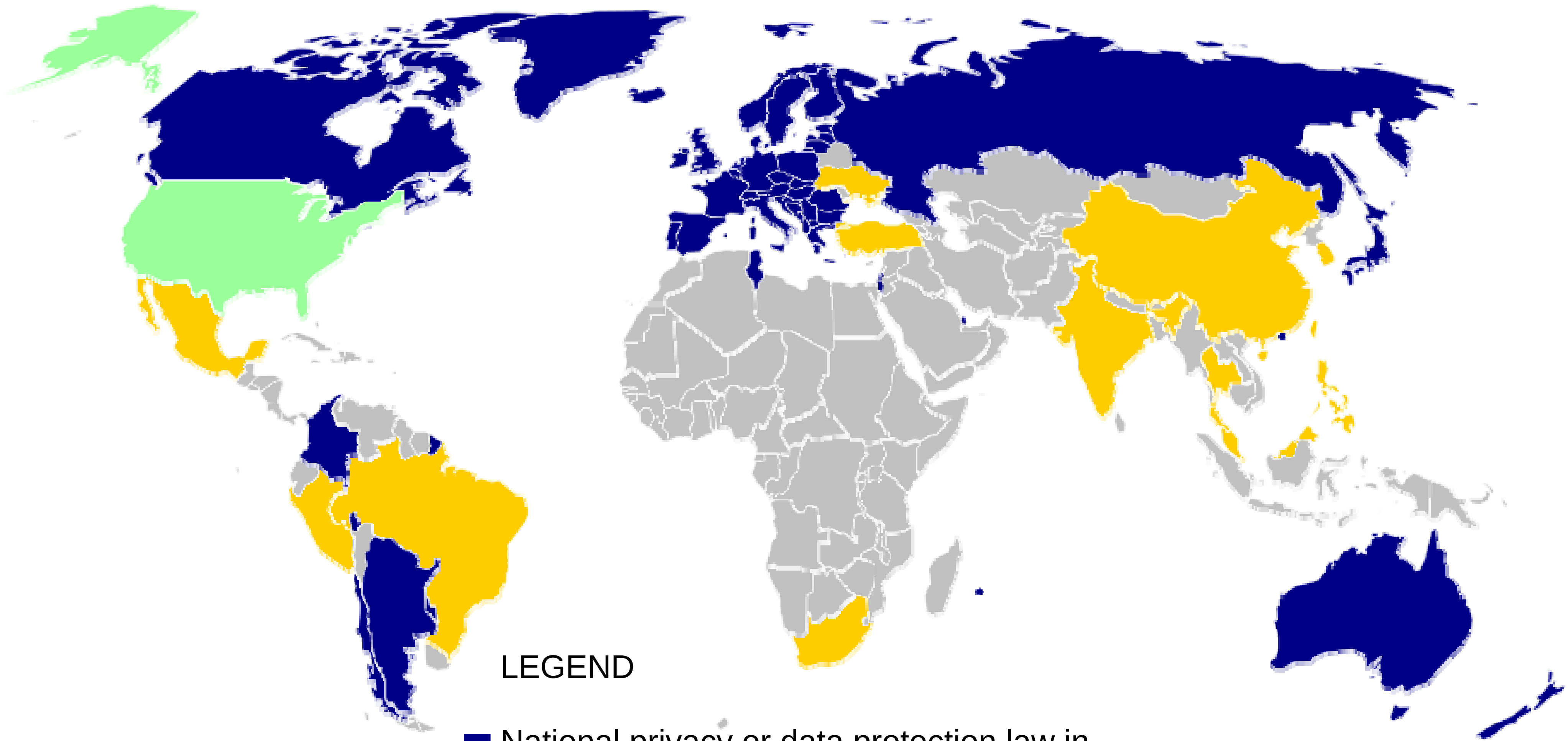
- **Names**
- Postal Addresses
- Telephone numbers
- Social Security Numbers
- Account Numbers
- Driver Licenses Numbers
- Financial Account Numbers – Credit Cards, Checking
- Logins and Passwords
- Habits of any sort or Personal preferences
- IP Addresses
- **Email addresses**

The rub

- Originally the Internet was motivated by the need to share information.

- We as a people will buy anything that’s one to a customer
  - Loyalty Programs
  - Express Checkout discounts

A Global Perspective is Needed



LEGEND

🟦 National privacy or data protection law in place
🟩 Other significant privacy laws in place
🟨 Emerging privacy or data protection laws

*Courtesy of the IAPP

Privacy in the U.S.

- Not a fundamental human right
- Patchwork of industry, local, state and federal laws.
- Typically an opt-out scheme with a dash of opt-in and notice.
- Privacy is a process of need by sector

U.S. - Future

- Wants to moving towards umbrella system like Canada and EU.
- Notice and consent for covered/sensitive information
  - Over broad definition
  - Transferring information to third parties
  - Notices needs to be on home page
- Used for any purpose
- Consent for tracking
- Opt-out needs to be clear

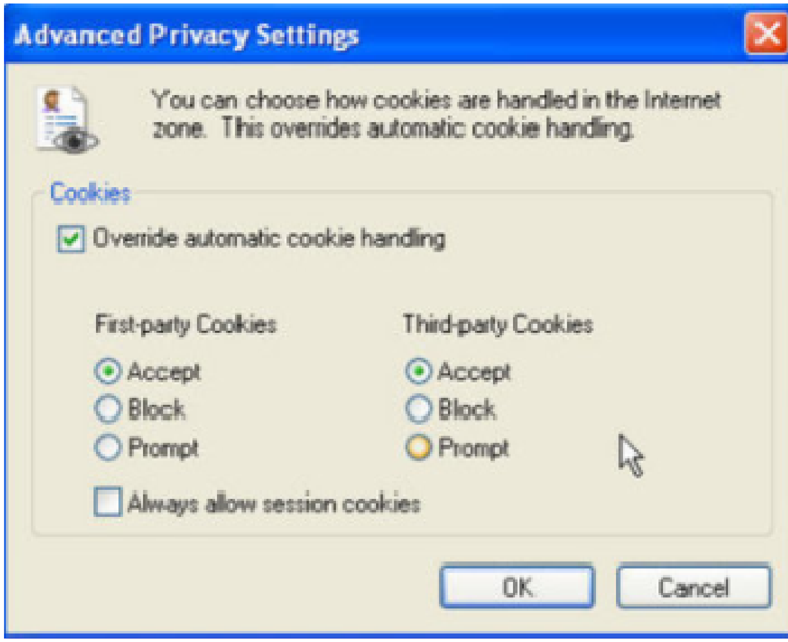
Privacy in Canada

- Fundamental human right
- Personal Information Protection and
- Electronic Documents Act (PIPEDA)
- Privacy law, not an email law
- Opt-in in model
- Give clear notices on why the need, uses, and secures data.
- Gives control of opt-out and inaccurate data
- PIPEDA follows an ombudsman model

Privacy in the European Union (E.U)

- Fundamental human right
- Privacy law, not an email law
- Opt-in in model
- E.U. Data Protection Directive
- Member nations are compelled to enact data protection laws and create supervisory bodies.
- Applies to processing of personal data by automatic means in a filing system

Privacy in the European Union (E.U) - Future



Advanced Privacy Settings

You can choose how cookies are handled in the Internet zone. This overrides automatic cookie handling.

Cookies

☑ Override automatic cookie handling

First-party Cookies	Third-party Cookies
● Accept	● Accept
○ Block	○ Block
○ Prompt	○ Prompt

□ Always allow session cookies

- Cookie/Tracking opt-in
  - Hidden in Telecom bill
  - Flash included. Any tracking
  - Building profiles requires opt-in
  - Obtain opt-in via privacy policy
  - May 2011 deadline
    - 28 members will all enact this differently
  - Browsers control
    - Satisfies opt-in?
    - First vs. third party cookie
  - Exemptions
    - Strictly necessary - Checkout

Privacy Principles overall

- Notice – When data is used
- Purpose – What data being used for
- Consent – Not disclosed without permission
- Security – Kept secure from abuse and sight
- Disclosure – Informed who is collecting
- Access- Ability to correct or remove
- Accountability – Data collectors held accountable

Differences in U.S. and E.U

- Fundamental human right in E.U
- The United States prefers what is called a “sectoral” approach to data protection legislation.
- To date, the U.S. has no single, overarching privacy law comparable to the EU Directive.
- Privacy legislation in the United States tends to be adopted on an “as needed” basis.
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Cable Television Consumer Protection and Competition Act of 1992
  - Fair Credit Reporting Act

Role of privacy in my email program

- Notice: Opt-in in most cases
- Choice: Provide opt-out or preference center
- Purpose: Use data for only what you said you would use it for
- Disclosure: In some countries, you can’t track by default
- Don’t sign up customer for whatever you feel
- Don’t use to much PII in email programs
- Don’t link to customer accounts

Data Transfers

- Transfers of personal data to countries outside of the E.U. are only permitted to countries that provide adequate level of protection.
  - Canada, Argentina, Switzerland
  - U.S. Safe Harbor program participants, etc
- You could be fined for unauthorized transfers
- Private right of action by persons damaged
- Lose customers out of trust issues
- PR nightmare

U.S. Safe Harbor Program

- Safe Harbor Privacy Policy sets forth the privacy principles that companies must follow if they want to transfer personal information from the European Union (EU) to the United States (U.S.)

- The United States Department of Commerce and the European Commission agreed on a set of data protection principles (the "Safe Harbor Principles”)

U.S. Safe Harbor principles

- U.S. organization that is subject to the jurisdiction of the Federal Trade Commission (FTC).
- Make reference to your Safe Harbor Adherence in your Privacy Policy
- Provide an accurate privacy policy and is available to the public
- Establish an independent process to investigate unresolved complaints
- Are required to have procedures in place for verifying compliance
- Designate a Contact Point Within Your Organization Regarding Safe Harbor

U.S. Safe Harbor principles (cont.)

- In order to have a Privacy Policy Statement that conforms to the Safe Harbor Principles:
  - Notice
  - Choice
  - Onward transfer to third parties
  - Access
  - Security
  - Data integrity
  - Enforcement

APEC Privacy

- Asia-Pacific Economic Cooperation (APEC) is a forum for 21 Pacific Rim countries

- APEC Privacy Framework requires organizations to hold themselves accountable when transferring personal data outside of those member countries.

- Provides weaker data protection than the EU Directive

APEC Privacy (cont.)

The nine principles of the APEC Privacy Framework are:

1. Preventing harm
2. Notice
3. Collection Limitations
4. Uses of Personal Information
5. Choice
6. Integrity of Personal Information
7. Security Safeguards
8. Access and Correction
9. Accountability

How to write a good policy

- DMA's Privacy Policy Generator
  - http://www.dmaresponsibility.org/PPG/

- Tips for optimizing your privacy policy:
  - Write it for consumers
  - Keep it short
  - Index it or give it headers so people can find what they want quickly
  - Audit the policy at least once a year (and have non-lawyers also read it for clarity)
  - Link out to relevant sections of your policy to "contact us" features so readers with questions can get answers
  - Inform customers about policy changes, but be sure to do so before the changes go public and give people a chance to change preferences prior to launch
  - Highlight the policy throughout the site

External Resources

- US Department of Commerce Safe Harbor
  - http://www.export.gov/safeharbor/

- Federal Trade Commission Privacy Initiatives
  - http://www.ftc.gov/privacy/

- Organisation for Economic Co-operation and Development (OECD) – Privacy Policy Generator
  - http://www2.oecd.org/pwv3/

- International Association of Privacy Professionals (IAPP)
  - https://www.privacyassociation.org/index.php

Privacy Impact

Unfair Trade Practices, Violation of Section 5 of the FTC Act

•FTC vs. Gateway Learning

- Company rented customer information it pledged to Keep Private per it’s privacy policy in the past

- The FTC alleged that, after collecting consumers’ information, Gateway Learning changed its privacy policy to allow it to share the information with third parties without notifying consumers or getting their consent

- FTC fined Gateway learning for misrepresentation, halted data sharing prior to privacy change, and FTC has oversight for five (5) years to make Gateway demonstrate compliance with their orders. This includes review of privacy policies, opt-in consent information, and invoices/contracts relating to third parties.

Conclusion

- Privacy policies and data collection and use policies should be human readable, comprehensive, and easy to locate
- Write your policy for customers
- Only the minimum amount of information reasonably necessary to provide you with services should be collected and maintained, and only for so long as reasonably needed
- Changes to privacy policies should be communicated to customers ASAP with ability to change or opt-out
- Have clear, conspicuous and repeated notice of data collection and use throughout your site
- Audit your policy once a year for data flow changes.

Lunch Topics

- Please join us for roundtable lunch discussions:
  - Email Authentication
  - Deliverability
  - North American Anti-Spam Legislation
    - CASL, CAN-SPAM
  - Regulatory landscape
    - Privacy, Security & Data Governance
  - Cloud, Social & Mobile

- Be back for afternoon sessions by 1:10

Protecting Integrity Of Email & Maximizing Deliverability

Robert Consoli
Silverpop
Director, Deliverability & Provisioning Services

Michelle Pelletier
Return Path
Sr. Director, Professional Services

2011 Email Evolution Conference

Agenda for this Section

- Integrity of Email
- Deliverability and Reputation
- Deliverability and Engagement
- Authentication
- Branding

INTEGRITY

But Why Does It Really Matter

And Really…

Deliverability & Reputation

No Inbox.

No Click.

No ROI.

In fact, 1 in 5 emails sent never sees the inbox!

That means 20% of email goes here, NOT the inbox!

That’s good money down the drain.

Why do my good emails get blocked?

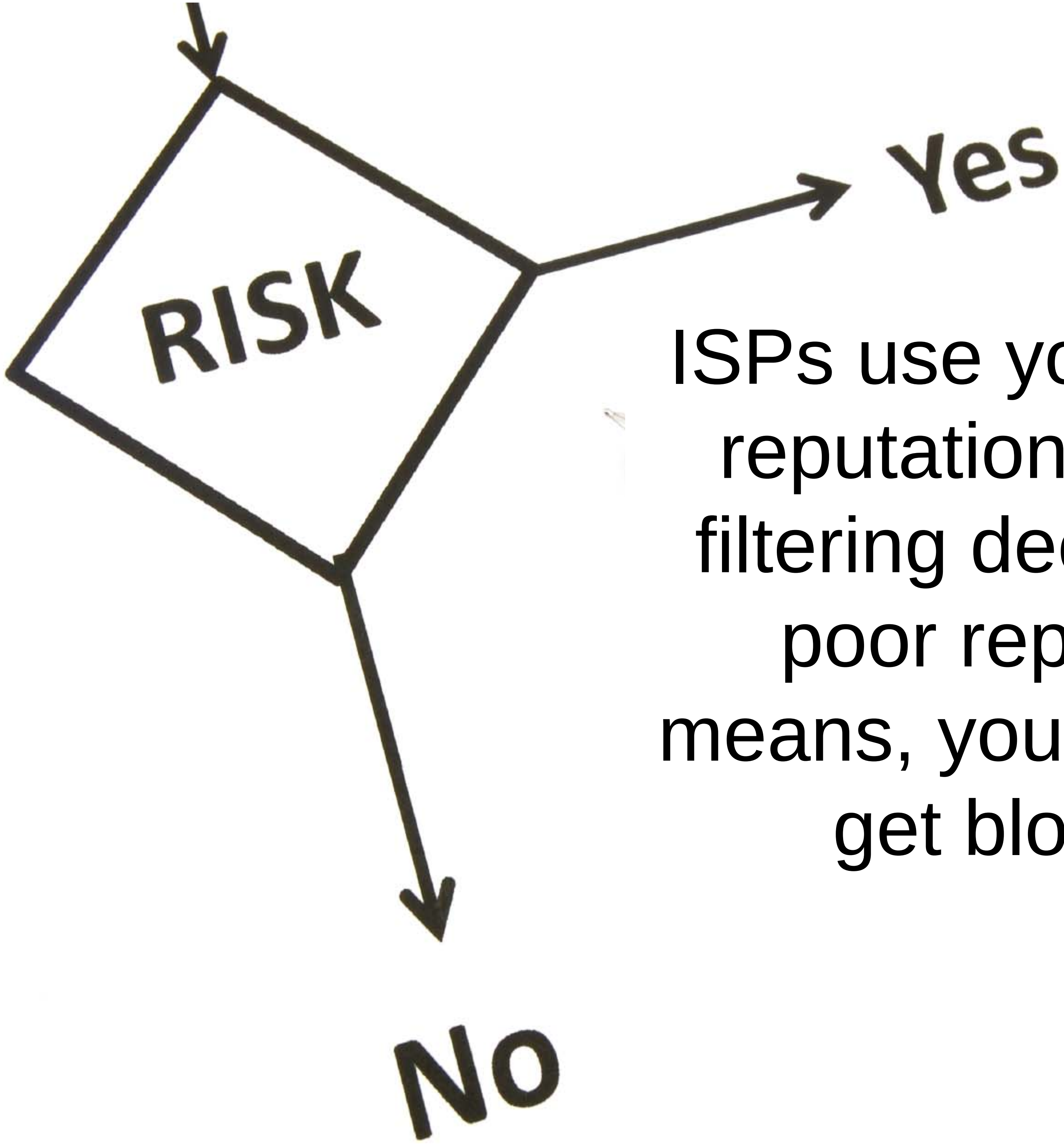
Quick wins instead of having to invest loads of money and time….

- ***Do Not*** *buy lists.*
- ***Do Not*** *add recipient's that may not understand why they are being added.*
- ***Do Not*** *keep recipient's that do not want to be on your list.*
- ***Target*** *your emails – make them relevant!*
- *Make sure you have proper authentication(SPF, Sender ID, DomainKey's/DKIM) in place* ***prior*** *to sending*.

…..It’s the exact same message I sent last week and it wasn’t blocked then….

- Did you send to a new list that you haven't sent to before?
- Did you receive a lot of abuse complaints?
- Did you send to many spam traps?
- Has the reputation on the IP address gone down?
- ISPs can and will change their filters thousands of times a day
- A word/phrase that was accepted 2 hours ago, may be blocked now
- Test your content before sending to your live lists

Sender reputation drives inbox placement and therefore, response.



ISPs use your sender reputation to make filtering decisions. A poor reputation means, your email will get blocked.

But there are a few hurdles to cross…

Each ISP has their own rules for using reputation to determine inbox placement.

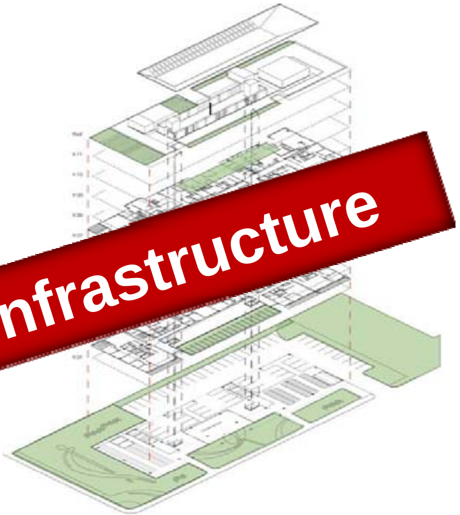
Yahoo! **AOL** **Hotmail** **Gmail** **Comcast**

	Complaint	Unknown User	Spam Trap
AOL	✓	✓	✓
Windows Live	✓	✓	✓
YAHOO!	✓		✓
Gmail by Google	✓	✓	✓

Reputation is a set of metrics based on your sending behavior.

Complaints

List Hygiene



Infrastructure

IP Permanence

$4.95 ships your order
when you buy from our eco-conscious collection—48 HRS ONLY
feel-good bags
by baggallini
SHOP OUR GREEN GROUP >
100% recycled, 100% stylish!
see entire eco collection >
DID YOU KNOW?

Message Quality

Engagement

Compliance Is Only The Beginning

Take Charge of Your Program!

You’re already in control!

- Complaints
- List Hygiene
- Sending Infrastructure and Authentication
- Sending Permanence
- Content
- Engagement

Three Words to Remember..

Deliverability Loves Engagement!

Question…

What did Deliverabilitysay to Engagement?

YOU Complete ME!

2011 Email Evolution Conference

Deliverability and Engagement

- Managing recipient engagement is **KEY** to your deliverability success.
- Facts:
  - o Engaged users complain less
  - o Engaged recipients open more often
  - o Engaged recipients stay engaged
  - o ISP's love engaged recipients
  - o Deliverability loves engaged ISPs

I
DON'T
CARE

Measuring Engagement

Types of Engagement Metrics Used

- Recipient Engagement is here to stay!
  - o Tracking:
    - The amount of time the email stays in the inbox before deleted
    - Opens
    - Clicks
    - TINS (This is Not Spam) Clicks
    - Spam Complaints
    - Email Deletions
- Panel data
- Mail sent to inactive accounts (Spam Traps)

Windows Live
Hotmail

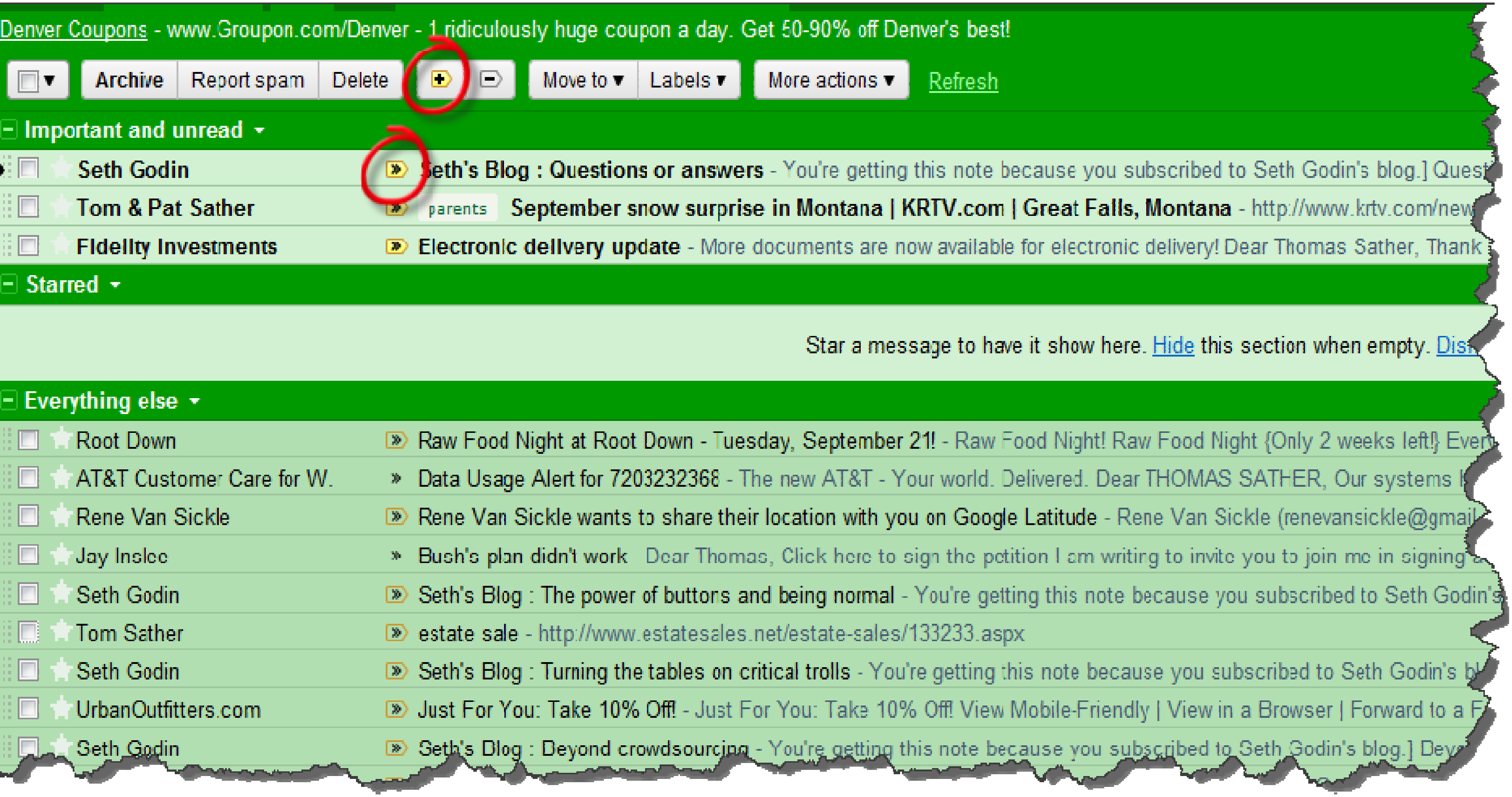
YAHOO!

Gmail™
by Google

Windows Live Hotmail

1. **Messages read, then deleted**
2. **Messages deleted without being read**
3. **Messages replied to**

1. Google Prediction
2. Starred mail
3. How it's addressed
4. Importance



Denver Coupons - www.Groupon.com/Denver - 1 ridiculously huge coupon a day. Get 50-90% off Denver's best!

Important and unread ▾

- Seth Godin — **Seth's Blog : Questions or answers** - You're getting this note because you subscribed to Seth Godin's blog.] Quest
- Tom & Pat Sather — parents **September snow surprise in Montana | KRTV.com | Great Falls, Montana** - http://www.krtv.com/new
- Fidelity Investments — **Electronic delivery update** - More documents are now available for electronic delivery! Dear Thomas Sather, Thank

Starred ▾

Star a message to have it show here. Hide this section when empty. Dis

Everything else ▾

- Root Down — Raw Food Night at Root Down - Tuesday, September 21! - Raw Food Night! Raw Food Night {Only 2 weeks left!} Ever
- AT&T Customer Care for W. — Data Usage Alert for 7203232368 - The new AT&T - Your world. Delivered. Dear THOMAS SATHER, Our systems
- Rene Van Sickle — Rene Van Sickle wants to share their location with you on Google Latitude - Rene Van Sickle (renevansickle@gmail
- Jay Inslee — Bush's plan didn't work - Dear Thomas, Click here to sign the petition I am writing to invite you to join me in signing
- Seth Godin — Seth's Blog : The power of buttons and being normal - You're getting this note because you subscribed to Seth Godin's
- Tom Sather — estate sale - http://www.estatesales.net/estate-sales/133233.aspx
- Seth Godin — Seth's Blog : Turning the tables on critical trolls - You're getting this note because you subscribed to Seth Godin's bl
- UrbanOutfitters.com — Just For You: Take 10% Off! - Just For You: Take 10% Off! View Mobile-Friendly | View in a Browser | Forward to a F
- Seth Godin — Seth's Blog : Beyond crowdsourcing - You're getting this note because you subscribed to Seth Godin's blog.] Bey

What can I do about Subscriber Engagement?

Did You Know?

- Deliverability is Portable.
- Most B2B Domains:
  - o Use a Filter Device (Umbrella Service).
  - o Are hosted by a Provider with a spam filter.
  - o **Are hosted by Large ISPs and Inbox Providers!**
- ISP’s and Inbox Providers pay very little attention to the type of mailer.
- Primary focus for ISPs and Inbox Providers are their own recipients.

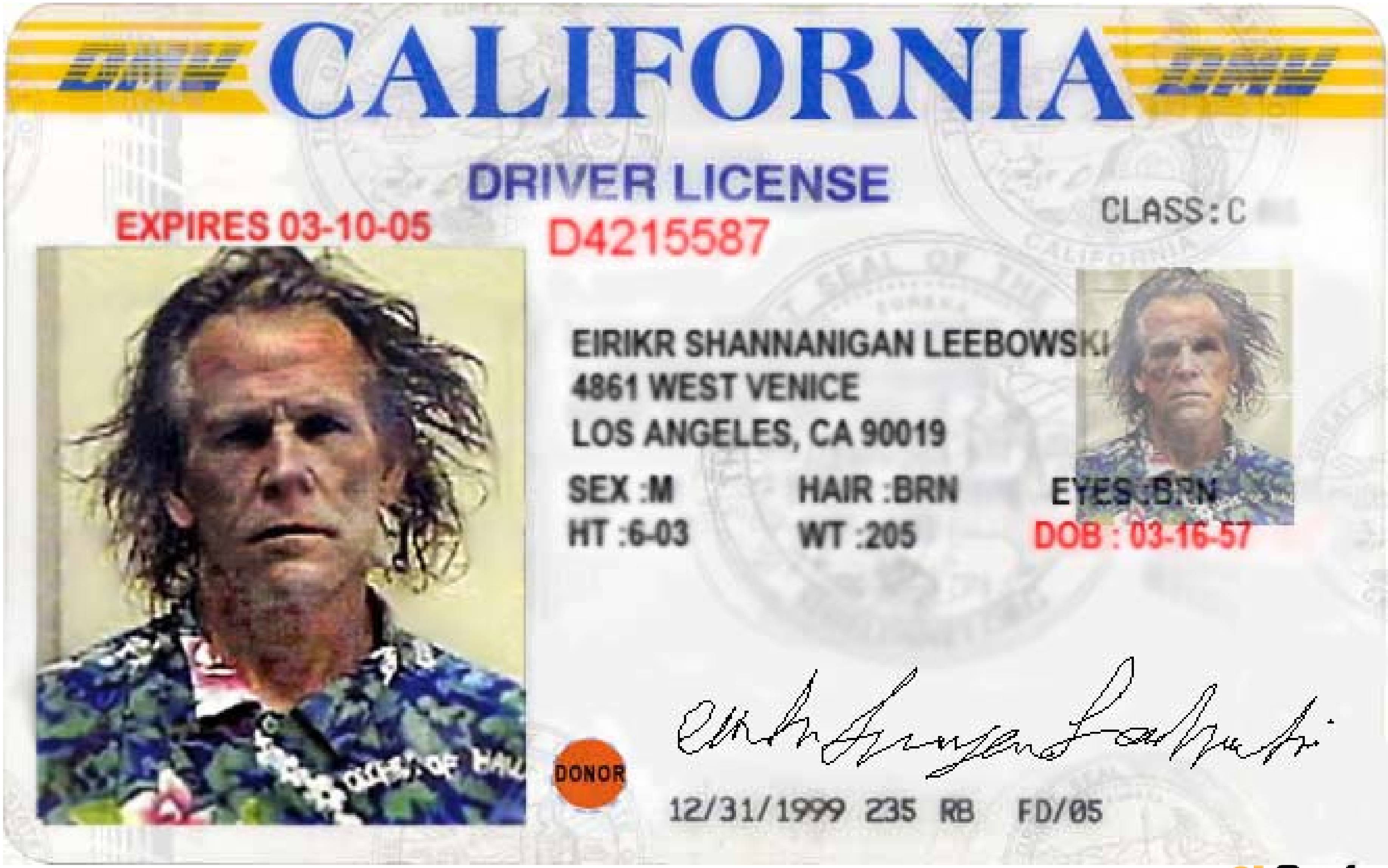
So…Doesn’t My ESP Handle this?

But how do I *know* what my sender reputation is?

www.senderscore.org
www.dnsstuff.com
www.senderbase.com

Authentication

Authentication



DMV CALIFORNIA DMV

DRIVER LICENSE

EXPIRES 03-10-05

D4215587

CLASS: C

EIRIKR SHANNANIGAN LEEBOWSKI
4861 WEST VENICE
LOS ANGELES, CA 90019

SEX :M	HAIR :BRN	EYES :BRN
HT :6-03	WT :205	DOB : 03-16-57

DONOR

12/31/1999 235 RB FD/05

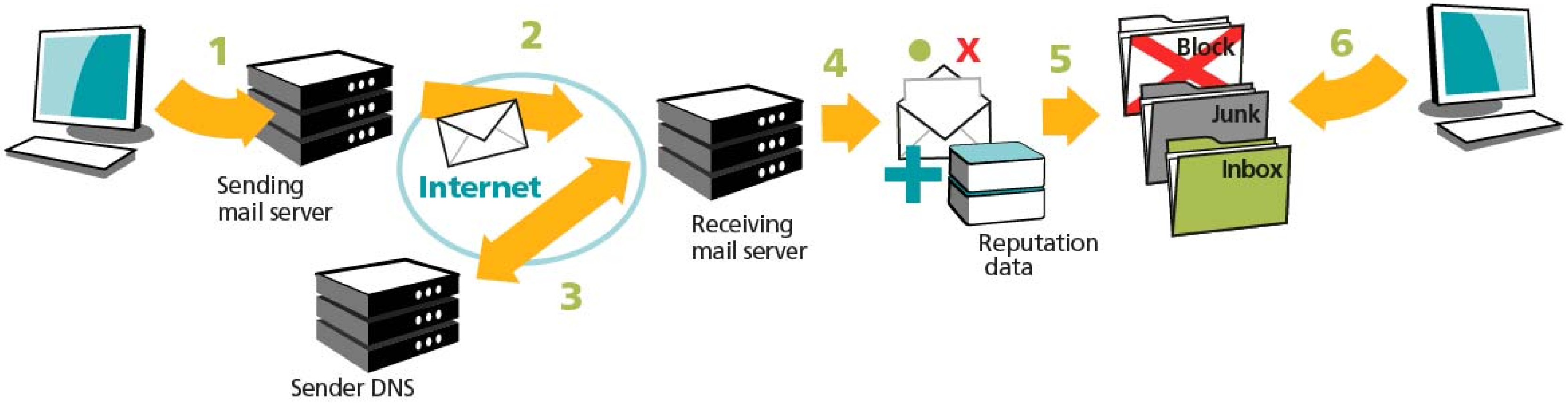
Types of Authentication

- SPF (Sender Policy Framework)
- Sender ID
- DomainKeys
- DKIM (DomainKeys Identified Mail)

Why we need it

- Spoofing
- Phishing
- Spam

Email Authentication – How it works



2011 Email Evolution Conference

What Authentication Does and Doesn’t Do

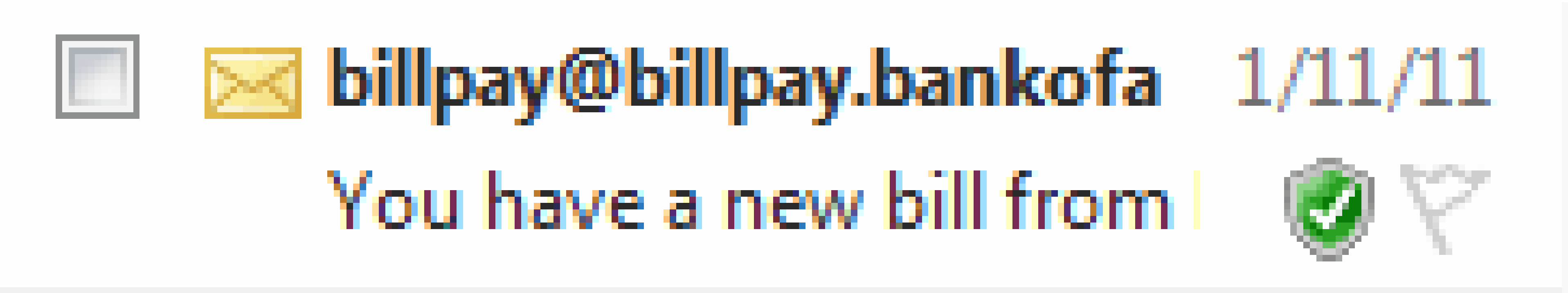
- Does
  - Verify Sender
  - Establishes Reputation
  - Sets Foundation for Domain Reputation
  - Implicit Benefits
    - FBL
    - Trust Icons
    - Assurance for your Brand

- Doesn't
  - No Explicit Deliverability Benefits
  - Doesn't Stop Phishing or Spoofing

Reputation/Authentication

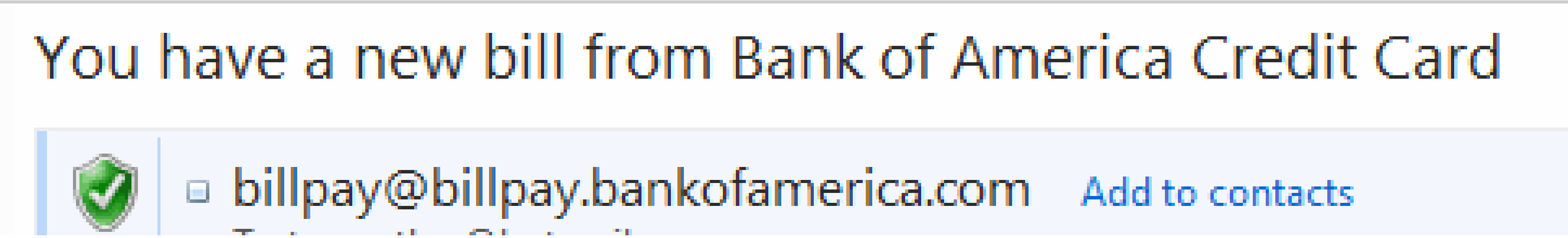
- *Brands should be protected.*
- *Email Authentication technology helps good senders build and control their own reputation.*
- *SPF / Sender ID – based on the from domain and the IP of the sending email server.*
- *DomainKeys/DKIM – based on the from domain and configuration settings of the email server.*

Trusted Icon



billpay@billpay.bankofa 1/11/11

You have a new bill from



You have a new bill from Bank of America Credit Card

billpay@billpay.bankofamerica.com Add to contacts

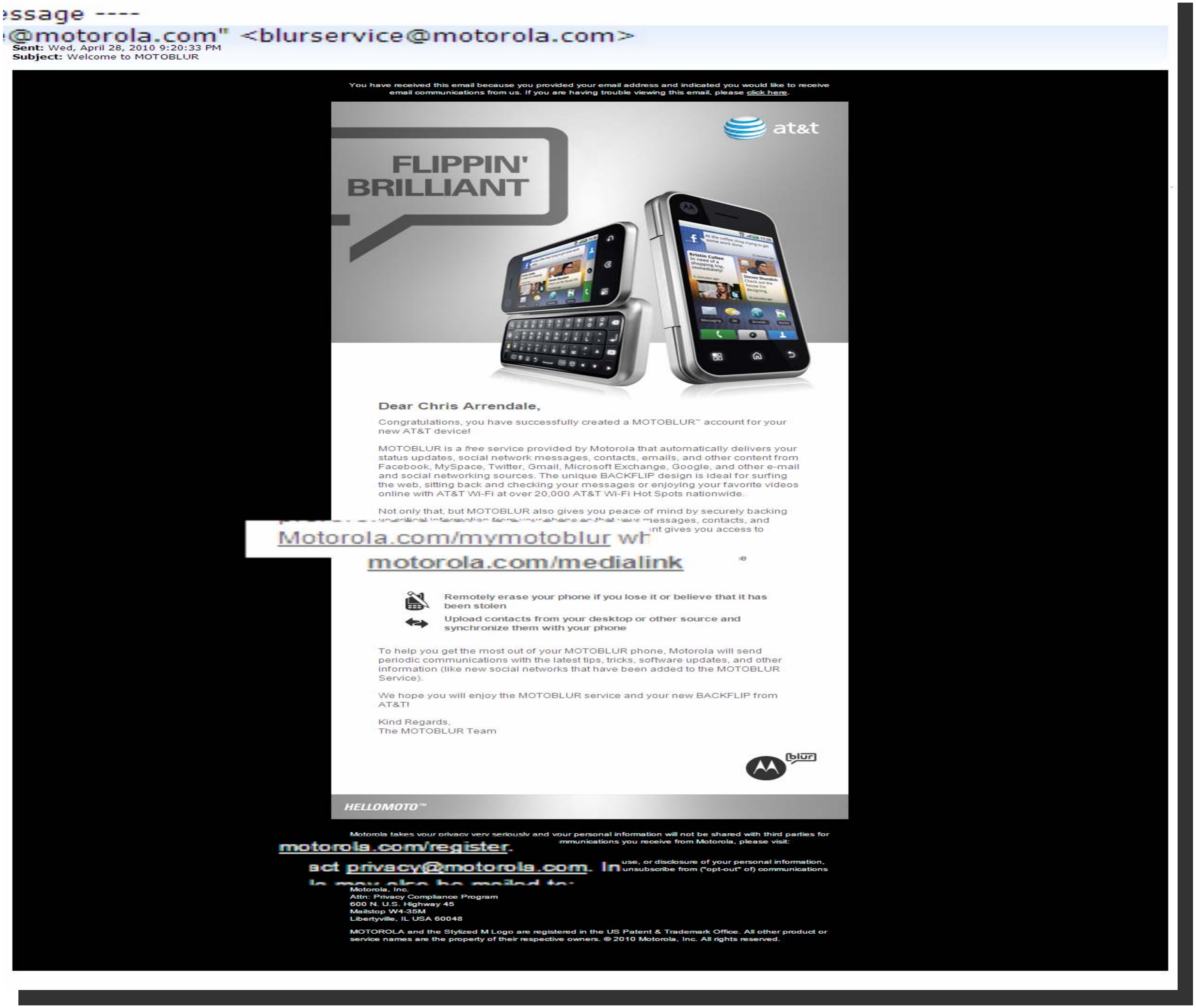
Welcomes & Branding

Don’t wait to send

- Reasons not to wait:
  1. **Stay relevant!**
  2. **Meet expectations!**
  3. **Keep your data fresh!**
  4. **Reduce complaints!**
  5. **Establish a relationship!**
  6. **Take advantage of a need!**
  7. **Demonstrate your integrity!**

Branding

- *Very Important for Subscribers to recognize your Brand and what you are sending:*
  - *Branded From Email Address*
  - *Branded From Name*
  - *Branded Subject Line*
  - *Branded Links*
- *Goal is to make Subscribers open and engage in your emails.*



essage ----

@motorola.com" <blurservice@motorola.com>

Sent: Wed, April 28, 2010 9:20:33 PM
Subject: Welcome to MOTOBLUR

You have received this email because you provided your email address and indicated you would like to receive email communications from us. If you are having trouble viewing this email, please click here.

Dear Chris Arrendale,

Congratulations, you have successfully created a MOTOBLUR™ account for your new AT&T device!

MOTOBLUR is a *free* service provided by Motorola that automatically delivers your status updates, social network messages, contacts, emails, and other content from Facebook, MySpace, Twitter, Gmail, Microsoft Exchange, Google, and other e-mail and social networking sources. The unique BACKFLIP design is ideal for surfing the web, sitting back and checking your messages or enjoying your favorite videos online with AT&T Wi-Fi at over 20,000 AT&T Wi-Fi Hot Spots nationwide.

Not only that, but MOTOBLUR also gives you peace of mind by securely backing up critical information from your phone so that your messages, contacts, and

Motorola.com/mymotoblur wh nt gives you access to

motorola.com/medialink e

- Remotely erase your phone if you lose it or believe that it has been stolen
- Upload contacts from your desktop or other source and synchronize them with your phone

To help you get the most out of your MOTOBLUR phone, Motorola will send periodic communications with the latest tips, tricks, software updates, and other information (like new social networks that have been added to the MOTOBLUR Service).

We hope you will enjoy the MOTOBLUR service and your new BACKFLIP from AT&T!

Kind Regards,
The MOTOBLUR Team

Motorola takes your privacy very seriously and your personal information will not be shared with third parties for

motorola.com/register. mmunications you receive from Motorola, please visit:

act privacy@motorola.com. In use, or disclosure of your personal information, unsubscribe from ("opt-out" of) communications

ls may also be mailed to:

Motorola, Inc.
Attn: Privacy Compliance Program
600 N. U.S. Highway 45
Mailstop W4-35M
Libertyville, IL USA 60048

MOTOROLA and the Stylized M Logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners. © 2010 Motorola, Inc. All rights reserved.

4 Steps to the Inbox:

Configure:

- *Setup Authentication - SPF, SenderID, DomainKeys, DKIM.*

Make Friends:

- *Get signed up on all feedback loops and white lists possible – not all ISP’s/Inbox Providers have one but research those that do and sign up!*

Design Campaigns:

- *Make sure your Image to Text Ratio is ~30/70.*
- *Include an “Add to Address” Book statement.*
- *Include text or html unsubscribe link (not an image) – one click opt out is best.*
- *Include Postal Address in Footer.*

Monitor and Maintain:

- *Keep User Engagement High – Target recipients with relevant content and stop sending to any that are not interested.*
- *Keep your abuse complaint rate below 0.3% - remove complaints immediately.*
- *Keep your bounce rates below 10% - remove hard bounces immediately.*
- *Entice and remind recipient’s to add your from address to their address book.*
- *Respond to replies.*

Focus Points:

- *Reputation! As more and more providers are starting to turn to reputation for folder placement, it's never been more important to monitor both IP and domain reputation.*

- *When issues are found, look at any changes that were recently made and research improvements to correct – quickly!*

- *Bounce management, Complaint Management, Spam Traps and Blacklists should always be monitored to ensure good deliverability.*

- *Brand recognition is HUGE. User engagement has never been more important and Brand recognition will go a long way in helping to keep user engagement high.*

- *Remember the 4 steps to getting into the inbox:*
  - *Configure*
  - *Make friends*
  - *Design campaigns*
  - *Maintain*

ISP	SPF	Sender ID	DomainKeys	DKIM	Action Auth Fail	WL/FBL Offered	Action on Abuse
Free.fr	X				Y	N/N	U
Deutsche Telekom	X				Y	N/N	Y
Arcor.de	X	X	X	X	Y	N/N	Y
Telus.ca	X				Unk	N/Y	Y
Bell Canada	X	X	X	X		Y/Y	Y
AOL				X	N	Y/Y	Y
Gmail	X	X	X	X	Unk	N/N	Y
Hotmail		X			Y	N/Y	Y
Yahoo			X	X	Y	Y/Y	Y
Earthlink			X	X		N/Y	Y
RoadRunner	X					Y/Y	Y
Comcast			X	X	Unk	N/Y	Y
Cox				Testing	n/a	N/Y	Y

Tools to use:

Corporate Blacklists & Spam Filters

- Fortiguard Antispam from Fortinet - http://www.fortiguard.com/antispam/antispam.html
- Sophoslabs - http://www.sophos.com/security/ip-lookup
- Symantec Brightmail - http://www.symantec.com/business/security_response/landing/spam/index.jsp
- Barracuda - http://www.barracudacentral.org/lookups/ip-reputation
- Proofpoint - https://support.proofpoint.com/rbl-lookup.cgi

Reputation Services

- SenderScore - https://www.senderscore.org/
- Cisco IronPort SenderBase - http://www.senderbase.org/
- McAfee TrustedSource - http://www.trustedsource.org/
- Pivotal Veracity - http://www.pivotalveracity.com/email-marketing-solution/email-reputation.html

2010 / 2011 Email Authentication Scorecard *Foundation of Derivability & Consumer Trust*

Craig Spiezle
Online Trust Alliance
Executive Director & President

2011 Email Evolution Conference

Why Email authentication?

- Line of defense for spoofing, fraud & malicious threats
  - Allows receiving networks (Enterprise and ISPs) to validate the mail is coming from the purported sender
  - Sender, Commerce Sites, Financial Institutions, Gov.
  - Two complementary efforts; SPF/ Sender ID & Domain Keys Identified Mail (DKIM)
  - Allows for applying reputation scoring
  - Need to check / reject for non-existent domains

2011 Email Evolution Conference

What has changed ……

- Broader call for data governance
- More aggressive law suits by State AG's
- Redefinition of what is PII & adequate notification
- Call for allowing for private right of action except for approved safe harbor program.
- Failure of business taking reasonable steps
- ESPs & Ad supply chain being exploited (Malvertising compromised)

Complimentary Standards

SPF/Sender ID

- “Path Based”
  - Senders publish acceptable message paths (IP) for domain
- Near-zero deployment requirements for senders
  - DNS records only, no change to outbound servers
- Scalability; near-zero impact to CPU resources
- Forwarding introduces new IP address not in SPF record

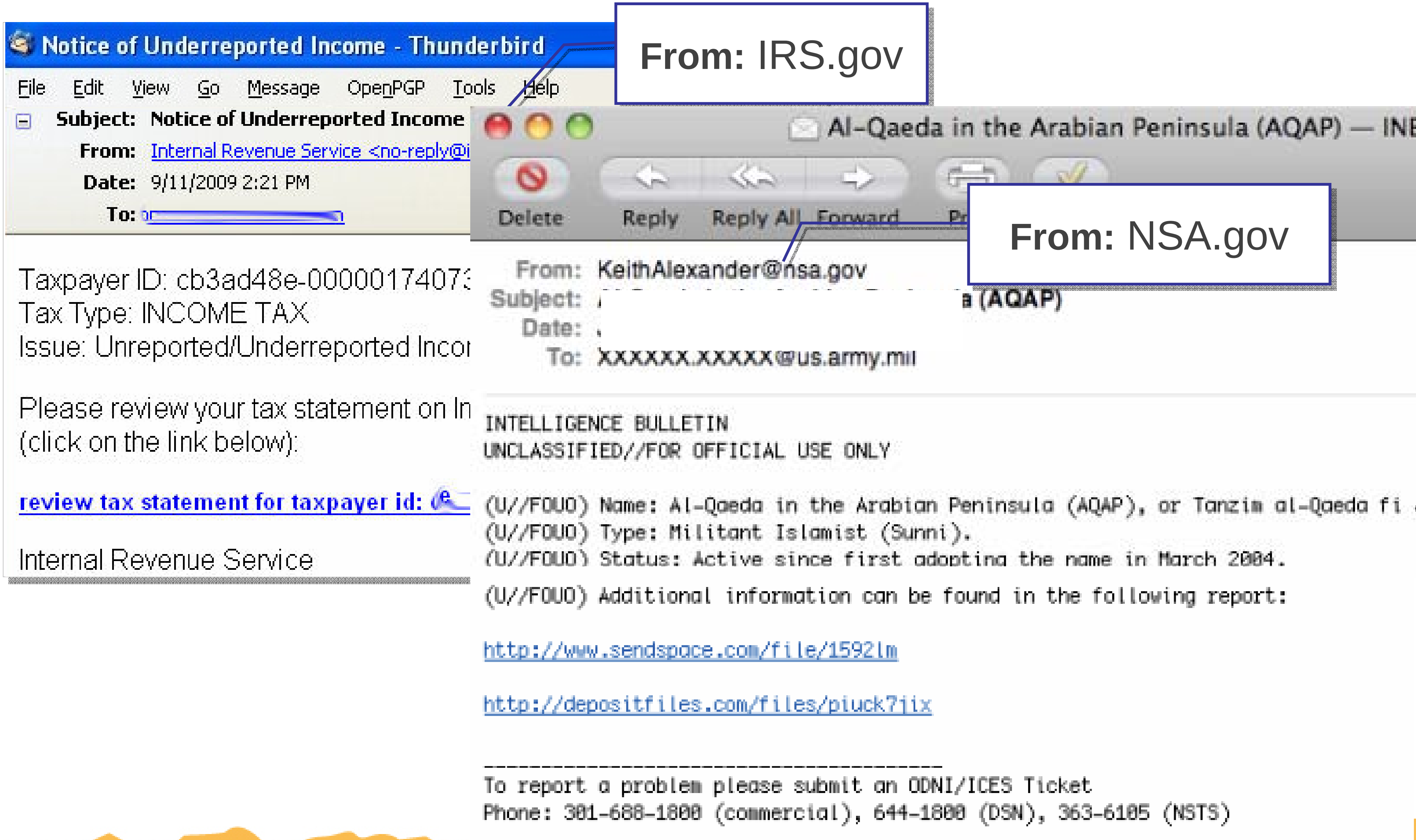
Is the messenger (server) permitted?

DKIM

- “Signature based”
  - Senders insert digital cryptographic signature in emails for domain
- Requires cryptographic operation by sender and receiver’s gateway infrastructure
- Supports forwarding, may survive multiple “hops”

Is the signature authentic?

IRS and NSA Attacks



Notice of Underreported Income - Thunderbird

Subject: Notice of Underreported Income
From: Internal Revenue Service <no-reply@i
Date: 9/11/2009 2:21 PM
To: [redacted]

Taxpayer ID: cb3ad48e-00000174073
Tax Type: INCOME TAX
Issue: Unreported/Underreported Incor

Please review your tax statement on In
(click on the link below):

review tax statement for taxpayer id: (

Internal Revenue Service

From: IRS.gov

Al-Qaeda in the Arabian Peninsula (AQAP) — INE

From: KeithAlexander@nsa.gov
Subject: [redacted] a (AQAP)
Date:
To: XXXXXX.XXXXX@us.army.mil

INTELLIGENCE BULLETIN
UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U//FOUO) Name: Al-Qaeda in the Arabian Peninsula (AQAP), or Tanzim al-Qaeda fi
(U//FOUO) Type: Militant Islamist (Sunni).
(U//FOUO) Status: Active since first adopting the name in March 2004.

(U//FOUO) Additional information can be found in the following report:

http://www.sendspace.com/file/1592lm

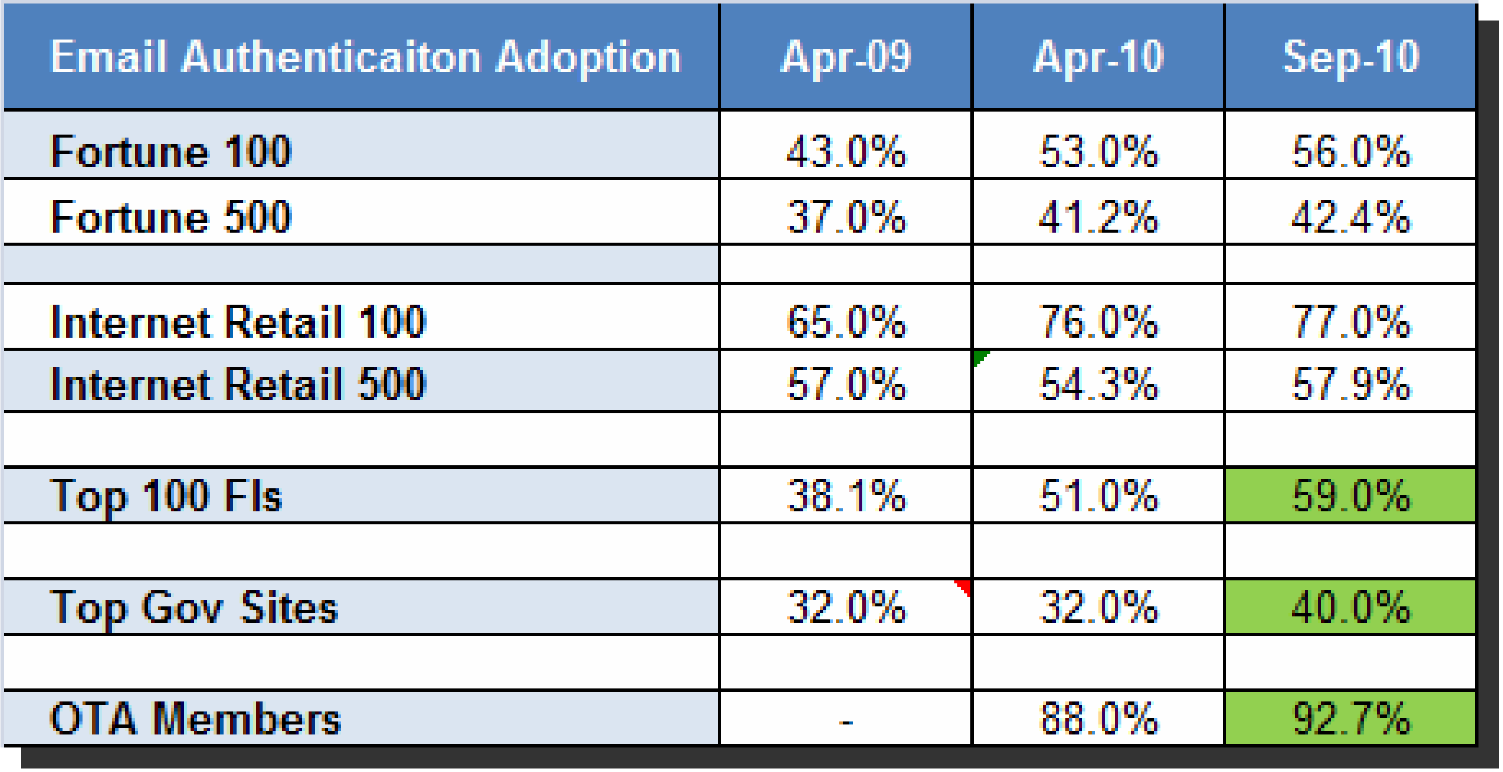
http://depositfiles.com/files/piuck7jix

To report a problem please submit an ODNI/ICES Ticket
Phone: 301-688-1800 (commercial), 644-1800 (DSN), 363-6105 (NSTS)

From: NSA.gov

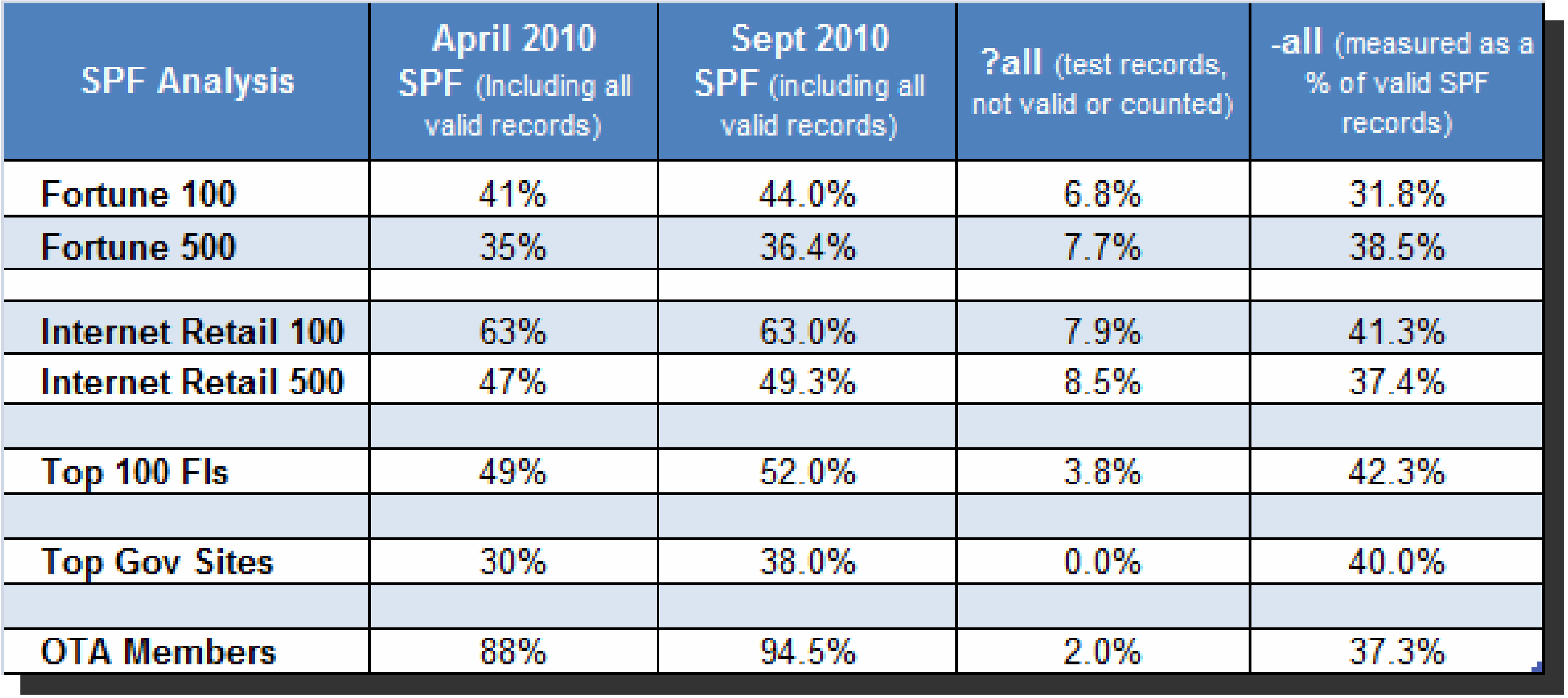
Summary Adoption

- Increases in financial services, government & OTA Members
- Includes SPF, SenderID & DKIM



Email Authenticaiton Adoption	Apr-09	Apr-10	Sep-10
Fortune 100	43.0%	53.0%	56.0%
Fortune 500	37.0%	41.2%	42.4%
Internet Retail 100	65.0%	76.0%	77.0%
Internet Retail 500	57.0%	54.3%	57.9%
Top 100 FIs	38.1%	51.0%	59.0%
Top Gov Sites	32.0%	32.0%	40.0%
OTA Members	-	88.0%	92.7%

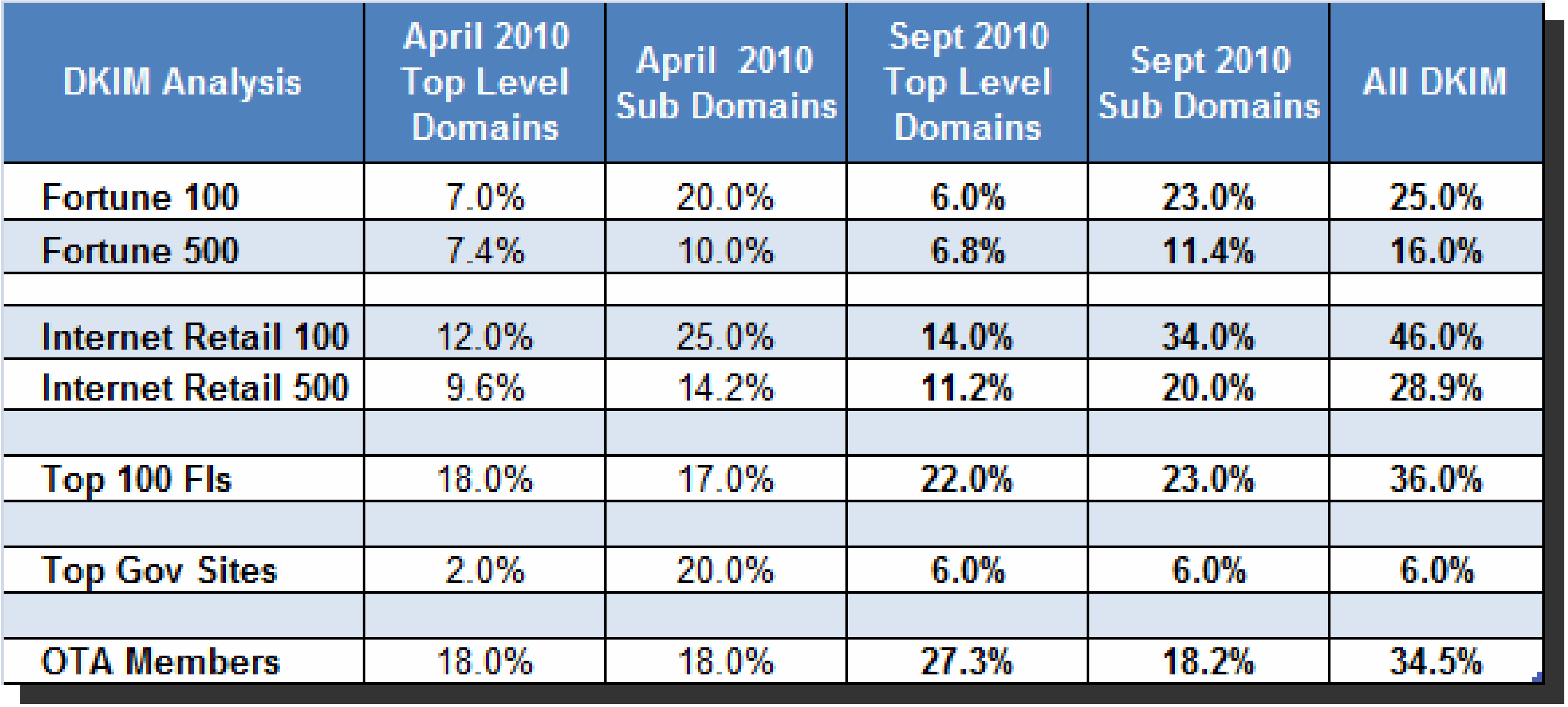
SPF



SPF Analysis	April 2010 SPF (Including all valid records)	Sept 2010 SPF (including all valid records)	?all (test records, not valid or counted)	-all (measured as a % of valid SPF records)
Fortune 100	41%	44.0%	6.8%	31.8%
Fortune 500	35%	36.4%	7.7%	38.5%
Internet Retail 100	63%	63.0%	7.9%	41.3%
Internet Retail 500	47%	49.3%	8.5%	37.4%
Top 100 FIs	49%	52.0%	3.8%	42.3%
Top Gov Sites	30%	38.0%	0.0%	40.0%
OTA Members	88%	94.5%	2.0%	37.3%

- Focused on the TLD of the organization only for fraud detection.
- *May undercount usage by not including delegated sub-domains.*
- Retail and Banking lead in efforts to counter fraud
- Continued growth and increase usage of – all records
- Record quality improving. Education required to discourage usage of ?all

DomainKeys Identified Mail (DKIM)



DKIM Analysis	April 2010 Top Level Domains	April 2010 Sub Domains	Sept 2010 Top Level Domains	Sept 2010 Sub Domains	All DKIM
Fortune 100	7.0%	20.0%	6.0%	23.0%	25.0%
Fortune 500	7.4%	10.0%	6.8%	11.4%	16.0%
Internet Retail 100	12.0%	25.0%	14.0%	34.0%	46.0%
Internet Retail 500	9.6%	14.2%	11.2%	20.0%	28.9%
Top 100 FIs	18.0%	17.0%	22.0%	23.0%	36.0%
Top Gov Sites	2.0%	20.0%	6.0%	6.0%	6.0%
OTA Members	18.0%	18.0%	27.3%	18.2%	34.5%

- To maximize protection BOTH the Top Level Domain (TLD) and sub domains sites should sign and use a ADSP
- The TLD is typically most recognizable to the consumer and what the home page of the site resolves to.

2011 Data Breach &Loss Incident Planning Guide

Preparing for the inevitable

Craig Spiezle
Online Trust Alliance
Executive Director & President

2011 Email Evolution Conference

2010 Data Breach Highlights

- 602 reported breaches, 26 MM records
  - o 40% via hacking (94% of records)
  - o 28% social engineering (3% of records)
  - o 96% non-sophisticated tactics
- SQL injection into sites
- Stolen laptops
- User names, passwords & email
- Common passwords

2011 Email Evolution Conference

Why Email Marketers Must Care

- Costs
  - $6.75 MM per incident / $204 per record
- Impact to your brand
  - Can I trust you with my customer data
  - Can I trust the brand
  - Email reputation
  - Impact to the email channel
- Recent trend exploiting email marketers

2011 Email Evolution Conference

Why Email Marketers Must Care

- Are you taking reasonable steps to protect systems, data & infrastructure from exploits?
  - o Increasing regulatory scrutiny - FTC Act
  - o Stock holder suits
  - o Private right of action
  - o Loss of business

2011 Email Evolution Conference

Risk Assessment - Are you ready?

1. Do you know what sensitive information is maintained by your company, where it is stored and how it is kept secure?

2. Do you have an incident response team in place ready to respond 24/7?

3. Are management teams aware of security, privacy and regulatory requirements related specifically to your business?

2011 Email Evolution Conference

Risk Assessment - Are you ready?

4. Have you completed a privacy and security audit of all data collection activities including cloud and outsourced services?
5. Are you prepared to communicate to customers, partners and stockholders?
6. Do you have readily available access codes and credentials to critical systems in the event key staff are not available or are incapacitated?

Risk Assessment - Are you ready?

7. Are employees trained and prepared to notify management in the case of accidental data loss or a malicious attack?

   Do your policies require notification to management?

   Are employees reluctant to report such incidents for fear of disciplinary action or termination?

2011 Email Evolution Conference

Risk Assessment - Are you ready?

8. Have you coordinated with all necessary departments with respect to breach readiness?

9. Do you have a privacy review and audit system in place for third-party service providers? Have you taken necessary or reasonable steps to protect users' confidential data?

10. Do you review the plan on a regular basis to reflect key changes?

2011 Email Evolution Conference

Data Loss Can be Prevented

- 90% can be addressed with simple steps and operational discipline

2011 Email Evolution Conference

Key Elements

1. Data Classification
2. Audit & Validate Access
3. Intrusion & Breach Analysis & Auditing
4. Data Loss Prevention Technologies
5. Data Minimization & Destruction Policies
6. Curb Abuse to Your Brand, Domain & Email
7. Inventory System Access & Credentials
8. Creating an Incident Reponses Team
9. Establish Vendor Relationships

2011 Email Evolution Conference

Key Elements

10. Create a project plan
11. Determine who needs to be notified
12. Communicate & draft responses
13. Provide Assistance & Remedies
14. Employee Training
15. Critique & Post Mortem
16. Analyze Legal Implications
17. Funding & Budgeting

2011 Email Evolution Conference

Focus or Email Marketers

1. Data Classification
4. Data Loss Prevention Technologies
6. Curb Abuse to Your Brand, Domain & Email
8. Creating an Incident Reponses Team
9. Establish Vendor Relationships
10. Create a project plan
11. Determine who needs to be notified
12. Communicate & draft responses
13. Provide Assistance & Remedies

2011 Email
Evolution
Conference

Elements of an Effective DIP

- Data Governance & Loss Prevention
  - o Data Classification
  - o Data In Use
  - o Data In Transit
  - o Data at Rest
  - o Audit & Validate Data Access

Email Evolution Conference 2011

Loss Prevention Email Marketers

- Use of Secure Socket Layer (SSL) for all forms
- Data & Disk encryption (suppression lists….)
- Encryption of wireless routers
- Upgrading to browsers
- Email authentication to help detect malicious and deceptive email and web sites
- Automatic patch management for operating systems, applications & add-ons

2011 Email Evolution Conference

Response Plan

- Defined & empowered team
  - o 24/7 1st responders
- Know your law enforcement contacts
- Understand forensics requirements
- Communicational templates, & scripts
- Notification tree, partners, customer & employees
- Remedies – Credit Monitoring Services
- Employee training

2011 Email Evolution Conference

Open Discussion

- Do we care?
- What have we learned?
- What is actionable?

2011 Email Evolution Conference

More Information

Online Trust Alliance
https://otalliance.org

Data Breach & Los Guide
https://otalliance.org/resources/Incident.html

+1 425.455.7400

craigs@otalliance.org

OTA
Online Trust Alliance

2011 Email Evolution Conference

THANK YOU

Questions?

2011 Email Evolution Conference