Smart in your world®
Arent Fox

The road to PCI Compliance: The Marriage of Law, IP, and Accounting Fields

Presented by

Anthony V. Lupo

Patty Eichinger

Arent Fox LLP

Jun1, 2009

Presenters

Anthony V. Lupo, IP and Privacy Partner, Arent Fox

- **Is one of the leading Privacy and IP attorneys and was named as the number one IP lawyer by the Washington Business Journal**
- **Represents clients such as Google, Pixar, Apple, LG, Discovery Channel, and Sony on IP and Advertising issues.**
- **Assisted the governments of Indonesia, Egypt and Vietnam is rewriting or implementing their IP laws.**

Patty Eichinger, Regional Director of Finance

- **Over 15 years experience as a property Controller in multiple hotels**
- **Presently overees 22 hotel accounting office s for the largest independent operator of multiple hotel brands in the industry**
- **Over 20 years experience in processing credit card transactions on hotel sites**

Overview

(1) Personally Identifiable Information ("PII") Defined

(2) Collection Portals

(3) Legal Requirements at each Collection Portal

(4) Maintaining Credit Card Data – PCI DSS Compliance

What is Personally Identifiable Information ("PII")?

- Name?
- Address?
- Email Address?
- Username?

Of course!

But are they protected?

It depends …

Home
Groups
Profile
Contacts
Inbox (1)
Applications
Add Connections

Sarah Bruno
ssociate at Arent Fox
hat are you working on?
Your profile is 40% complete [Edit]

Anthony Lupo (1st)

Partner at Arent Fox

Washington D.C. Metro Area | Law Practice

Current	• Partnet at Arent Fox
Education	• Georgetown University Law Center • Howard University School of Law
Connections	29 connections
Public Profile	http://www.linkedin.com/pub/4/340/898

Experience

Partnet

Arent Fox
Law Practice industry
Currently holds this position

Recommend Anthony's work at Arent Fox

Education

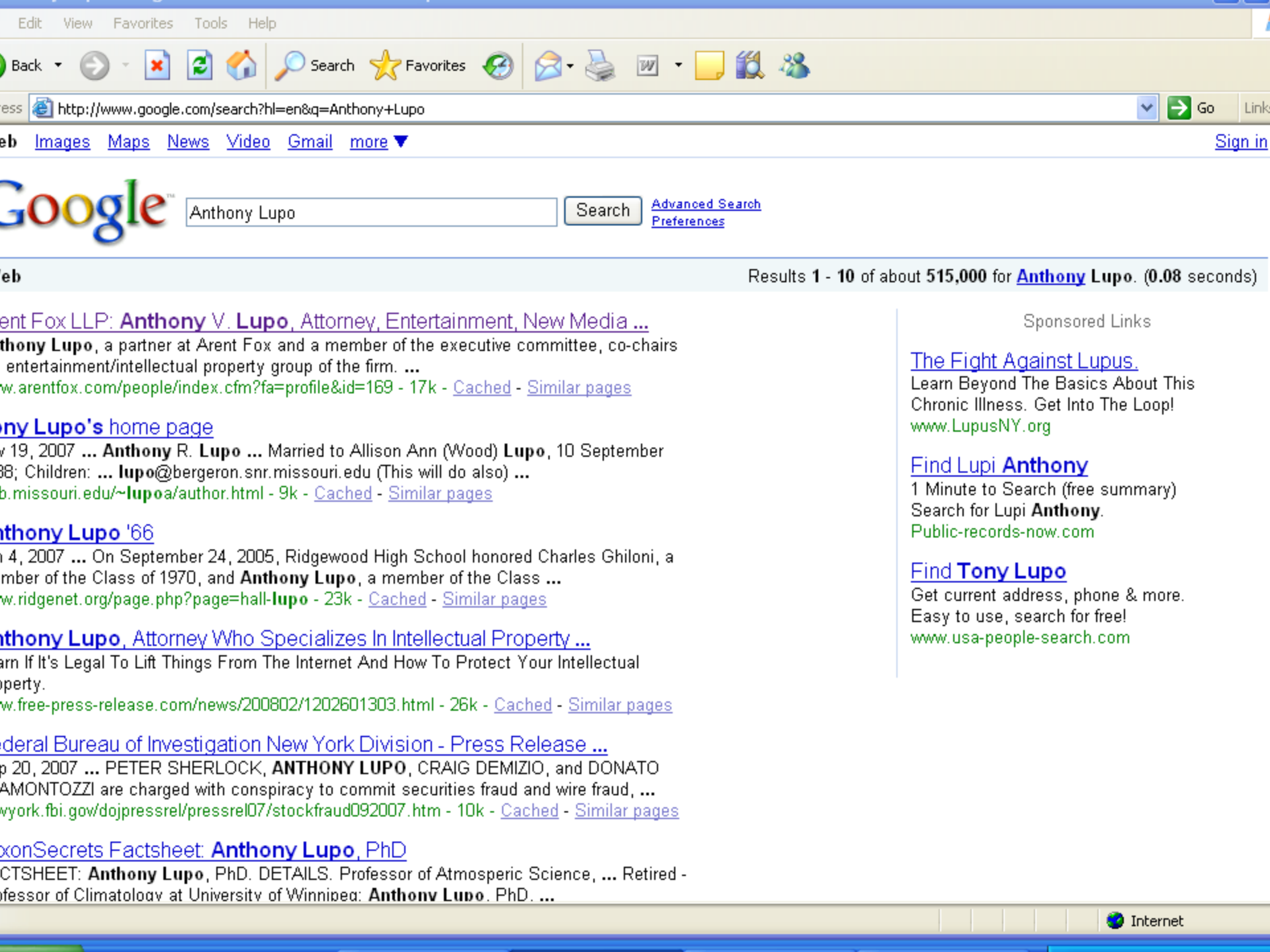
Georgetown University Law Center
LLM, Law
1990 – 1992

Recommend Anthony's work at Georgetown University Law Center

Send a message
Recommend this person
Forward this profile to a connection

Your private info about Anthony

Email & Phone:
avlupo@arentfox.com primary


Edit View Favorites Tools Help
Back Search Favorites
http://www.google.com/search?hl=en&q=Anthony+Lupo
Go
eb Images Maps News Video Gmail more
Sign in
Google
Anthony Lupo
Search
Advanced Search
Preferences
eb
Results 1 - 10 of about 515,000 for Anthony Lupo. (0.08 seconds)
ent Fox LLP: Anthony V. Lupo, Attorney, Entertainment, New Media ...
thony Lupo, a partner at Arent Fox and a member of the executive committee, co-chairs
entertainment/intellectual property group of the firm. ...
w.arentfox.com/people/index.cfm?fa=profile&id=169 - 17k - Cached - Similar pages
ny Lupo's home page
19, 2007 ... Anthony R. Lupo ... Married to Allison Ann (Wood) Lupo, 10 September
88; Children: ... lupo@bergeron.snr.missouri.edu (This will do also) ...
b.missouri.edu/~lupoa/author.html - 9k - Cached - Similar pages
thony Lupo '66
4, 2007 ... On September 24, 2005, Ridgewood High School honored Charles Ghiloni, a
mber of the Class of 1970, and Anthony Lupo, a member of the Class ...
w.ridgenet.org/page.php?page=hall-lupo - 23k - Cached - Similar pages
thony Lupo, Attorney Who Specializes In Intellectual Property ...
arn If It's Legal To Lift Things From The Internet And How To Protect Your Intellectual
operty.
w.free-press-release.com/news/200802/1202601303.html - 26k - Cached - Similar pages
deral Bureau of Investigation New York Division - Press Release ...
p 20, 2007 ... PETER SHERLOCK, ANTHONY LUPO, CRAIG DEMIZIO, and DONATO
AMONTOZZI are charged with conspiracy to commit securities fraud and wire fraud, ...
wyork.fbi.gov/dojpressrel/pressrel07/stockfraud092007.htm - 10k - Cached - Similar pages
xonSecrets Factsheet: Anthony Lupo, PhD
CTSHEET: Anthony Lupo, PhD. DETAILS. Professor of Atmosperic Science, ... Retired -
ofessor of Climatology at University of Winnipeg: Anthony Lupo, PhD. ...
Sponsored Links
The Fight Against Lupus.
Learn Beyond The Basics About This
Chronic Illness. Get Into The Loop!
www.LupusNY.org
Find Lupi Anthony
1 Minute to Search (free summary)
Search for Lupi Anthony.
Public-records-now.com
Find Tony Lupo
Get current address, phone & more.
Easy to use, search for free!
www.usa-people-search.com
Internet

Bruce Springsteen

Become a Fan

Wall | Info | Boxes | Photos

Basic Info

Members:	Bruce Springsteen
Genre:	Rock
Hometown:	Freehold, NJ
Record Label:	Columbia Records

Detailed Info

Website:	http://www.brucespringsteen.net
Current Location:	Freehold, NJ
Biography:	When Bruce Springsteen finally broke through to national recognition in the fall of 1975 after a decade of trying, critics hailed him as the savior of rock & roll, the single artist who brought together all the exuberance of '50s rock and the thoughtfulness of '60s rock, molded into a '70s style. He rocked as hard as Jerry Lee Lewis, his lyrics were as complicated as Bob Dylan's, and his concerts were near-religious celebrations of all that was best in music. One critic became so enamored that... (read more)

What is Protected?

- **Name, email address and Mailing Address?**
  - Consumer should still be given some control over this data.
  - Notice
- **Name, email address, mailing address + Customer Preferences?**
  - Customer should be given some control
  - Notice
- **Name, email address, mailing address + credit card info and/or social security number?**
  - Heightened standard of protection
  - Notice AND security are required by statute

Additional Considerations

Financial Data

- Heightened standard of protection
- Gramm-Leach-Bliley Act
- Notice and Security (at the very least)

Medical Information

- Heightened standard of protection
- HIPAA
- Notice and Security (at the very least)

Collection Portals

- Your Web Site
- Third Party Partner Web Site
- At Check-In
- On site facilities, i.e., restaurants, spas, gym, shops

Legal Requirements for each Collection Portal

Web Site

- **PII at issue:**
  - Name
  - Email Address
  - Mailing Address
  - Credit Card Information
- **Requirements: Notice and Security**

Notice: Privacy Policy

What's Required?

- **What type of information is collected via the Web Site**
  - PII and non-PII
- **With Whom are you Sharing the Data?**
  - Categories of parties
- **Opt-Out options**
- **May a consumer change or delete their information from your servers?**
- **How are you protecting the data?**
- **Effective Date of Policy**

Security of Data

- **New State Laws Requiring Encryption**
  - Massachusetts
  - Nevada
- **Several states require destruction of data after it is no longer needed**
- **Massachusetts also requires the development and implementation of a security program**
- **PCI DSS Compliance**

Legal Requirements for each Collection Portal

Partner Web Site

- **Third party is collecting data and transferring it to you**
  - Name
  - Email Address
  - Mailing Address
  - Credit Card Information
- **Requirements: Notice and Security**
  - Privacy Policy
  - What's Secure?

Security of Data

- **If credit card data is included, encryption of data at transfer.**
- **Can you be liable for the third party's non-compliance?**
  - Possibly!
- **Should have an agreement covering the transfer of data**

Terms of the Agreement

- **Warranty**
  - Permission to transfer the data to you
  - Lawful acquisition of the data
  - Compliance with all laws, including PCI DSS
- **Require encryption at transfer**
- **Third party may want to prohibit your subsequent transfer of data**

Legal Requirements for each Collection Portal

Check-In and On-Site Facilities

- **No notice requirement (offline collection)**
- **Security of Data is still imperative**
  - State laws requiring encryption
  - State laws requiring the destruction of data
- **PCI DSS Compliance**

PCI DSS Compliance

- **Applies to every entity that collects, stores or transmits credit card data**
- **The PCI DSS framework is divided into 12 security requirements which are organized in 6 categories:**
  - Build and maintain a secure network
  - Protect cardholder data
  - Maintain a vulnerability management program
  - Implement strong access control measures
  - Regularly monitor and test networks
  - Maintain an information security policy

PCI DSS Compliance

Compliance Levels

- Level 1: Merchants from whom cardholder data has been compromised and Merchants with more than 6 million credit card transactions annually, across all channels, including e-commerce.
  - Required: Annual onsite PCI data security assessment and quarterly network scans
- Level 2: Merchants with between 1 and 6 million credit card transactions annually.
  - Required: Annual self assessment and quarterly network scans
- Level 3: Merchants with between 20,000 and 1,000,000 credit card e-commerce transactions annually
  - Required: Annual self assessment and quarterly network scans
- Level 4: All other merchants
  - Required: Annual self assessment and quarterly network scans

PCI DSS – Other Considerations

Who else must comply?

- Your service providers? Organizations that process, store or transmit your cardholder data
- Hosts?
- Backup management companies?
- Contractors?

Ensuring Compliance – contractually

- Indemnity
- Warranty of their compliance

Click to add subtitle

Presenters

- Click to add photo

- [Name & Title Here]
- Please include 3 bio points here. Do not write your biography in paragraph format. Only bulleted points will be accepted.
- 3-bulleted bio points per presenter
- Bio info

- Click to add photo

- Patty Eichinger, Regional Director of Finance
- Over 15 years experience as a property Controller in multiple hotels
- Presently overees 22 hotel accounting office s for the largest independent operator of multiple hotel brands in the industry
- Over 20 years experience in processing credit card transactions on hotel sites

FRAUD PREVENTION

IT - Processing

On Site Policy

PCIP compliance:

- Beginning December 09, credit card issuers will start to assess fines and possibly suspend merchant agreements if the data encryption is not certified, firewalls are not certified, and they will require on site certification to win any charge back or fraud disputes.
-

- Fraudulent Transaction Costs are passed on to the merchant in the fee structure :

  Card Present Swipes/ Card not Present

  Volume of transactions

  Age of the Batch Transmittal

  Type of Card

  Chargeback

- Transaction Cycling
  - Visa MasterC ard
  - American Express
  - Discover

- Business Policy
- Privacy

- Business Policy

- Information Technology
  - Interfaces
  - Encryption
  - Firewall
  - File Server Access

- Business Policy

- On Site Transaction Processing
  - Data Storage
  - Data Access
  - Imprinters
  - Settlement Records

- Business Policy

- Electronic Reservations – Card Present
  - Firewalls
  - Encryption
  - Data Storage

- Business Policy

- Reservations without card present / swipe
  - Phone Gaurantee
  - Banquet Functions
  - Advance Deposit
  - Rooming List

- Best Practices

- Pay Pal
- Secure Fax
- Record Retention / Shredding
- Day of Services requirements
- Look up after check out

- Goals
- Card Present – Swipes
- Policy to protect Privacy
- Signature to prevent chargeback
- Firewalls / Data Encryption