Out of Sight, Out of Mind: What You Need to Know about Preventing and Arbitrating Business-to-Business (“B2B”) Data Breaches

March 9, 2017 – 1:00 pm to 2:30 pm ET

PROGRAM SUMMARY

Speakers: P. Jean Baker, Joseph DeMarco, Sandra Jeskie, and Sherman Kahn

Data breaches are now a fact of life. Almost everyone is familiar with breaches that occur when someone gains unauthorized access to consumer data held by a business – the “business-to-consumer” or “B2C” breach. Far less publicized are the “business-to-business (“B2B”) breaches. These breaches often occur quietly and don’t often appear on the front page of the newspaper but are not less important and can have disastrous effects on business. This webinar will provide an analysis of the two kinds of breaches and answer questions that should be of foremost consideration.

AGENDA

1:00 p.m. Welcome and Introduction of Speakers (5 minutes)

1:05 p.m. Data Breaches – B2C and B2B (75 minutes)

• What are the relevant differences between the two types of breaches?
• Why do B2B breaches often raise the same problems as B2C breaches? (Answer: employees!)
• What are some of the domestic and international legal regulations applicable to both types of breaches?
• How can/should business parties reduce/allocate the risk of a computer-based breach when they enter into a contractual relationship?
• Why should parties prefer arbitration over litigation of disputes arising from B2B breaches?
• How can AAA’s online tool (Clause Builder) assist with drafting an effective/efficient arbitration provision?
• What security considerations should lawyers and arbitrators keep in mind during arbitration or litigation of data/cybersecurity disputes?

2:20 p.m. Conclusion and Questions (10 minutes)

2:30 p.m. Evaluation (5 minutes)

2:35 p.m. Adjourn
Ms. Baker provides daily oversight of AAA’s Commercial Division activities in NJ, PA, DE, MD, VA and Washington, DC. Ms. Baker routinely conducts presentations for public and private sector audiences, both domestic and international, on a variety of ADR-related topics, assists large and small businesses with the design and implementation of commercial ADR programs, and serves as a mediator and trainer for AAA on special projects. In addition to authoring numerous articles, Ms. Baker is Co-Editor of the ABA Section of Litigation’s ADR Committee Newsletter, Conflict Management. Ms. Baker has taught ADR courses as an adjunct law professor at Georgetown University and Catholic University. Her inclusion since 1996 as an ADR professional in *Who’s Who in American Law* serves to highlight Mr. Baker’s contributions to the practice and theory of Alternative Dispute Resolution.

Ms. Baker received her Juris Doctor degree from California Western School of Law, a Master of Business Administration from Northeastern University and her Bachelor of Science degree (summa cum laude) from Wright State University.

In addition to her legal background, Ms. Baker held a variety of management positions at the following major corporations: General Electric, Racal Dana, and Fluke Manufacturing. She was included in the Silver anniversary edition of *Who’s Who in American Women* and the Diamond anniversary edition of *Who’s Who in America*.

(June 2011)
Joseph V. DeMarco is a partner at DeVore & DeMarco LLP where he specializes in counseling clients on complex issues involving information privacy and security, theft of intellectual property, computer intrusions, on-line fraud, and the lawful use of new technology. His years of experience in private practice and in government handling the most difficult cybercrime investigations handled by the United States Attorney’s Office have made him one of the nation’s leading experts on Internet crime and the law relating to emerging technologies.

From 1997 to 2007, Mr. DeMarco served as an Assistant United States Attorney for the Southern District of New York, where he founded and headed the Computer Hacking and Intellectual Property (CHIPs) Program, a group of five prosecutors dedicated to investigating and prosecuting violations of federal cybercrime laws and intellectual property offenses. Under his leadership, CHIPs prosecutions grew from a trickle in 1997 to a top priority of the United States Attorney’s Office, encompassing all forms of criminal activity affecting e-commerce and critical infrastructures including computer hacking crimes; transmission of Internet worms and viruses; electronic theft of trade secrets; illegal use of “spyware”; web-based frauds; unlawful Internet gambling; and criminal copyright and trademark infringement offenses. As a recognized expert in the field, Mr. DeMarco was frequently asked to counsel prosecutors and law enforcement agents regarding novel investigative and surveillance techniques and methodologies, and regularly provided advice to the United States Attorney concerning the Office’s most sensitive computer-related investigations. In 2001, Mr. DeMarco also served as a visiting Trial Attorney at the Department of Justice Computer Crimes and Intellectual Property Section in Washington, D.C., where he focused on Internet privacy, gaming, and theft of intellectual property.

Since 2002, Mr. DeMarco has served as an Adjunct Professor at Columbia Law School, where he teaches the upper-class Internet and Computer Crimes seminar. He has spoken throughout the world on cybercrime, e-commerce, and IP enforcement. He has lectured on the subject of cybercrime at Harvard Law School, the Practicing Law Institute, the National Advocacy Center, and at the FBI Academy in Quantico, Virginia, and has served as an instructor on cybercrime to judges attending the New York State Judicial Institute.

Prior to joining the United States Attorney’s Office, Mr. DeMarco was a litigation associate at Cravath, Swaine & Moore in New York City, where he concentrated on intellectual property, antitrust, and securities law issues for various high-technology clients. Prior to that, Mr. DeMarco served as law clerk to the Honorable J. Daniel Mahoney, United States Circuit Judge for the Second Circuit Court of Appeals.

Mr. DeMarco holds a J.D. magna cum laude from New York University School of Law. At NYU he was a member of the NYU Law Review. He received his B.S.F.S. summa cum laude from the Edmund A. Walsh School of Foreign Service at Georgetown University.

Mr. DeMarco is active in numerous professional associations including the:

- International Bar Association (Technology and Litigation Sections);
- American Bar Association, Criminal Justice Committee (Co-Chair, Cybercrime Committee, 2010-2011);
- New York State Bar Association, Commercial and Federal Litigation Section (Co-chair, Internet and IP Committee, 2009-present); and
- New York City Bar Association (Member, Copyright Committee; Past Member, Information Technology Committee).

Mr. DeMarco is a Martindale-Hubbell AV-rated lawyer for Computers and Software, Litigation and Internet Law, and is also listed in Chambers USA: America’s Leading Lawyers for Business guide as a leading lawyer nationwide in Privacy and Data Security. He has also been named as a “SuperLawyer” for his expertise and work in the area of Intellectual Property Litigation. He has published numerous articles and appeared on major news programs in his practice areas; is a member of the Professional Editorial Board of the prestigious Computer Law and Security Review (Elsevier); and serves on the Board of Advisors of the Center for Law and Information Policy at Fordham University School of Law.

Mr. DeMarco has received numerous professional awards, including the U.S. Department of Justice Director’s Award for Superior Performance, as well as the Lawyer of Integrity Award from the Institute for Jewish Humanities. In his spare time he enjoys parenting, golf, and listening to classical piano.
The AAA provides arbitrators to parties on cases administered by the AAA under its various Rules, which delegate authority to the AAA on various issues, including arbitrator appointment and challenges, general oversight, and billing. Arbitrations that proceed without AAA administration are not considered "AAA arbitrations," even if the parties were to select an arbitrator who is on the AAA's Roster.
discovery issues in construction case. Investigation included interviews of counsel, witness and party representatives and resulted in a settlement of the case.

- In re Processed Egg Products Antitrust Litigation (E.D. Pa.) - court-appointed special master to address e-discovery issues in MDL antitrust case. Prepared and filed a written report and recommendation, which was accepted by the Court.

- Appointed to the roster of special masters for electronic discovery by the U.S. District for the Western District of Pennsylvania.

### Alternative Dispute Resolution Training

### Professional Licenses
Admitted to the Bar: New Jersey; Pennsylvania; U.S. District Court: Eastern and Western Districts of Pennsylvania; District of New Jersey; U.S. Court of Appeals: First and Third Circuits. Real Estate License (escrow)

### Professional Associations
International Technology Law Association (Past President); Philadelphia Bar Association (Business Law Section, Past Chair); American Bar Association.

### Education
LaSalle University (BA, Computer Science-1984; MBA, Finance specialization -1991); Temple University School of Law (JD, magna cum laude-1997).

### Publications and Speaking Engagements
Selected Publications
- Miscellaneous other publications

Selected Speaking Engagements
- Speaker, "Arbitration and Mediation in Commercial Disputes: Maximizing Results While Minimizing Costs," Association of Corporate Counsel Delaware Valley In-House Counsel Conference, Philadelphia, Pennsylvania, 2010
- Moderator, Litigation: Cross-border discovery and data protection; Pre-Trial/Arbitration Discovery (US) and Court-appointed Appointed Expert Fact-Finding Procedures (EU) - Use and abuse in technology litigation; ITechLaw Annual European Conference, Berlin, 2010
- Speaker, "Overview of Software Licenses," Pennsylvania Bar Institute, Philadelphia, PA, December 5, 2011
- Miscellaneous other speaking engagements

### Citizenship
United States of America

### Languages
English

### Locale
Philadelphia, Pennsylvania, United States of America

Sandra A. Jeskie, Esq.
Neutral ID : 159311

The AAA provides arbitrators to parties on cases administered by the AAA under its various Rules, which delegate authority to the AAA on various issues, including arbitrator appointment and challenges, general oversight, and billing. arbitrations that proceed without AAA administration are not considered "AAA arbitrations," even if the parties were to select an arbitrator who is on the AAA’s Roster.
Current Employer-Title: Mauriel Kapouytian Woods - Attorney

Profession: Attorney, Arbitrator, Mediator


Experience: Experience with all aspects of complex business litigation with a particular emphasis on intellectual property, information technology and international issues.

Patent litigation and advice regarding technologies including semiconductor processing, communication software, medical devices, memory devices, programmable logic devices, 3D sound technology, construction lasers, video controllers, LCD and Plasma display technology, semiconductor circuit layout and design, telephony and videoconferencing, business systems, LED control, biotechnology, and supercomputer architecture.

Significant experience with Internet Protocol, VoIP, networking and security and encryption software. Significant experience with variety of software patent issues.

Experience with trademark and copyright infringement litigation.

Experienced with trademark and patent issues in apparel industry. Experience in matters involving art and antiquities.

International arbitration proceedings typically involving industrial, mining or IT issues including:
Arbitration in Zurich regarding construction of hot strip steel mill in Brazil;
International IT outsourcing disputes in London and New York;
International arbitration in Denver regarding performance of mining contractor at mine in Bolivia.

Handles litigation and government investigations regarding privacy and information security including data breach, privacy regulation, telemarketing regulation and behavioral advertising issues.

Handles matters in recording industry including privacy issues, intellectual property issues and government investigation of celebrity fan club website.

Practiced in Tokyo, Japan for five years. During that time was licensed as

Sherman W. Kahn, Esq.
Neutral ID: 158907

The AAA provides arbitrators to parties on cases administered by the AAA under its various Rules, which delegate authority to the AAA on various issues, including arbitrator appointment and challenges, general oversight, and billing. Arbitrations that proceed without AAA administration are not considered "AAA arbitrations," even if the parties were to select an arbitrator who is on the AAA’s Roster.
Sherman W. Kahn, Esq.
Neutral ID : 158907

Alternative Dispute Resolution Experience

Sat as panel chair, sole arbitrator, and wing arbitrator in numerous international and domestic arbitrations with subject matter including IT outsourcing, software development, mining, patent infringement and other IP issues, trademark licensing, unfair competition and trade disparagement, and other commercial issues.

Counsel in major international and domestic arbitration proceedings including, for example, a construction dispute regarding a steel mill in South America; international IT outsourcing disputes; and a dispute regarding a South American mining operation.

Other arbitrations have involved issues including semiconductor manufacturing; domain name disputes; a reinsurance dispute; and a variety of commercial issues.

Arbitrated under variety of institutional and ad hoc rules including AAA, ICDR, JCAA, and WIPO.

Mediated numerous commercial disputes.

Alternative Dispute Resolution Training


Professional Licenses

Admitted to the Bar: California, 1993; District of Columbia, 2003; New York, 2004; U.S. District Court: Southern and Eastern Districts of New York; Eastern District of Texas; Western District of Michigan; Central, Eastern and Northern Districts of California; U.S. Court of Appeals: Federal, Second, Ninth, and Eleventh Circuits.

Professional Associations

Chair, New York State Bar Association Dispute Resolution Section (2014-15) (previously Co-Chair Legislation Committee, Co Chair; Arbitration Committee); Co-Chair, Technology Committee, New York International Arbitration Center ; Subcommittee Chair, Task Force on New York Law in International Matters; Fellow, Chartered Institute of Arbitrators (FCIarb); New York Intellectual Property Law Association; California State Bar Association (Intellectual Property Section; International Section); International Arbitration Club of New York; New York City Bar Arbitration Committee; Director, member Tech List, Silicon Valley Arbitration and Mediation Center.

Education

University of California, Berkeley (BA-1989; JD-1993).

Sherman W. Kahn, Esq.
Neutral ID : 158907

The AAA provides arbitrators to parties on cases administered by the AAA under its various Rules, which delegate authority to the AAA on various issues, including arbitrator appointment and challenges, general oversight, and billing. Arbitrations that proceed without AAA administration are not considered "AAA arbitrations," even if the parties were to select an arbitrator who is on the AAA’s Roster.
The AAA provides arbitrators to parties on cases administered by the AAA under its various Rules, which delegate authority to the AAA on various issues, including arbitrator appointment and challenges, general oversight, and billing. Arbitrations that proceed without AAA administration are not considered "AAA arbitrations," even if the parties were to select an arbitrator who is on the AAA’s Roster.
The AAA provides arbitrators to parties on cases administered by the AAA under its various Rules, which delegate authority to the AAA on various issues, including arbitrator appointment and challenges, general oversight, and billing. Arbitrations that proceed without AAA administration are not considered "AAA arbitrations," even if the parties were to select an arbitrator who is on the AAA’s Roster.

*Sherman W. Kahn, Esq.*

*Neutral ID : 158907*
Strategies for Navigating Business-to-Business Data Breaches

There is no shortage of attention in the media to data breaches affecting consumers in the United States—so called “business to consumer,” or “B2C” data breaches. And rightfully so—the Identity Theft Resource Center, which has been tracking data breaches in the United States since 2005, released a report in January 2015 which showed that U.S. B2C data breaches hit a record high of 783 in 2014. This number represents an increase of 27.5 percent over similar breaches reported in 2013, and pushes the total number of U.S. data breach incidents tracked since 2005 to 5,029 reported incidents involving over 675 million estimated records.

For example, in January 2014, Target revealed that it had been the victim of a computer hack through which the contact information of 70 million individuals and information relating to 40 million credit and debit card accounts were stolen. In early 2015, Anthem announced that a cyberattack had compromised the personal information of almost 80 million individuals, including names, dates of birth, Social Security numbers, health care ID numbers, home addresses, email addresses, and employment information.

In large part, it is the number of consumers affected that has led to the increased media onslaught that follows these types of B2C breaches, as well as the call to arms for legislative changes to address these security issues across industries. It is no coincidence that the Obama Administration has made consumer data protection a priority with its proposed data protection act, which will, among other things, require companies to publicly disclose a data compromise within 30 days of it occurring.

In the midst of all this focus on consumer data protection and B2C breaches, however, the media and the Legislature have largely ignored data privacy breaches that are not directly consumer-facing privacy concerns—so-called “business to business,” or “B2B” breaches. Such breaches tend to occur quietly, for two main reasons: (1) there are currently no overarching statutory obligations to report data breaches that do not involve statutorily defined categories of personally identifiable information (PII) belonging to consumers; and (2) it is in a company’s best interest to keep breaches of this nature (really, any breaches at all) quiet, so as to prevent...
the public airing of their potential security flaws.

It is also for these reasons that companies tend not to focus their attention, and their resources, on B2B breach scenarios. It is easy to understand why a B2C breach, which can so directly affect a company’s bottom line in a much clearer and more quantifiable manner through public notification and media involvement, is generally where companies put their best thinking and resources. However, to ignore the potential damage that B2B breaches can cause would be a huge mistake. Indeed, companies can go a long way toward protecting themselves from B2B data breach incidents by implementing two simple, yet critical, measures: (1) retaining expert privacy counsel to perform due diligence on potential business partners and vendors, and (2) ensuring that vendor and other business contracts contain key clauses addressing potential cybersecurity incidents—in particular, arbitration clauses that cover data breaches.

**B2B Breaches**

While it is certainly in neither party’s interest in a B2B data breach to air its grievances publicly, this does not mean that such situations are simple affairs that are quickly and painlessly resolved. In fact, the opposite is most likely the case—without regulatory or statutory parameters to inform the discussion, and without a direct public fallout to steer companies in the right direction, these types of “quiet” breaches can result in very contentious disputes that may drag on and become difficult to resolve.

In one public example of just how far the fallout from a B2B breach can extend, it was reported in March 2014 that a security breach had impacted the e-commerce platform of Createthe Group (CTG), a digital luxury agency that provides e-commerce solutions to a number of recognizable brands in the retail and fashion space, including Calvin Klein, H&M, Hugo Boss, Louis Vuitton, and many more. CTG ultimately retired its e-commerce platform and exited the e-commerce space altogether (although the security breach was not cited specifically by CTG as a reason for this decision). Notably, in this case the security breach resulted in the alleged compromise of credit card numbers belonging to customers of the various brands CTG represented, no doubt one of the reasons why the breach was reported in the press at all.

Even without a public media backlash, however, it is not difficult to imagine how damaging a B2B data breach incident can be to a company. A compromise of a company’s systems, whether through malware received from a vendor or business partner, or through a breach of such a third party’s own security systems, consumes the time, energy, and resources of an organization. Even if no consumer data is impacted by the breach, the impact of a B2B breach can result in tremendous losses to a company, including the costs involved in assessing the breach itself, which often can encompass its impact on the company’s systems and data, determining and implementing solutions necessary to prevent such an incident from future, spending employee and attorney (in most cases, outside counsel) hours interfacing with the third party responsible for the breach, and managing any reputational damage that may have occurred.

**Pre-Contract Due Diligence**

One important step a company should take prior to entering into an agreement with a business partner or vendor is to ensure that these third parties follow robust, industry-appropriate security and privacy protocols. What these protocols should be will vary greatly depending on the industry and the size of the third party in question. As such, it is essential that each company contemplating a third-party business relationship retain outside, expert counsel to guide them in this process. The amount of money at stake in each business relationship and the level of data connectivity that will result between the company and the third party will determine how much due diligence is necessary prior to entering into a contractual relationship.

Smaller, simpler associations may only require a basic review of the third party’s policies and procedures, whereas for more complex and long-term relationships, a more robust
vetting of the third party’s cybersecurity policies and protocols may be appropriate. In all cases, the vetting should be done under counsel privilege to the maximum degree permitted by law.

While such due diligence may, on its face, appear arduous, in fact this type of “pre-screening” not only goes a long way toward preventing a potential external security breach that may affect the company, but also sends a very clear message about the level of importance the company places on cybersecurity matters. This can often be a critical deterrent to a third party that may ordinarily choose to play fast and loose with cybersecurity best practices.  

Contracts and Arbitration

Another key strategy companies can employ in protecting themselves from potential B2B data breaches is to ensure that contracts with vendors and business partners specifically address cybersecurity matters, from preventative measures, to risk allocation and dispute resolution in the event of a data security breach.

As a preliminary matter, contracts should outline the data security procedures and protocols that the third party agrees to comply with. What these procedures should be will, ideally, become clear in the due diligence phase discussed above. Contracts should also address the procedures that should be followed in the event of a security breach and how risk in that context should be allocated.

Specifically, companies should ensure that (1) the third party is contractually obligated to report any security incidents in a reasonably prompt manner to the company; (2) the contract includes a clause allocating risk for certain basic types of data breach incidents; (3) the contract addresses indemnification in the data breach context; and (4) the contract includes a broad-form arbitration clause covering all disputes, including disputes relating to data security and privacy matters, and data breaches in particular.

Arbitration affords parties the ability to elect in advance whether to have the arbitrator (or arbitrators) issue a bare, standard award or a reasoned award, which has implications relating to delay, expense, and susceptibility to vacatur.

An arbitration clause is, in our view, a critical component to handling data security breaches in B2B relationships. There are undoubtedly numerous advantages to companies across various industries that choose to arbitrate rather than litigate, their contractual disputes, regardless of the subject matter of the dispute itself. However, B2B data breach incidents actually present what appears to be the perfect case for the use of arbitration clauses.

First, arbitrating a B2B security incident is more likely to result in a speedier, more efficient, and less costly resolution, not least of all because the evidentiary hearing can proceed uninterrupted, hour-to-hour, on sequential days as needed, as opposed to courtroom proceedings with myriad interruptions and off-days. Additionally, pre-hearing procedures such as discovery and motion practice are streamlined. This frees up company resources to address and rectify the root problems that resulted in the breach, particularly when preceded by mediation, as is generally recommended by the various arbitration associations.

Notably, the efficiency of an arbitration proceeding can be greatly increased by carefully negotiating contractual agreements between parties, such as including a “stepped” arbitration clause, which requires the parties to engage in meaningful mediation prior to entering into a formal arbitration proceeding, and an indemnification clause that covers various security incident scenarios. Here, too, having knowledgeable, expert data privacy counsel to review contracts with third parties for data security issues will go a long way in preventing long and messy disputes when breaches do occur.

Second, an arbitration not only can ensure that legitimate subject-matter expert arbitrators, with all the technical qualifications necessary to understand complex data security and privacy
matters, will resolve the matter, but also eliminates the possibility that an emotional jury, panicking at the prospect of potential effects on consumers from the breach and ill-equipped to comprehend the technical nature of the subject matter, will be the ultimate decision-makers. Additionally, arbitration affords parties the ability to elect in advance whether to have the arbitrator (or arbitrators) issue a bare, standard award or a reasoned award, which has implications relating to delay, expense, and susceptibility to vacatur.

Third, arbitration proceedings can be kept confidential, whereas courtroom proceedings typically cannot be, even if a jury is not involved. This is a key factor for companies navigating a security breach incident, particularly in the current climate of intense scrutiny facing reported breaches. In many cases, it is a tremendous uphill battle to recover from the reputational damage that can result from the public revelation of a data breach, for both parties involved—so much so, that without the option of a confidential arbitration, companies may choose to forgo dispute resolution, swallowing their losses instead. Arbitration provides an ideal environment to ensure that such situations do not arise.

Fourth, arbitration affords far greater finality of decision than court proceedings, where appellate possibilities abound. In data breach disputes, this finality allows both parties to put the dispute behind them quickly, and focus their energies on rectifying the breach and working toward preventing future incidents.

**Top of the Agenda**

Ultimately, in this current environment of record-high breaches and, undoubtedly, record-high scrutiny of companies impacted by breaches, it is in each company’s best interest to put cybersecurity at the top of the agenda, regardless of whether or not consumer data is likely to be implicated in a security incident. Preventive and protective measures can go a long way toward saving a company from catastrophic losses, both financial and reputational.

9. Notably, it is also possible that a B2B or other type of breach will impact certain customer data, but not the types of data that trigger reporting obligations. For example, in New York (and many other states), name, date of birth, and address information, although considered “personal information,” are not, standing alone, “private information” that, if compromised, requires notification of either individuals impacted or governmental agencies. See N.Y. Gen. Bus. Law § 899-aa.
10. Of course, it is also crucial for companies to ensure they have appropriate cybersecurity insurance coverage that will protect them from security incidents prior to entering into contracts with third parties. This is not an easy task—all too often companies purchase expensive products that are peppered with loopholes, either rendering the coverage ineffective even in some of the most basic breach scenarios, or requiring policy modifications in order to become effective. Legal expertise, through outside data privacy counsel, can be critical here to ensure that the most cost-effective, robust policy is purchased, and that it appropriately covers B2B and data breaches.
11. There are a range of reasons why arbitration clauses may be beneficial for all business-to-business matters. While a discussion of those reasons is beyond the scope of this article, we note that broad-form arbitration clauses are, at the very least, procedurally preferable. This is because carving up disputes into different silos for different treatment can be incredibly problematic and inefficient, particularly if parties are forced to arbitrate certain claims and litigate others (and, indeed, to go to court to determine what disputes are covered by the scope of the arbitration clause).
12. For example, under the American Arbitration Association Rules, parties must mediate disputes for claims in excess of $75,000 unless one of them actively opts out of the mediation process. See American Arbitration Association’s Commercial Rules and Mediation Procedures, Rule 9.
Click here to go to the Commercial Arbitration Rules

Click here to go to the Commercial Arbitration Rules
Effective 10/1/13

Click here to go to the Construction Arbitration Rules

Click here to go to the Employment Arbitration Rules

Click here to go to the Labor Arbitration Rules