IN THIS ISSUE:

Introducing Our Latest Additions to the Alston & Bird Litigation Practice
*An interview with five of the firm’s newest litigation partners*

What Is Reasonable Security? Steps Companies Can Take Now to Avoid Enforcement Actions
*By Kimberly Peretti and Dominique R. Shelton*

The Supreme Court’s Class Action Certification Trilogy
*By Cari K. Dawson and David Venderbush*

The Next Wave of Employment Litigation: The Recent Increase in Employment-Related Fair Credit Reporting Act Class Actions
*By Lisa H. Cassilly and Brett E. Coburn*

The Business Judgment Rule After *FDIC v. Loudermilk*
*By Steven M. Collins, Robert R. Long, and Brian D. Boone*

Export Control Reform: Enforcement Trends Build Higher Walls Around Fewer Items
*By Jason M. Waite and Diego Marquez*
Trends features updates on key legal issues and highlights Alston & Bird’s broad and diverse litigation practices.

In this edition, Kyle Wallace of our Litigation & Trial Practice Group interviews five litigation partners who have recently joined Alston & Bird – Brett Jaffe in New York, Dominique Shelton in Los Angeles, Gregg McDougal and Mike Kaeding in Raleigh, and George Abney in Atlanta. These talented and accomplished attorneys bring additional depth and breadth to our team. In addition, Kim Peretti and Dominique Shelton of our Litigation & Trial Practice Group discuss the red-hot issues of data privacy and cybersecurity and offer proactive steps that companies can take to protect themselves and their customers from data breaches and avoid enforcement actions and lawsuits. Cari Dawson of our Litigation & Trial Practice Group and David Venderbush of our Products Liability Group then analyze a trio of recent Supreme Court decisions in Walmart Stores v. Dukes (2011), Comcast v. Behrend (2013), and Halliburton v. Erica P. John Fund (2014) that are transforming class action litigation in federal court. Lisa Cassilly and Brett Coburn of our Labor & Employment Group address the recent wave of class actions alleging Fair Credit Reporting Act violations in connection with running background checks on job applicants and employees, and offer practical suggestions to employers for complying with the FCRA and avoiding such litigation.

Next, Steve Collins and Brian Boone of our Litigation & Trial Practice Group and Robert Long of our Securities Litigation Group join together to discuss the business judgment rule, its application to bank and corporate directors and officers, and a recent landmark decision by the Georgia Supreme Court in a case that they handle. Lastly, International Trade attorneys Jason Waite and Diego Marquez address recent reforms in the U.S. export control system, including the Export Control Reform Initiative and how the new rules will likely impact enforcement trends.

Our Winter 2015 edition of Trends is filled with a variety of short articles addressing interesting and timely topics. We hope you enjoy reading it, and as always, we value your comments.
Introducing Our Latest Additions to the Alston & Bird Litigation Practice

Our Trends co-editor, Kyle Wallace, a partner in the Atlanta office, recently sat down with several of the most recent lateral partners to join the Litigation Group to discuss their practices, why they joined Alston & Bird, and some trends they see in their respective practice areas. Joining Wallace were Dominique Shelton, Litigation & Trial Practice partner in Los Angeles; Brett Jaffe, Litigation & Trial Practice partner in the New York office; George Abney, Tax partner in the Atlanta office; and Gregg McDougal and Mike Kaeding, Litigation & Trial Practice partners in Raleigh.
Kyle Wallace: Thank you all for participating and making time this afternoon to tell us and our clients more about you and your practices. We are so glad to have each of you at Alston & Bird. So we can all get to know you a little better, please tell us about your practices and when you joined the firm. Dominique, let’s start with you.

Dominique Shelton: My practice focuses on helping companies navigate the thorny privacy issues associated with digital marketing and advertising through mobile apps, websites, and social networking sites. On the litigation front, I focus on complex commercial litigation, with particular attention to privacy litigation, intellectual property, unfair competition, and antitrust matters. Given the rash of high profile privacy matters over the past several years, many companies want to focus on litigation avoidance and compliance as a key strategy to avoid regulatory enforcement and class actions. In that respect, I also provide strategic digital marketing and privacy compliance counseling on cutting edge issues, such as mobile apps, the Video Privacy Protection Act, Big Data, and behavioral advertising. I joined the firm in June 2013.

Brett Jaffe: I joined Alston & Bird in June 2014. I’m a litigator, and my practice focuses on complex corporate and commercial disputes; shareholder, securities, and derivative litigation; and corporate control and M&A litigation. I have significant experience representing what I’d refer to as “Wall Street clients” – hedge funds, private equity funds, broker-dealers, investment advisors, and other entities in the securities business. I represent those clients in actual securities litigation, such as prosecuting or defending claims arising out of the federal securities laws, as well as disputes involving securities products and transaction-related litigation. The remainder of my civil practice involves representing corporate and individual clients in litigation matters throughout the country, in federal or state courts, or in ADR proceedings, and across various industries like real estate, airlines, construction, energy, media, and many others. In addition to my civil practice, I also frequently represent corporate and individual clients in connection with government investigations, including those by the SEC, CFTC, and DOJ, and internal, board, and audit committee investigations.

George Abney: As I tell folks, “I fight the IRS.” I represent clients in all phases of civil and criminal tax disputes. In the civil arena, I represent clients during IRS audits, the IRS administrative appeals process, and litigation in the U.S. Tax Court, the U.S District Courts, and the various appellate courts. In the criminal arena, I represent clients facing IRS criminal investigations, grand jury investigations, and criminal jury trials and appeals. I have represented clients in civil and criminal tax matters ranging from individuals, to closely held businesses, to public corporations. I began my legal career as a Trial Attorney with the Tax Division of the U.S. Department of Justice. I joined Alston & Bird in October 2013.
Gregg McDougal: I joined Alston & Bird in January 2014. I am a trial lawyer who represents plaintiffs and defendants in a wide range of litigation matters. My practice consists primarily of complex commercial litigation disputes, and I occasionally handle catastrophic personal injury matters, recovering over $75 million for these clients in the last 15 years. I have represented large corporations from all industries, including hospitality, heavy manufacturing, telecommunications, commercial and residential flooring, automotive products, and commercial real estate in complex commercial disputes throughout the United States. I recently handled an ICC matter in Japan on behalf of a pharmaceutical company. I have also successfully defended numerous directors and officers in cases filed throughout the country.

I also have been lead counsel in numerous high-profile cases and represented a number of well-known clients, including an Olympic gold medalist in a defamation suit; three of the all-time greatest golfers in a complicated case involving photographs and forged autographs; a well-known football coach after he was terminated by a large university; and a Malaysian corporation in a breach of contract action against a popular country singer-songwriter and actor.

Mike Kaeding: Like Gregg, I joined Alston & Bird in January 2014. I have a broad litigation practice that covers a wide range of complex civil and white collar criminal matters. Over the course of my 17-plus years practicing law, I have handled just about every type of complex dispute that can arise in civil litigation and have represented both plaintiffs and defendants. I also have defended individuals and corporations in investigations and enforcement matters involving a number of government entities, including state attorneys general and the DOJ, SEC, OCC, FINRA, FDIC, CFPB, CPSC, NHTSA, and FDA. I have significant trial experience and have litigated cases throughout the country and internationally.

Wallace: You've all had accomplished careers prior to coming to Alston & Bird. Tell us what enticed you to join us.

“I was attracted to the breadth and depth of the practices. My clients frequently have needs that go beyond litigation.”

Jaffe: I was drawn to the firm by the lawyers I now count as my partners and colleagues. Alston & Bird is a firm full of incredibly talented, creative, and business-savvy counsel who are truly committed to serving their clients—while also being really fun people to work with. Beyond the people, I was attracted to the breadth and depth of the practices. My clients frequently have needs that go beyond litigation. For example, they might need help with a corporate transaction or IP issue, or guidance on the broker-dealer regulations. I felt—correctly, I think—that I would benefit from a platform that could meet my clients’ broader needs. By the same token, I was drawn to the opportunity to help the firm’s existing clients
solve their problems. Finally, I enjoy the flexibility Alston & Bird gives me with my engagements. It is important to me that I am able to represent both plaintiffs and defendants and that I have flexibility to develop fee arrangements that make sense for the particular client and matter involved.

**Kaeding:** I joined Alston & Bird because of the strength of its litigation practice. Over the course of my career, I had the privilege of working alongside Alston & Bird attorneys in a number of antitrust, financial services, and government investigation matters. I came away from those experiences extremely impressed with the lawyers and the firm. The firm’s litigation department has the bench strength and experience to field an extremely formidable team to handle any type of litigation or investigation matter in any part of the country. The firm has an extremely strong group of real trial lawyers who have consistently proven their advocacy skills by successfully trying cases to verdict. That is very important to me. For example, the firm’s trial lawyers recently secured a $106.7 million dollar verdict in New York federal court. And, here in North Carolina, the firm won the largest jury verdict in the state’s history—$318 million.

**Shelton:** Alston & Bird represented a confluence of strengths in a platform that I was looking for: best-in-class lawyers with expertise ranging from privacy, class actions, IP, regulatory, and government contracts. On top of this, it meant a great deal to me to learn that the firm has been ranked as one of the “100 Best Companies to Work For” by Fortune for 15 consecutive years. This means that there was the opportunity to work with incredible lawyers in an atmosphere that is collaborative and that places the client first.

**McDougal:** Mike and I joined Alston & Bird for similar reasons—the strength of the firm’s litigation practice, both nationally and in the Southeast. I was also particularly attracted to the firm because of its rising national reputation and its quality leadership and firm culture. Obviously, my new colleagues here have experienced the same features that all drew us to this firm.

**Abney:** For my part, Alston & Bird has a great reputation in the legal community and has one of the largest tax practices in the U.S. And, similar to what Brett said, because Alston & Bird is a full-service law firm, I am able to serve all of my clients’ legal needs. Beyond the firm’s services, the culture here makes it a great place to work. Everyone—from the file clerks to the senior partners—is valued and treated with respect. That creates an atmosphere of cooperation and camaraderie. Having been with the firm for over a year now, I find myself asking, “Who wouldn’t want to practice here?”

**Wallace:** We’ve been talking about the past for a bit; now, let’s move ahead to the future. What trends do you see in your practice areas and what would you tell our clients to do to be prepared for these developments?

**Jaffe:** Businesses are facing closer scrutiny than ever before—from shareholders, business partners, and of course, the government. I think it is important for clients to think proactively about the litigation and regulatory risk that may arise from a particular course of conduct and to evaluate those risks long before a lawsuit is commenced or SEC subpoena arrives at the door. But at the same time, there is the opportunity for clients to use litigation offensively to enforce their rights and maximize return on their investments. This is especially true in the hedge fund and private
equity space where I spend a lot of my time. From distressed investments or private equity deals gone awry, to activist situations, clients should regard litigation as a tool which can be used effectively to advance their businesses.

**Abney:** In the past decade, the IRS and the Justice Department have become increasingly more aggressive in their tax enforcement efforts. Audit and investigative techniques that were once prohibited or frowned upon have now become commonplace. For example, the IRS once prohibited simultaneous civil and criminal investigations of the same taxpayer. Now, however, the IRS fully endorses “parallel” civil and criminal tax investigations and prohibits civil auditors from telling taxpayers that they are also under criminal investigation. Also, the IRS and the Justice Department have become much more aggressive in challenging privilege claims, from the attorney-client privilege to the Fifth Amendment privilege against self-incrimination. With the IRS becoming more and more aggressive in its tax enforcement efforts, it is increasingly important for taxpayers—both big and small—to seek legal representation at the beginning stages of a tax dispute. When a client receives an audit letter from the IRS, in most cases their first inclination is to call their accountant. In this aggressive era of tax enforcement, their first inclination should be to call their lawyer.

**Kaeding:** My practice is broad, but let me highlight two important trends that I see. First, privacy and data security issues pose significant and growing compliance and litigation risks across industries. Companies face increasingly complex state and federal requirements governing privacy and data security, and at the same time, third-party attacks are becoming more persistent and sophisticated. Our clients must navigate this perfect storm of regulatory and data breach threats or face the risk of government investigations and private litigation. We can assist them with this process by creating data protection compliance programs, revising existing data privacy processes, and conducting security assessments subject to the attorney-client privilege. When the need arises, our world-class litigators and privacy/data security experts can defend the complex class action litigation and regulatory investigations that inevitably result from accusations that a company has violated applicable laws protecting the privacy of consumer or health care information.

Second, in the financial services area, the DOJ, the CFPB, and OCC regulators have indicated they will be aggressively targeting fair lending and mortgage pricing and servicing practices, including loan modifications for struggling borrowers. Here, too, our clients must proactively assess their compliance practices and protocols throughout the affected areas. We can assist with evaluation of existing compliance processes and implementation of necessary revisions in a manner subject to the attorney-client privilege. When necessary, our financial services litigators can defend regulatory investigations and enforcement activities and any private, piggyback class action litigation that might arise from the alleged violations.
Shelton: I agree with Mike. Privacy is obviously an incredibly active area of law, but one good example is mobile apps. There are more than 1,600 mobile apps uploaded into app stores every day by more than 140 million smartphone users in the United States. As people increasingly shop for products, search the Internet, and make decisions through their mobile devices, the issues concerning best practices for privacy and e-commerce involving digital advertising on a mobile platform are front and center. Further, mobile apps cut across industries, including financial and health care, and are subject to different types of law—not just IP or privacy. For example, there are currently more than 38,000 health and fitness apps and more than 24,000 medical apps available today. California’s Confidentiality of Medical Information Act was amended effective January 1, 2014, for example, to add mobile app developers to the definition of “providers of healthcare.” This is important to understand as the Act provides for civil penalties of up to $250,000 per violation. In 2013, there were four regulatory guidance reports regarding privacy disclosures and mobile apps from the California State Attorney General, the FTC, the Department of Commerce NTIA, and the Article 29 Working Group.

In recent months, particular regulatory focus has been placed on behavioral tracking data gathered through mobile apps. Recently, on December 9, 2014, a coalition of 23 global privacy authorities (including the FTC) called upon several companies to modify their app marketplaces to include easy access to their privacy policies before users download apps. A “mobile sweep” conducted earlier in 2014 revealed that of the 1,200 most popular mobile apps available in app stores, many appeared to collect consumers’ personal information but failed to include any upfront privacy disclosures. The plaintiff’s bar has picked up on these developments domestically, filing some 12 class actions involving mobile apps over the past 13 months. In addition, the FTC has issued two very important mobile app privacy enforcement consent orders.

A main focus of my practice is counseling clients in best practices for staying on top of and out in front on the critically important and continually evolving issues in the privacy area. When lawsuits are filed, our team is ready to defend our clients’ interests, not only on tackling the legal issues, but by focusing on their overall business concerns and objectives.

McDougal: While litigation generally continues to trend upward, litigation spending remains affected by the recent economic downturn. As a consequence, clients are requesting more than ever before that law firms consider alternative fee arrangements that are tailored to the specific engagement and provide for better cost certainty. For both lawyer and client, this requires a sophisticated and proactive approach to analyzing litigation matters and determining the best path forward. It also requires honest and constant communication. Fortunately, Alston & Bird has been an industry leader in partnering with its clients to find fee arrangements that are tailored to their specific legal needs.

Wallace: Those are very helpful insights. Thank you again for taking a few minutes out of your day to discuss your practices and share your thoughts on some of the trends that you are seeing and anticipate for the coming year. Welcome again to the firm.
What Is Reasonable Security? Steps Companies Can Take Now to Avoid Enforcement Actions and Class Actions in the Future

By Kimberly Peretti and Dominique R. Shelton

Privacy, data, and cybersecurity are in the news. It seems just about every day a major company is learning that data on its servers, clouds, or data management platforms have been hacked. As the threat of hacking from domestic and, increasingly, foreign sources continues to rise, companies that have been victimized by a data breach are finding themselves on the other side of regulatory investigations, class action lawsuits, and attacks on their boards of directors. The crux of these complaints centers around the elusive concept of “reasonable security” often analyzed from the rearview mirror of the time period after a breach occurs. Further, California has amended its data breach law again (effective January 1, 2015) to include a separate category of companies responsible for security referred to as “maintainers” of personal information.
So how can companies develop a robust data security plan that covers data collected through websites, contests, sweepstakes, and most importantly in recent months, mobile apps? What are the red flags companies have encountered in Federal Trade Commission (FTC) investigations? And what strategies best position a company for arguing that they have met reasonable security standards based upon established precedent in the form of prior cases and FTC enforcement actions?

What Is a Data Security Program and How Can Companies Develop One?

Increasingly, after a data breach, regulators (and courts) ask what has the company, including its board of directors and officers, done to protect against cyber-theft? Companies should be proactive in assessing and mitigating their risks. If they have not already done so, companies should consider developing a data security plan for protecting personal information and customer data.

The cornerstone of plan development begins with an enterprise-wide security risk assessment to understand (1) what information companies are collecting, (2) where it is stored, (3) what vulnerabilities and risks exist, and (4) mitigation steps to prevent loss. Not only is such a risk assessment the cornerstone for increasingly accepted data security plan development recommended by the National Institute of Standards and Technology (NIST) and other frameworks, it is a requirement under Massachusetts law for companies that collect personal information from Massachusetts residents.\(^1\)

\[\text{“The cornerstone of plan development begins with an enterprise-wide security risk assessment.”}\]

A necessary step of developing a risk assessment is to understand where personal information, and in certain instances business-critical information, resides on your company’s systems. While regulatory enforcement for data breach has focused on personal information, companies may also wish to take care that they know where trade secrets and business-critical data reside. In at least one case, a court held that a company did not take sufficient steps to maintain confidentiality of its trade secrets since it did not treat its own trade secrets with the level of security it treated personal information covered by privacy conventions.\(^2\)

Finally, companies should develop a data breach response plan that clearly delineates, among other items, which internal and external resources (such as outside counsel, vendors, and insurance) will be contacted in the event of a breach and identifies (by name and role) the different company stakeholders’ responsibilities. The plan should be tested for efficacy using a table-top exercise, a service that Alston & Bird provides.\(^3\)

---

\(^1\) 201 Mass. Code Regs. § 17.03(1).


\(^3\) For more details, see Alston & Bird’s Cyber Risk Legal Package, described on our website at http://www.alston.com/resources/cyber-risk-legal-package/.
Red Flag for Cyber Security in 2015 – Mobile Devices and Apps

Companies that collect personal information via mobile devices or apps should take special care to ensure that adequate attention has been paid to security. One recent FTC enforcement action, In re HTC America, Inc., No. 122 3049 (F.T.C. June 25, 2013), Docket No. C-4406, is worth noting.

In its complaint, the FTC alleged that HTC failed to employ reasonable security measures, many of which were straightforward and inexpensive to implement, in the customization of its mobile devices. The FTC claimed that a number of HTC practices exposed its mobile devices to security vulnerabilities, including:

- HTC introduced numerous “permission re-delegation” vulnerabilities through its custom, pre-installed applications.
- HTC devices contained programming flaws that would allow third-party applications to bypass Android’s permission-based security model.
- HTC failed to use readily available and documented secure communications mechanisms in implementing logging applications on its devices, placing sensitive information at risk.
- HTC failed to deactivate a debug code before its devices shipped for sale to consumers. As a result, sensitive information ended up in the system log and was accessible to third-party applications.
- HTC made representations to consumers in its user manual and user interface that consumers’ information would be secure.

The FTC relied on both prongs of its powers under Section 5 of the FTC Act in the complaint. In Count 1, the FTC alleged an unfair practice. The FTC complaint alleged that HTC’s failure to employ reasonable and appropriate security practices in the design and customization of the software on its mobile devices was an unfair act or practice.

“Companies that collect personal information via mobile devices or apps should take special care to ensure that adequate attention has been paid to security.”

Counts 2 and 3 alleged a violation of the FTC Act for “Deceptive User Manual and User Interface.” The complaint alleged that HTC’s representations to consumers in its user manual and user interface that they would be notified when a third-party application accessed their information constituted a deceptive practice under Section 5(a) of the FTC Act in light of the aforementioned vulnerabilities.

The FTC concluded that the conduct alleged in the complaint constituted either an unfair or deceptive act or practice and therefore violated of Section 5(a) of the FTC Act. The parties ultimately stipulated to a Decision and Order that will continue until 2033. Decision and Order, In re HTC America, Inc.

With regard to mobile apps that permit e-commerce, the FTC recently found that a mobile app publisher had failed to provide reasonable security because it (1) overrode the default SSL certificate validation settings provided by the iOS APIs, (2) failed to appropriately test, audit, assess, or review its applications, and (3) failed to maintain an adequate
What Is Reasonable Security?

process for receiving and addressing security vulnerability reports from third parties.

By overriding the default validation process, the company allegedly undermined the security of purchases made through its app, exposing consumers’ credit card details, including card number, security code, ZIP code, expiration date, and consumers’ email addresses and passwords.4

“The FTC has sought enforcement against companies for failing to implement ‘reasonable security,’ but the FTC has not promulgated new guidelines on what constitutes ‘reasonable security.’”

Despite the fact that its recent decisions have sought enforcement against companies for failing to implement “reasonable security,” the FTC has not promulgated new guidelines on what constitutes “reasonable security.” Instead, the FTC in recent public statements has directed companies to review prior FTC guidance, complaints, and enforcement orders to understand the parameters of reasonable security.

California’s Amended Data Breach Law Went into Effect on January 1, 2015, Imposing New Obligations for Companies to Implement Reasonable Security

On September 30, 2014, California Governor Jerry Brown signed Assembly Bill 1710, which changed California’s existing data security law effective January 1, 2015. The new law requires businesses that “maintain” personal information on California state residents to adopt reasonable security procedures to protect personal information (a requirement that previously only applied to businesses that own or license such data).5

What Can Companies Do to Understand the Parameters of Reasonable Security?

For the most part, regulators seem to take the position that “reasonable security” will be evaluated on a case-by-case basis. To the degree regulators like the FTC have encouraged companies to review past enforcement orders and guidance to glean reasonable security, companies should do so. The FTC’s recent decision not to pursue an enforcement action against Verizon after it developed a plan to address the use of outdated encryption is an example of the benefit for companies in taking a proactive approach.

To assist in these efforts, Alston & Bird has created an update to our Cyber Risk Legal Package that reviews practices the FTC has found to be inadequate in the past and other prac-

---


5 For a full discussion of the law, see Alston & Bird’s advisory “California Governor Signs New Data Breach Law” (September 30, 2014).
tices the FTC has hailed as a best practice. Similarly, Alston & Bird’s Cyber Risk Legal Package includes a checklist and guidance for privacy practices in Big Data, mobile, video privacy, and children.

“Alston & Bird has created an update to our Cyber Risk Legal Package that reviews practices the FTC has found to be inadequate in the past and other practices the FTC has hailed as a best practice.”

Conclusion
In this fast-paced era, where companies can instantaneously find their brands (and their data) in the news, it is incredibly important to take a proactive, forward-looking approach to explore what steps can be taken now to implement best practices before a hacking event occurs.6

6 The team of experienced attorneys in Alston & Bird’s Privacy & Data Security Group offers compliance counseling to our clients before a breach and also works closely with the Class Action team to achieve favorable results for clients after a breach has occurred.
What Is Reasonable Security?

About the Authors

Kimberly Peretti

Kim Peretti is a partner in the firm’s White Collar Crime Group and co-chair of our Security Incident Management and Response Team. Ms. Peretti is also a former director of the cyber forensic service practice at PricewaterhouseCoopers and a former senior litigator for the Department of Justice’s Computer Crime and Intellectual Property Section. She focuses her practice on managing complex, technical electronic investigations and responses, often resulting from cyber intrusions and data breaches. She also counsels a wide range of clients in matters of cybersecurity, privacy, financial crime, fraud and regulation, payment systems compliance and risk mitigation, economic espionage, and intellectual property theft.

While at the Department of Justice, Kim led several benchmark cybercrime investigations and prosecutions, including the prosecution of the infamous TJX hacker Albert Gonzalez, currently serving 20 years in prison for his role in the largest hacking and identity theft case ever prosecuted by the department.

Dominique R. Shelton

Dominique Shelton is a litigation partner in Alston & Bird’s Los Angeles office. She focuses her practice on complex commercial litigation, with particular attention to privacy litigation, intellectual property, unfair competition, and antitrust matters. Dominique also provides strategic digital marketing and privacy compliance counseling on cutting edge issues, such as mobile apps, the Video Privacy Protection Act, Big Data, and behavioral advertising. In 2012, she was named Intellectual Property Lawyer of the Year by the Century City Bar Association. In 2014, she was named one of the Most Influential Lawyers: Digital Media and E-Commerce Law by the Los Angeles Business Journal. In 2014, The Recorder named her as a Leader in Technology Law.

She has litigated matters involving state and federal laws and has negotiated with the California AG and the FTC. Dominique represents Fortune 500 companies, start-ups, and privately held companies across a broad spectrum of industries that includes media, entertainment, technology, broadcasting, digital sales, marketing, advertising, wireless/mobile, Internet, health care, e-commerce, software, telecommunications, and health and beauty.
The Supreme Court’s Class Action Certification Trilogy

By Cari K. Dawson and David Venderbush

A trifecta of recent U.S. Supreme Court opinions has decisively transformed Rule 23 class certification from a pleading proceeding to a proof proceeding. The class certification hearing, post-trilogy, will essentially become a bench trial. To oppose plaintiff’s motion for class certification, persuasive legal argument alone may no longer be sufficient. Companies must develop a robust and comprehensive evidentiary record that is both admissible and persuasive. Is your company ready to defeat class certification in the post-trilogy world?

The first section of this article explains how the Supreme Court has transformed class proceedings in three recent decisions. The second half addresses the practical implications of that trilogy and suggests best practices for corporate counsel whose companies are targeted in class action litigation.
The Trilogy

It began in 2011 with *Wal-Mart Stores v. Dukes*, essentially an evidentiary sufficiency decision. The *Wal-Mart* majority announced that “Rule 23 does not set forth a mere pleading standard,” but requires “[a] party seeking class certification” to “affirmatively demonstrate his compliance with the Rule—that is, he must be prepared to prove that there are *in fact* sufficiently numerous parties, common questions of law or fact, etc.” The Court analyzed plaintiffs’ commonality evidence and found that it fell “well short.”

“The [Dukes] Court implicitly authorized a class certification battle of the experts over whether certain public statements had any impact on the trading price of a company’s stock.”

Two years later, *Comcast v. Behrend* again assessed plaintiffs’ certification evidence, this time on the Rule 23(b) predominance factor. Applying “[t]he same analytical principles” to proof of predominance, the Court reversed class certification because the trial and appellate courts had not rigorously analyzed whether the plaintiffs’ damages evidence was sufficient to prove predominance of common issues regarding damages. The Court conducted its own analysis of the damages model and held that the model could not prove class-wide damages because the expert did not connect it to the plaintiffs’ only viable liability theory.

And this year *Halliburton v. Erica P. John Fund* has further confirmed the necessity of class certification evidence. That case identified the class certification stage as the arena for plaintiffs to meet their burden of proving each of the prerequisites for the “fraud-on-the-market” reliance presumption, and for defendants to rebut the presumption with “direct, more salient evidence.” By highlighting the plaintiffs’ submission of an “event study” in support of certification and describing a hypothetical response by defendants based on their own event study, the Court implicitly authorized a class certification battle of the experts over whether certain public statements had any impact on the trading price of a company’s stock. Such evidentiary battles will certainly be a feature of securities class certification motions for the foreseeable future.

The Supreme Court explicitly identified *Halliburton* as consistent with its prior directives in *Comcast* and *Wal-Mart* that the Rule 23 certification prerequisites be proven, not merely pled, by plaintiffs. And *Wal-Mart* relied on the first *Halliburton* Supreme Court decision, citing “class action suits for securities fraud” as “the most common example” of having to “prove” the same issue both at the merits stage and “at the Rule 23 stage.”

With this trilogy of evidentiary cases firmly in place, class certification proceedings will now become more complicated and expensive, and look more like trials, which are also about presenting a party’s evidence. While few class actions get to trial, the Supreme Court has decreed that the critical proof proceeding is class certification.
Best Practices for Discovery

Pre-trilogy and even today, some practitioners advocate bifurcation of class and merits discovery. Many companies attempt to limit the scope of discovery, and understandably so, given the cost expended on electronic discovery and the risk that confidential trade secrets will be subject to production and public disclosure. With plaintiffs’ use of discovery as a weapon and the constant threat of sanctions looming, it is not surprising that many companies seek to limit discovery.

It is vital that a company develop its affirmative story by defining the issues and identifying facts supporting its themes, arguments and experts.”

Post-trilogy it is clear the Rule 23 analysis will frequently “overlap with the merits of the plaintiff’s underlying claim” because a “class determination generally involves considerations that are enmeshed in the factual and legal issues comprising the plaintiff’s cause of action.” That language (from Wal-Mart) coupled with the requirement of evidentiary proof, gives plaintiff’s counsel a sound basis for opposing bifurcation of class and merits discovery. And it often will be in the company’s best interest to be able to raise merits issues to oppose class certification. Attacking the class representatives’ individual claims through summary judgment, utilizing class experts and rebutting plaintiffs’ class experts through strategic Rule 702 (Daubert) motions, and refuting a plaintiff’s class trial plan as running afoul of the Rules Enabling Act and other due-process arguments are strategies that are enhanced by intertwining merits arguments relevant to the class determination.

This does not mean that defendants should always pursue or acquiesce to broad discovery pre-class certification. But defendants should resist the knee-jerk reaction to automatically bifurcate discovery. We advocate strategic case management and scheduling orders that prioritize the legal and factual issues that will support the defense’s litigation strategy. For example, a company should consider advocating a case management and scheduling order that prioritizes discovery regarding issues such as standing, injury-in-fact, causation and the proof necessary to establish the elements of plaintiffs’ causes of action. A company should provide the court with an explanation of why certain discovery should be prioritized and the case, regardless of whether the discovery is for class or merits issues.

Developing the Company’s Affirmative Story

It will no longer be enough for a defendant to argue in a brief or at a hearing that a class is heterogeneous, and dissimilarities within the class impede the generation of common answers in a class-wide proceeding—or neither liability nor damages are susceptible to common proof. A company must prove why a class cannot be certified through compelling and persuasive evidence—factual and expert. To win class certification post-trilogy, the facts are equally if not more important than the law, and that evidence must be admissible and credible.

Discovery propounded by plaintiffs’ counsel is focused on eliciting documents and deposition testimony supporting plaintiffs’ theory of
the case, so it is vital that a company develop its affirmative story by defining the issues and identifying facts supporting its themes, arguments and experts. The sources of these factual arguments include, but are not limited to, current and former company witnesses, internal company documents and databases, third-party witnesses and documents, named class representatives, unnamed class members and expert testimony, research, and studies.

An affirmative story and factual argument strategy must be conceptualized, managed and executed by the company. Focus groups can aid in testing affirmative themes not only on juries but also on the judge. Defendants should also consider presenting a tutorial for the judge on complicated or complex factual or technical issues. A tutorial will benefit defendants by educating the judge on key issues in advance of her rulings on critical motions. Finally, defense counsel should vet and test company experts to ensure that they can withstand a Rule 702 challenge and are articulate, credible and good on their feet at an evidentiary hearing.

**Legal Challenges to Class Certification**

Of course, legal challenges to class certification will still be appropriate. But post-trilogy, defendants must broaden their arguments beyond the formal Rule 23 criteria, and combine those arguments with practical challenges that force plaintiffs to explain—and the trial court to consider—precisely how a class trial can proceed in a legally permissible manner. The trilogy highlights arguments tying legal requirements of due process and the Rules Enabling Act to the practical aspects of class trial. The Rule 23 factors do not exist in a vacuum, but must be tied to how plaintiffs would prove their causes of action at trial.

“Defendants must ... combine [their Rule 23] arguments with practical challenges that force plaintiffs to explain ... precisely how a class trial can proceed in a legally permissible manner.”

It is not enough to simply file a brief in opposition to class certification. Defendants must first require a plaintiff to submit a trial plan and then insist on the opportunity to refute. Attacking trial by formula, ascertainability of the class and the class definition should not be overlooked. Rule 702 motions challenging plaintiffs’ class experts as a source of common proof and summary judgment motions targeting the class representative’s claims can be used in concert with the class opposition brief to defeat plaintiffs’ claims. This three-prong attack creates an evidentiary record that better supports a Rule 23(f) petition for interlocutory appeal and provides a more robust appellate record.

The bottom line: Every case is unique, and strategy should be tailored for the specific case, judge and jurisdiction. But in this new, post-trilogy age, the class certification is tantamount to the trial. Let the evidentiary battles begin!

Reprinted with permission from the August 1, 2014, edition of *Corporate Counsel* © 2014 ALM Media Properties, LLC. All rights reserved. Further duplication without permission is prohibited. For information, contact 877-257-3382, reprints@alm.com or visit www.almreprints.com.
About the Authors

Cari K. Dawson

Cari Dawson chairs the Class Action Practice Team and has an established track record of successfully defending Fortune 500 companies as lead counsel in high-profile enterprise litigation throughout the United States. In addition to defending hundreds of class actions across a broad spectrum of industries, she assists clients in the areas of commercial litigation, strategic counseling, and crisis management.

In 2013, the National Law Journal named Cari one of the “100 Most Influential Lawyers in America” for her work as lead class action counsel in the Toyota Unintended Acceleration MDL in California. For the past several years, Chambers USA has named her to their list of “The Best Lawyers in America” in the area of commercial litigation. In 2014, Cari was recognized as one of the Top 50 Women Super Lawyers in Georgia by Super Lawyers magazine, and she was named one of the “2014 Most Powerful & Influential Women” by the National Diversity Council.

David Venderbush

Throughout his 20-year career, David Venderbush has always been at the heart of bet-the-company litigations literally ripped from the headlines. In litigations involving breast implants, asbestos, cell phones, Vioxx, Seroquel, and unintended automobile acceleration, Mr. Venderbush’s work in various virtual law firms has helped reduce eventual client expense to a fraction of initial potential exposure.

As counsel in the Products Liability Group, Mr. Venderbush focuses his practice on trial and appellate work, with particular experience in legal strategies for managing complex litigation. As a member of national counsel teams in several multidistrict litigations, he has served as national litigation strategist, supervised local counsel, and implemented litigation management and expense control programs. Mr. Venderbush has been particularly successful at effectively ending mass tort litigations through the exclusion of expert witness testimony on complex scientific issues under Federal Rule of Evidence 702 and Daubert.
Any time an employer uses an outside vendor to run a credit or criminal background check on an applicant or employee, it is obtaining a consumer report and must follow a number of specific requirements under the Fair Credit Reporting Act (FCRA) and, in several jurisdictions, counterpart state laws. With increasing frequency, employers are being targeted by lawsuits alleging technical violations of these laws. Even more alarming, because the FCRA and some state laws allow for statutory damages for willful violations without a showing of actual harm, laws governing an employer’s use of consumer reports are the subject of a growing wave of class action claims.
Federal and State Requirements When Using Consumer Reports to Make Employment Decisions

The FCRA contains specific requirements for employers that use consumer reporting agencies (CRAs) to obtain credit and background reports for job applicants and/or existing employees. The most important of these requirements—and the ones that are at issue in the recent surge in FCRA litigation—are:

1. **Disclosure and Consent Before Obtaining a Consumer Report.** Before obtaining a consumer report from a CRA, an employer must (a) give the applicant or employee a clear and conspicuous written disclosure notifying him or her that it may obtain a consumer report for employment purposes, and (b) obtain the applicant’s or employee’s written authorization to do so. The disclosure must be in a stand-alone document consisting of only the disclosure, but the written authorization may be given on the same document as the disclosure.¹

2. **Notice Before Taking Adverse Action.** Before taking any adverse employment action based in whole or in part on information contained in a consumer report, an employer must provide the applicant or employee with a “pre-adverse action notice” indicating the intent to take an adverse action and providing a copy of the report and a summary of the consumer’s rights under the FCRA.² Employers should wait at least five business days after sending the notification before taking the contemplated action.³

3. **More Notice After Taking Adverse Action.** After taking the adverse action based in whole or in part on information contained in a consumer report, the employer must provide the applicant or employee a separate “adverse action notice” indicating that such action was taken and providing (a) the name, address, and phone number of the consumer reporting agency that supplied the report; (b) a statement that the company that supplied the report did not make the decision to take the adverse action; and (c) a notice of the person’s right to dispute the accuracy or completeness of the report.⁴

Because many employers are either unclear about, or unaware of, the FCRA’s highly technical disclosure, consent, and dual-notice provisions, it is no surprise that the recent uptick in employment-related FCRA lawsuits has primarily involved alleged violations of one or more of these requirements. In addition,

---

³ The FCRA does not specify how much advance notice must be given to an applicant or employee before the adverse action is taken, but the requirement is generally understood as being intended to give the person a meaningful opportunity to review the report and to address any inaccuracies or otherwise respond. Accordingly, the Federal Trade Commission (FTC), which was the federal agency tasked with enforcing the FCRA before that task was recently taken over by the Consumer Financial Protection Bureau (CFPB), has suggested that five business days is typically a reasonable amount of time to satisfy the pre-adverse action notice requirement, and at least one federal district court has agreed. See Reardon v. Closetmaid Corp., No. 08-1730, 2011 U.S. Dist. Lexis 45373, at *11 (W.D. Pa. Apr. 27, 2011) (finding FTC guidance was entitled to “respect” from the courts).
some states have adopted FCRA-like statutes that regulate how employers use consumer reports related to their applicants and employees, and some states have imposed even more onerous requirements on employers in that context. For example, California’s law imposes an additional notice obligation on employers that use CRAs to screen applicants and employees.5 California not only limits the use of consumer reports to specific types of jobs, but before ordering the report, the employer must notify the individual in writing of the specific basis for permissibly using the consumer credit report.6

Statutory Incentives for FCRA Class Actions Against Employers

The FCRA provides a private cause of action against an employer for either “negligently” or “willfully” failing to comply with any of the statute’s requirements. Negligent failure to comply with the FCRA can make an employer liable to applicants or employees for actual damages, costs, and attorneys’ fees.7 For willful FCRA violations, however, plaintiffs may elect to seek either actual damages or statutory damages between $100 to $1,000 per violation with no need to show actual damages.8 Employers that willfully violate the FCRA can also be liable for punitive damages, costs, and attorneys’ fees.9

“The FCRA’s employment requirements can easily become an expensive trap for the unwary employer.”

The availability of statutory damages for willful FCRA violations makes the statute especially attractive to plaintiffs looking to bring large class-action lawsuits against employers that use CRAs to screen applicants and employees. Because there is no requirement to prove actual damages to recover for willful violations of the FCRA, plaintiffs can circumvent individual assessment for class-action purposes by asserting that an employer should be held liable regardless of whether the alleged willful violations resulted in actual losses for individual plaintiffs. Moreover, courts have set the “willfulness” bar relatively low for FCRA violations—an employer’s FCRA violations can be considered “willful” if the employer repeatedly, systematically, or typically vio-

---

6 Cal. Labor Code § 1024.5 establishes a general prohibition against the use of consumer credit reports for employment purposes in California. With limited exceptions for certain financial and insurance companies, Section 1024.5(a) provides that an employer or prospective employer “shall not use a consumer credit report for employment purposes unless the position of the person for whom the report is sought is” one of eight specifically listed types of positions (e.g., a “managerial position” or “a position that involves regular access to cash totaling ten thousand dollars ($10,000…during the workday”). Pursuant to Cal. Labor Code § 1785.20.5, employers or prospective employers wishing to use a consumer report for employment purposes must provide the individual notice of the specific exemption under which such use is permitted.
lated the statute.\textsuperscript{10} As such, an employer that regularly violates one or more of the technical requirements described above will most likely be found to have acted willfully and thus be liable for statutory damages, as well as punitive damages and attorneys’ fees and costs. Because the plaintiff class in an FCRA class action will often be a large group of job applicants, damages of $100 to $1,000 per violation can add up quickly. For all of these reasons, the FCRA’s employment requirements can easily become an expensive trap for the unwary employer, which the plaintiffs’ bar has started to take greater notice of.

Another reason FCRA claims against employers are gaining in popularity is the statute’s limitations period, which was recently amended to extend up to five years. Specifically, actions for liability under the FCRA must be brought no later than the earlier of (1) two years after the date when a plaintiff discovers the violation; or (2) five years after the date on which the violation occurred.\textsuperscript{11} Such a long statute of limitations is highly unusual for a federal statute and has the potential to be devastating to employers that screen hundreds or thousands of job applicants each year.

\textbf{Practical Advice for Employers}

Given the recent uptick in FCRA lawsuits against employers—a trend that will very likely continue for the foreseeable future—there is no time like the present for employers to take steps to minimize risk and liability in this regard. Below are some practical tips for employers to consider:

1. **Ensure FCRA-Compliant Policies and Practices.** Employers would be well-advised to ensure that their policies and practices regarding the use of consumer reports in the hiring, firing, reassignment, and/or promotion process comply with the requirements discussed above. Employers may want to consider conducting a privileged review of their background check consent forms, pre-adverse and adverse action notices, and any other policies or procedures they follow when conducting background and credit checks of their applicants and employees.

\textsuperscript{10} The Supreme Court has interpreted “willfulness” under the FCRA to include reckless violations, which can occur when a company is aware of the FCRA and takes actions that do not comport with a reasonable reading of the statute with regard to the requirement that was allegedly violated. See Safeco Ins. Co. of America v. Burr, 551 U.S. 47 (2007). Some courts have found that willfulness can be based on only a handful of similar or repeated violations, with no requirement for a plaintiff to show that the defending employer was even aware of its FCRA obligations. See, e.g., Smith v. HireRight Solutions, Inc., 711 F. Supp. 2d 426, 435 (E.D. Pa. 2010) (finding that a plaintiff had sufficiently alleged willfulness where the complaint indicated that the defendant had repeatedly engaged in ‘objectionable conduct’ by reporting a single criminal history incident multiple times on a consumer report—an assertion that could, “at minimum, rise to the level of reckless disregard”).

2. **Ensure Appropriate Document Retention.** Because of the potentially long statute of limitations for claims under the FCRA, employers should keep records relating to employment-related consumer reports and their efforts to comply with the FCRA for at least six years.

3. **Be Aware of Other Legal Requirements.** As noted above, some states and municipalities have consumer reporting laws that are similar to the FCRA but may contain different requirements. Additionally, an increasing number of states and municipalities continue to impose hiring practice restrictions such as so-called "ban the box" laws and social media laws that limit the information employers can seek during the hiring process and how employers may make decisions based on such information. Employers must know and comply with the laws of the states and municipalities where they operate and employ people.
About the Authors

Lisa H. Cassilly

Lisa Cassilly concentrates on the representation of management interests with a special emphasis on litigated matters. She has defended against all types of employment claims in administrative proceedings, arbitrations, and trial and appellate courts throughout the country. Lisa has extensive experience conducting internal investigations and audits, handling SOX and other whistleblower claims, and prosecuting and defending actions involving claims for breach of restrictive covenants, employee piracy, breach of fiduciary duties, and trade secret misappropriation.

Lisa is the immediate past chair of the Labor & Employment Group at Alston & Bird and has been repeatedly recognized as a leading employment lawyer by Best Lawyers and Chambers USA, which reports that, “she is one of the top performers in her field” whose clients describe her as “brilliant, strategic, and extremely effective.” Super Lawyers has ranked her among the Top 50 Female Attorneys in Georgia in seven annual rankings. She regularly appears in Georgia Trend magazine’s Legal Elite listing.

Brett E. Coburn

Brett Coburn is a partner who concentrates his practice on employment litigation and counseling. He regularly litigates employment discrimination and retaliation cases, as well as wage and hour cases under the FLSA and various state laws. He has extensive experience litigating cases involving breach of employment contracts, violation of non-competition and other restrictive covenants, misappropriation of trade secrets, defamation, breach of employee duties, tortious interference, and related customer and employee raiding claims. He also litigates cases involving claims against public accommodations under Title III of the ADA.

In addition to litigation, Brett’s practice includes drafting and advising clients regarding employment agreements, restrictive covenants, and separation agreements; counseling employers on compliance with federal and state employment laws; assisting employers in identifying and reducing risks associated with their hiring processes; minimizing exposure during reductions in force; assisting federal contractors in affirmative action compliance; defending against EEOC, OFCCP, and U.S. Department of Labor Wage & Hour Division investigations and audits; and advising on employment-related issues arising in corporate transactions.
For the last six years, the Federal Deposit Insurance Corporation (FDIC) has rummaged through the rubble of the Great Recession, seeking to pin the losses from the global financial crisis on leaders of banks and other financial institutions. Since 2008, the FDIC has filed more than 100 lawsuits against bank directors and officers.

The barrage of FDIC lawsuits has brought into relief state laws governing director and officer liability. In many states—including Delaware, the leading light on corporate law—the FDIC must plead and prove gross negligence to recover against directors or officers because the state’s business judgment rule insulates management from liability for ordinary negligence. See, e.g., Aronson v.
Lewis, 473 A.2d 805, 812 (Del. 1984) (“under the business judgment rule director liability is predicated upon concepts of gross negligence”).

This past July, the Georgia Supreme Court in FDIC v. Loudermilk, 761 S.E.2d 332 (Ga. 2014), clarified the reach of Georgia’s business judgment rule and offered a road map to directors and officers for coming within the rule’s protections. That guidance holds not only for Georgia directors and officers but also for directors and officers in those many other states that apply a business judgment rule similar to Georgia’s.

In Loudermilk, the FDIC sued former directors and officers of The Buckhead Community Bank, a Georgia bank that did not survive the financial crisis.1 Questions remain after the decision, but Loudermilk made a few things clear:

1.  **Georgia has a business judgment rule.**

   If there were any doubts before Loudermilk, it’s now clear that the business judgment rule is a part of Georgia law: “From our precedents, we conclude that the business judgment rule is a settled part of our common law in Georgia, and it generally precludes claims against officers and directors for their business decisions that sound in ordinary negligence.….” Loudermilk, 761 S.E.2d at 338.

2.  **Georgia’s business judgment rule differs from Delaware’s.**

   It’s now just as clear, however, that Georgia’s business judgment rule differs from Delaware’s. In Delaware, the business judgment rule shields directors and officers from liability for ordinary-negligence claims of any kind—whether coming in the form of a straightforward challenge to the wisdom of a business decision or more stealthily as a challenge to the process by which the director or officer reached the decision. See Brehm v. Eisner, 746 A.2d 244, 259 (Del. 2000).

   “Georgia’s [business judgment] rule does not categorically insulate directors or officers from claims that their decisional process was negligent.”

   As Loudermilk makes clear, that is not true of Georgia’s business judgment rule. Georgia’s rule precludes ordinary-negligence claims against directors and officers “except to the extent that those decisions are shown to have been made without deliberation, without the requisite diligence to ascertain and assess the facts and circumstances upon which the decisions are based, or in bad faith.” 761 S.E.2d at 338. The upshot is that Georgia’s rule does not categorically insulate directors or officers from claims that their decision-making process was negligent.2

---

1 The authors represent the directors and officers in Loudermilk.

2 In reaching that conclusion, the Loudermilk Court overruled two earlier decisions from the Georgia Court of Appeals holding that Georgia’s business judgment rule offered protections at least as broad as Delaware’s. See FDIC v. Loudermilk, 761 S.E.2d 332, 338–39 (Ga. 2014) (overruling Brock Built, LLC v. Blake, 686 S.E.2d 425 (Ga. Ct. App. 2009), and Flexible Prods. Co. v. Ervast, 643 S.E.2d 560 (Ga. Ct. App. 2007)).
But the difference between Georgia’s rule and Delaware’s may prove smaller than it first appears. The Loudermilk Court emphasized that “ordinary diligence” in the banking context “is less demanding than the standard of ‘ordinary diligence’ with which most ordinary negligence claims are concerned.” Loudermilk, 761 S.E.2d at 344. Unlike in a run-of-the-mill negligence case—where there is no presumption that the defendant acted reasonably—“officers and directors are presumed to have acted in good faith and to have exercised ordinary care.” Id. at 345. That presumption can be rebutted, but the “plaintiff bears the burden of putting forward sufficient proof to rebut it.” Id. In judging whether a plaintiff has rebutted the presumption, the court continued, courts and juries must remember that Georgia’s banking code “conclusively presumes” that directors and officers may reasonably rely on financial data and information from bank employees, lawyers, and public accountants. Id. at 344. Judges and juries must apply an objective standard in testing a plaintiff’s allegations or evidence, measuring the defendant’s conduct against “ordinarily prudent’ officers and directors of a similarly situated bank.” Id. at 344.

Like courts in Delaware and other jurisdictions, the Loudermilk Court emphasized that directors and officers who act as “mere dum- mies or figureheads” cannot rely on the business judgment rule’s protections. Id. at 345. Neither can those who make “unreasoned and uninformed decisions” (Id. at 335) or who do nothing more than allow their “name[s] to be printed on the bank’s station[e]ry.” Id. at 336.

3. Directors and officers should document their decision-making process.

Loudermilk clears the way for some process-focused negligence claims to survive the pleading stage, although rulings in cases fol-

lowing on the decision will more precisely define the contours of those claims. Regardless, the key takeaway from Loudermilk is this: Directors and officers should carefully document their business judgments, focusing not only on the ultimate decision but also on the decision-making process.

“Directors and officers should carefully document their business judgments, focusing not only on the ultimate decision but also on the decision-making process.”

A few tips on that score: Meeting minutes should reflect robust debate over decisions when it happens. Documents should reflect that decision-makers gathered and evaluated information in ways that are standard to their industry. In that regard, boards should seek advice from third-party consultants or legal counsel about whether their information-gathering and decision-making processes adhere to industry norms. Companies should also develop protocols for ensuring that directors and officers have sufficient time to review information before making decisions.

* * *

Non-bank corporations in Georgia have another option for responding to Loudermilk. O.C.G.A. § 14-2-202(b)(4) of Georgia’s corporate code permits a non-bank company to amend its charter to insulate its directors (but not officers) from personal liability for everything except self-dealing, intentional mis-
conduct, or knowing violations of law. Banks may amend their charter in the same way, but the analogous provision in the state's banking code protects only against shareholder actions, not against suits by the FDIC. See O.C.G.A. § 7-1-493(e).

Beyond that, some have called for a legislative response to *Loudermilk* to answer the questions left open by the decision. In particular, some have pushed for a statutory amendment setting a gross-negligence standard for both substantive and procedural challenges (as Delaware does). The authors favor such an amendment.
About the Authors

Steven M. Collins

Steve Collins is a partner practicing in the firm’s Litigation & Trial Practice and Securities Litigation Groups. As the principal components of a commercial litigation practice, he focuses on securities litigation, investigations, and enforcement proceedings; financial services litigation; and professional liability litigation.

Mr. Collins’s experience in securities litigation and investigations includes representation of clients in SEC, stock exchange, and state securities investigations and enforcement proceedings, in internal and other corporate investigations, in corporate governance matters, and in shareholder class actions and other litigation under the federal securities laws. His experience in financial services litigation includes representation of financial institutions in connection with consumer class actions, D&O claims, and disputes arising from loans, mergers and acquisitions, and other commercial transactions. His experience in professional liability litigation includes counseling clients on professional liability matters and representing clients in professional liability litigation.

Robert R. Long

Robert Long is a corporate and finance litigator with experience in mergers and acquisitions, corporate governance, regulatory compliance, internal investigations, and director and officer liability. He has substantial experience as lead counsel in matters regarding shareholder disputes, fiduciary duties, and numerous federal agencies, including the FDIC, OCC, Federal Reserve, Department of Justice, and SEC. Robert also advises corporations on director and officer insurance coverage issues. He is recognized by Georgia Trend magazine as one of Georgia’s “Legal Elite” and by Atlanta magazine as a “Rising Star.”

Robert leads the Securities Litigation Group’s publication of the treatise Securities Litigation: Forms & Analysis (Thomson Reuters © 2009) and frequently publishes and speaks on banking, securities, and director and officer liability.
Brian D. Boone

Brian Boone is a member of the Litigation & Trial Practice Group. Brian has represented clients before the U.S. Supreme Court, federal and state appellate and trial courts, and arbitration panels in cases (including many class actions) involving constitutional law, antitrust laws, RICO, the False Claims Act, health care laws, securities laws, and state consumer fraud laws. Recently, Brian and fellow Alston & Bird litigator Nowell Berreth convinced the U.S. Supreme Court to grant review in Dart Cherokee Basin Operating Co., LLC v. Owens, No. 13-719, and then to rule in their clients’ favor on the merits. The Supreme Court victory prompted Law360 to name Brian and Nowell to its list of “Legal Lions” for the week of December 15, 2014.
Export Control Reform: Enforcement Trends Build Higher Walls Around Fewer Items

By Jason M. Waite and Diego Marquez

In August 2009, President Obama launched an Export Control Reform (ECR) Initiative that called for a broad interagency review of the U.S. export control system with the goal of strengthening national security and the competitiveness of key U.S. manufacturing and technology sectors by focusing on current threats and adapting to the changing economic and technological landscape. Now, more than five years into this ECR Initiative, the Administration has made several revisions to the applicable regulations, with many final rules going into effect this past year.
While some may view ECR as an effort to streamline controls or decontrol less sensitive items, the initiative also is undoubtedly an effort to reprioritize controls, an effort that includes tightening higher-priority controls and focusing enforcement efforts on more sensitive items. Former Secretary of Defense Robert Gates once described the objective of ECR as the development of “a system where higher walls are placed around fewer, more critical items.” Exporters adjusting to ECR need to follow reform closely and understand not only how revised rules impact licensing for their products and services, but also how “higher walls” may impact enforcement trends and compliance risks moving forward.

“ECR is undoubtedly an effort to reprioritize controls, an effort that includes tightening higher-priority controls and focusing enforcement efforts on more sensitive items.”

With items moving from control under the International Traffic in Arms Regulations (ITAR) administered by the Directorate of Defense Trade Controls (DDTC) to control under the Export Administration Regulations administered by the Department of Commerce, Bureau of Industry and Security (BIS) as a result of ECR, an increase in enforcement activity by BIS can be expected simply as a result of increased responsibility over exports. Notably, BIS enforcement capacity, practice, and procedure vary significantly from the enforcement approach exporters would have experienced with DDTC. BIS has a robust Office of Export Enforcement staffed by special agents conducting investigations around the country. In contrast, DDTC does not maintain that same type of enforcement apparatus, and instead depends on a different, typically more cooperative model under which compliance specialists engage with exporters about potential violations. DDTC has traditionally been very judicious in its selection of cases that warrant an enforcement response and has always made far fewer administrative cases than BIS.

One of the interesting trends to consider is the increase in criminal enforcement in FY 2013. It may only be coincidence, but a curious coincidence it would be given the Administration’s focus on criminal enforcement throughout ECR. For example, the Administration worked with Congress to harmonize statutory criminal penalties for export control violations and raised concerns regarding the low penalties (frequently below the U.S. Sentencing Guidelines) in criminal convictions for export control violations.1 Meanwhile, investigations conducted by BIS in FY 2013 resulted in the criminal conviction of 52 individuals and businesses for export violations, nearly double the 27 convictions in FY 2012.2 The penalties for these convictions came to $2.7 million in criminal fines (down from $4.8 million), more than

---


$18 million in forfeitures (up from $5 million), and more than 881 months of imprisonment (up from 187). While an exporter convicted in FY 2013 received on average roughly 10 more months of prison time than in FY 2012, it is difficult to know for certain whether the increase in criminal enforcement is directly tied to the “higher walls” of ECR. It is certainly a trend worth watching, however, particularly given that one of the first criminal enforcement actions in FY 2014 resulted in a Chinese citizen being sentenced to almost five years in prison for attempting to export high-grade carbon fiber to China without a license.

Generally speaking, as has been the case in the past, criminal enforcement in FY 2013 focused on export violations involving countries that are the target of U.S. sanctions or that involve significant national security concerns. For example, 22 of the 52 criminal cases in FY 2013 involved exports to Iran. Other cases involved exports to Hezbollah (1) or activity in Belarus (5), China (8), Pakistan (2) (involving exports to a nuclear power plant), Sudan (2), and Ukraine (1). This trend has continued in FY 2014, and we expect it to continue in the future.

On the administrative side, BIS investigations resulted in the completion of 71 administrative export and antiboycott cases against individuals and businesses in FY 2013 (up from 42 in FY 2012) and $6.5 million in civil penalties (down from $7.4 million). However, the most significant development over the past year in administrative enforcement by BIS came early in FY 2014 with the largest civil penalty ever levied by BIS. Weatherford International Ltd. in Houston and four of its subsidiaries agreed to pay a $50 million civil penalty to BIS as a result of allegations that the companies exported oil and gas equipment to Iran, Syria, and Cuba, as well as items controlled for nuclear nonproliferation reasons to Venezuela and Mexico. An additional $50 million in penalties was imposed by the Department of Justice. The Weatherford case followed the pattern we have seen in criminal investigations and involved exports to sanctioned countries as well as related violations of the Foreign Corrupt Practices Act.

“Investigations conducted by BIS in FY 2013 resulted in the criminal conviction of 52 individuals and businesses for export violations, nearly double the 27 convictions in FY 2012.”

Whether or not this is a direct result of the “higher walls” initiative of ECR, BIS enforcement activity is increasing; and exporters should plan for this heightened focus on enforcement to continue. BIS plans to increase its enforcement capabilities and resources in FY 2014 by adding 22 full-time equivalent employees and is targeting an increase in the number of enforcement actions of nearly 30 percent. Exporters can expect BIS to continue...
to focus on the more egregious violations and the more problematic countries. A comprehensive and risk-based export control compliance program is more important than ever as companies learn to manage the transitional period of ECR and as the government works to focus and expand its enforcement activities.
About the Authors

Jason M. Waite

Jason Waite concentrates his practice on the regulations impacting the global movement of goods, technology, and services. He counsels clients on export controls, economic sanctions, customs, and free trade agreements, with an emphasis on compliance, transactional matters, strategic planning, and enforcement defense.

Jason conducts internal investigations and compliance self-assessments, develops internal trade compliance and training programs, represents clients in audits and origin verifications, and guides clients through voluntary disclosures of actual and potential import and export violations. Jason has significant experience representing clients that are the subject of government investigations involving alleged violations of export, import, and economic sanctions regulations as well as the Foreign Corrupt Practices Act. He defends clients in administrative proceedings and in litigation concerning civil and criminal penalties, debarment, forfeiture, and liquidated damages. He also represents clients in conducting trade compliance due diligence and in negotiating and documenting trade compliance responsibilities among parties to transactions.

Diego Marquez

Diego Marquez concentrates his practice on government relations and compliance. A senior associate in the International Trade & Regulatory Group in the Washington, D.C. office, Mr. Marquez advises clients on a wide range of legislative, public policy, and regulatory matters. His practice includes regular counsel to clients on all aspects of their interaction with the federal government, as well as representation of his clients’ public policy interests before Congress and the Administration.

Mr. Marquez specializes in issues pertaining to international trade, federal elections, and government ethics. His clients include domestic and multinational companies, trade associations, political organizations, and individuals. He has significant experience counseling clients on compliance with complex regulatory schemes and representing clients that are the subject of government investigations or enforcement actions. Mr. Marquez also assists clients with strategic business planning and the development and implementation of internal compliance policies and procedures.