# Compliance 2.0

Geoffrey Parsons Miller
Stuyvesant Comfort Professor
Director, Program on Financial Institutions
Co-Director, Program on Corporate Compliance and Enforcement
New York University Law School
New York, New York USA

Remarks at the Conference: Compliance in Brazil and in the World
São Paolo, Brazil
December 9, 2015

The second decade of the Twenty-First Century has witnessed a remarkable shift in the relationship between regulators and the firms they supervise.

Responding to a perception that corporate misconduct had reached unprecedented and unacceptable levels, regulators have massively enhanced their expectations and have backed these expectations with spectacular fines and other sanctions.

In response, banks and other regulated industries have greatly upgraded their systems of controls designed to deter and detect violations of applicable norms.

These changes are so profound as to represent nearly a revolution in how business is conducted at regulated firms – a change so profound that some commentators have taken to labeling the current environment as "Compliance 2.0".

My remarks today will describe and critically assess the transition to this new environment.

## The New World of Enforcement

To understand the magnitude of these changes, it is useful to review some of the enforcement actions that have punctuated the headlines of business pages over the past few years.

Financial institutions:

Many financial institutions – commercial and investment banks – have been swept up in government enforcement actions.

Here is a partial list:

● In 2012 five U.S. banks agreed to pay up to $25B to settle charges that they had engaged in abusive practices in originating or servicing home mortgage loans.

● In 2013 JPMorganChase agreed to pay $13B to settle charges that it had misrepresented the quality of mortgage-backed securities.

● In 2012 HSBC agreed to pay $1.9B for failing to comply with U.S. money laundering regulations.

● In 2015 Credit Suisse agreed to pay $2.6B to settle charges that it had conspired to defraud the U.S. taxing authorities; this followed a $780M fine imposed on UBS for similar misconduct.

● In 2015 BNP Paribas agreed to pay $8.9B and was sentenced to five years of probation for violating U.S. sanctions regulations.

● In 2014 and 2015 five of the world's largest banks agreed to pay approximately $9B to U.K. and U.S. regulators growing out of charges that they had manipulated foreign exchange markets.

● Beginning in 2012 and continuing to the present, several of the world's largest banks have agreed to pay fines approximately $5B to settle charges that they manipulated the LIBOR interest rate. Other enforcement proceedings related to this case are ongoing.

Pharmaceutical marketing:

These huge fines have not been limited to financial institutions. The pharmaceutical industry has been heavily sanctioned for violating restrictions on marketing drugs for unapproved uses.

Fines here include:

● 2013, GlaxoSmithKline: $3B

● 2009, Pfizer: $2.3B

● 2013, Johnson & Johnson, $2.2B

● 2102, Abbott Labs, $1.5B

Public safety and environmental violations:

Huge fines and other sanctions have also been imposed on companies that engaged in activities that endangered the public health and safety:

● In 2015 General Motors agreed to pay $900M in fines and faces possible exposure to billions more in private damages over charges that it marketed cars with faulty ignition switches and concealed the defect from regulators and the public.

● In 2015 British Petroleum agreed to pay a fine of $20B in connection with the Deepwater Horizon oil spill in the Gulf of Mexico; in addition BP will pay more than $28B in civil settlements and cleanup costs. The total bill to the company is approximately $48B.

● The Volkswagen emission control cheat scandal may prove to be the most costly of all, with estimates of total company costs ranging from about $30B to more than $80B.

Corrupt practices:

Many companies have been caught up in enforcement actions over bribes and other corrupt practices. A leading, but far from the only, source of liability in this area is the U.S. Foreign Corrupt Practices Act.

Major settlements under the FCPA include:

- Siemens: $800M in 2008
- Alstrom: $772M in 2014
- KBR/Halliburton: $579M in 2009
- BAE: $400M in 2010.

Today, moreover, allegations of international bribery often trigger enforcement actions in multiple countries, including the U.K. under that country's Bribery Act and also in the country or countries where the alleged corrupt practices occurred.

* * *

And these are only examples of the largest fines. Hundreds of smaller but still significant enforcement actions have occurred in recent years.

Moreover, so far I have only been describing the fines and other monetary penalties. There are other bad consequences including:

- Enormous legal and professional fees. The consumer products company Avon, for example, reportedly paid out approximately $340M in attorney fees for years in connection with an internal FCPA investigation.
- Damage to reputation. Consider the harm experienced by Volkswagen, formerly viewed in a favorable light in the public eye.
- Debarment from providing services to governments or international agencies.

● Criminal liability for the company and its senior officers.

● Civil liability to customers or others who are damaged by the misconduct.

● Job loss or pay cuts for the CEO.

And so far I have only been talking about business firms and compliance.

But compliance problems can arise in any complex organization, whether or not it is organized for profit.

Sports:

● Doping scandals in international cycling, Major League Baseball, and athletes on Russian national teams.

● The ongoing scandal in the world soccer organization that last week saw indictments against 16 more top officials from around the world.

Religious and public service organizations:

● Sexual abuse by priests in the Catholic Church

● Alleged fundraising abuses at the Red Cross

Governments:

Compliance problems also affect governments and government officials. These include:

● Multiple charges of official corruption against high level officials in China

● The Petrobas matter here in Brazil

● Scandals involving other government officials in many other parts of the world.

## Compliance 2.0

Taken together, this list of enforcement actions – all occurring within the past decade – is an astonishing testament to the importance of compliance in today's world.

The response to these developments is captured in the phrase "Compliance 2.0".

The term implicitly refers to the fact that there was an earlier iteration, Compliance 1.0.

The earlier approach to compliance had the following elements:

● Compliance 1.0 was rule-based and paper-intensive. It focused on ensuring that people filled out forms and followed procedures.

● Compliance 1.0 was not based on an assessment of risk.

● Compliance 1.0 was carried out by relatively low-level, low-paid, and low-status employees.

● Compliance 1.0 was usually an adjunct of the legal department and reported to the company's general counsel.

● Compliance 1.0 was carried out on a department-by-department basis, with little central organization or planning.

Compliance *2.0*, as you might have guessed, has changed virtually all of these features. Traces of the old approach are still visible in modern compliance departments, but the influence is fading.

Compliance 2.0 is a group of new practices that, collectively, represent a paradigm shift in how the compliance function is carried out.

The following are its leading features:

● Compliance 2.0 greatly enhances the powers and responsibilities of internal control functions and offices:

First, internal audit: Internal audit was, traditionally, a low status job whose function was essentially to make sure that people were following the rules pertaining to financial reporting. It was a "check-the-box" job with little originality and limited scope for imagination.

Today, internal audit staffing has been greatly upgraded and levels of training and expertise for internal auditors have increased enormously. The chief audit officer typically "C-Suite" status as a leading executive and often reports directly to the audit committee of the board of directors.

Moreover, the heads of internal audit sometimes participate in the formulation of strategic policy for the institutions they serve.

Second, compliance: The compliance function at banks was traditionally a rather low level, low paid, and low status job presenting few opportunities for advancement within an organization.

This has changed nearly completely at many organizations.

Today, compliance can be a well-compensated, high status position with genuine involvement in strategic policymaking. The CCO is given the status of a "C-Suite" official and may have a reporting line to the CEO or, sometimes, to a relevant committee of the board of directors.

Third, risk management: risk management used to be a technical job involving the purchase of insurance. Risk managers had essentially no influence on strategy or policy. Today, risk managers exercise substantial influence at financial firms. The head of risk management is typically designated as a member of the C-Suite, and may enjoy reporting rights to the CEO or even the board of directors. Staffs at risk management departments have been massively increased and salaries have skyrocketed.

An important aspect of the enhanced powers of these internal control officials is the professionalization of their jobs.

We are today witnessing the maturation of one profession – internal audit – and the birth of two others – compliance and risk management. I predict that in within a dozen years, internal auditors, compliance officers and risk managers will be recognized as professionals alongside auditors, accountants, lawyers, appraisers and other highly trained service providers.

● Next, Compliance 2.0 involves a company's senior leaders.

The CEO, in particular, is the institution's most important compliance officer. She is expected to demonstrate a commitment to compliance by scrupulously following the rules in her own conduct; and also to communicate a commitment to compliance in many sorts of communication with employees at all level. A genuine commitment to compliance by the CEO is sometimes referred to as "tone at the top." It is one of the most important requirements of an effective compliance program in the modern sense.

Members of the board of directors are also expected to display concern for compliance. Particularly important is the chairman of the board, the official leader of the supervisory group. Members of the audit committee or other board committee tasked to overseeing the firm's compliance activities also have important roles to play.

The relevant board committee is expected to give significant time to compliance issues and to hold itself ready to confer privately with the company's senior internal control officials. Some companies have considered it desirable to recruit members who are familiar with compliance-related issues.

Responsibility for compliance is not limited to top officials. Even mid-level managers are expected to display a commitment to compliance in their personal and professional lives – the so-called "tone at the middle."

● Next, Compliance 2.0 utilizes a risk-based approach.

This means that all compliance activities are based on a risk assessment in which the probability and magnitude of potential violations are evaluate in order to identify areas where the danger of violations is greatest. Resources and attention of the compliance department are then allocated according to the assessment of risk.

The risk-based approach is not limited to the compliance department. All internal control operations, including internal audit and – of course – risk management also use a risk-based methodology. So do external control offices such as the firm's outside auditor and its principal regulator or regulators.

● Compliance 2.0 is conducted on an enterprise-wide basis.

Even if responsibility for compliance is to some extent distributed across departments or offices, there is central control over the compliance function. It is only through central control that risks of violations to the enterprise can be fully recognized, assessed and controlled.

● Compliance 2.0 is data-driven.

Instead of relying solely on manual inspection of forms and documents, the new compliance makes heavy use of computerized algorithms. Data analysis is particularly important in the fields of foreign corrupt practices, money laundering and sanctions regulations, and insider trading on securities markets.

● Compliance 2.0 focuses on individual misconduct.

In the past, regulatory sanctions were typically administered against the offending organizations, with the individuals who organized the misconduct receiving light penalties.

No longer.

U.S. prosecutors and regulators have announced that they will routinely seek to punish those within an organization who are responsible for the company's offenses, including prison time for serious offenders.

● Compliance 2.0 is a principles-based activity that emphasizes function over form.

The new compliance is not simply a "check-the-box" exercise, but rather an intuitive and analytical activity. Central to modern compliance is the upfront analysis of issues as well as a "lessons learned" exercise that seeks to identify root causes of violations and considers ways to prevent their recurrence.

● Compliance 2.0 includes a significant risk of criminal enforcement.

Every year, U.S. prosecutors obtain dozens of convictions, plea agreements, and deferred prosecution agreements with companies charged with engaging in violations of the law. So far criminal penalties against corporations have been principally a U.S. phenomenon. But the trend is growing around the world, as evidenced by the fact that the U.K. just entered into its first deferred prosecution agreement with a corporate offender.

● Compliance 2.0 makes heavy use of vendors who provide analytical, consulting, and task management services.

● Compliance 2.0 focuses on behaviors and cultural factors as well as economic incentives. Regulators and thought leaders in the compliance field speak frequently of the need to create a "culture of compliance" that pervades the organization.

The hope is that such a culture will cause people to refrain from engaging in misconduct simply because it is not part of their identity to do so. The use of behavioral and cultural drivers is a potentially lower-cost method of encouraging compliant behavior by employees as compared with other types of enforcement.

● Compliance 2.0 includes significant government requirements for compliance programs.

Several U.S. laws now require that such programs be established, and prosecutors and regulators consider an effective compliance program to be a mitigating factor when deciding whether to charge a company with violations and what sanctions to impose as part of a settlement of an enforcement action.

Settlements of criminal or regulatory enforcement proceedings frequently contain detailed provisions requiring the offending company to establish and maintain a robust compliance program.

Reports indicate that legislation about to be introduced in France will require all large companies to create formal compliance programs – something other countries have yet to do.

● Compliance 2.0 relies extensively on internal reporting and whistleblowing.

State of the art compliance programs contain multiple avenues by which employees who observe misconduct on the job can report their concerns on a confidential basis to senior officers.

When violations are found or suspected, companies are expected to conduct an internal investigation; and when the violations are serious or the misconduct occurs at a high level, the investigation may be turned over to an outside law firm specializing in such matters.

If the investigation turns up evidence of violations, the company is expected to inform the government of what it has learned. Potential claims of attorney client privilege may be waived.

The government also depends on information obtained from employees.

Government-sponsored whistleblowing programs offer guarantees against retaliation and provide bounties or rewards to informants whose information results in a successful enforcement action. U.S. whistleblowers have earned millions of dollars from tips: one named Bradley

Birkenfeld collected $104M for disclosing information about Swiss bank involvement in tax fraud, even though he himself had served time in federal prison for the same offense.

## Evaluation

I close with some thoughts about these developments.

There is cause for optimism but also for concern.

There can be little doubt that the uptick in government enforcement and the significant compliance response has, overall, enhanced incentives for law-abiding behavior by complex organizations. And there is every indication that these developments are durable – the growth of the compliance function is not a transitory or temporary development.

This is much to be applauded.

However, there are also reasons for concern. The following appear most salient:

● Compliance 2.0 comes at a significant cost.

The officials who insist on compliance activities by regulated firms do not pay these costs and therefore are often not sensitive to considerations of cost-effectiveness.

It is not only the fines that must be paid – these are painful but at least the money goes into the government, where we hope it will be spent for good uses.

But some of the costs of compliance are not recycled in such positive ways.

Many organizations have doubled or tripled their expenditures on compliance over the past few years. JPMorganChase announced that it was hiring more than 3,000 new compliance officers in 2014. Costly systems have to be brought on line and implemented. It is not clear that the social benefit of such expenditures actually exceeds their cost.

Things get worse once misconduct is discovered.

Firms that commence an investigation into potential violations lose control over the cost of these inquiries. Avon, the U.S. consumer products company, reportedly paid nearly $100M per year for the years it took to complete an internal investigation into foreign corrupt practices.

Similarly, obligations required by settlements of regulatory proceedings can be more extensive than what is really necessary to deter violations. And if a compliance monitor is appointed, the company has little ability to resist the monitor's potentially exorbitant compensation demands.

● Compliance 2.0's focus on tone and culture may lead to problems because these can be faked.

It is easy to forget the lessons of Enron Corp. Enron had state-of-the art corporate governance and an apparently excellent tone at the top. Yet it was all a sham covering up a massive fraud executed at the highest corporate levels. More recent examples can be cited. The problem is that it is difficult to distinguish truly good corporate culture from culture that is only a pretense.

● Compliance 2.0 may drive business into the shadows of questionable, poorly capitalized, or illegal organizations. Good companies will be compliant but misconduct may continue at the same or even an increased level in the shadow sector. This would not be a constructive development.

● Insofar as it relies heavily on risk assessments, Compliance 2.0 comes with own serious risk: the risk that the risk assessment may be wrong.

And risk assessments can be wrong. Few observers thought it remotely possible, in 2006, that the world's financial system would collapse in a severe liquidity crisis; but that is exactly what happened in 2008.

If the underlying risk assessment is wrong, we can be worse off with risk-based compliance than we were with the old, now discredited "check-the-box" approach.

● Compliance 2.0 arguably discourages innovation.

No company wants to be the one signaled out for potentially devastating fines and other sanctions. They may therefore refrain from engaging in innovative business practices that may attract unwelcome attention from regulators.

But competitive economies thrive on innovation. Especially in the financial services sector, where technological change is occurring at a massive pace, government policy should ordinarily encourage rather than discourage experiments into new ways of doing things. Compliance 2.0 may run counter to this objective.

● Compliance 2.0 gives spectacular and perhaps dangerous authority to the government.

Powerful government is fine as long as the authority so granted is exercised faithfully and in the public interest. But with authority comes potential for abuse.

Some have charged that recent corruption prosecutions in China and Russia have been motivated in part by a wish on the part of government officials to punish political rivals. The same charges have been made in the U.S. For example, Rick Perry, a former governor of Texas and a prominent Republican politician, was indicted by a Democratic prosecutor who alleged that Mr. Perry had engaged in a criminal abuse of office. Republicans claimed, in response, that the indictment was itself a cynical attempt to destroy the career of a political enemy.

● Compliance 2.0 can create a risk of complacency.

We may come to believe that the problems of corporate misconduct are essentially solved by this new, tech-savvy approach. In consequence, we may let down our vigilance against misconduct.

But while the new approach indeed provides greater assurance of good behavior, it is not a cure-all. Frauds, crimes, and other violations will continue to occur, and Compliance 2.0 will not deter them all or catch all of them when they do occur.

● Compliance 2.0 does not address one of the leading causes of misconduct.

It is easy to forget that the principal drivers of misconduct in the financial sector have not been greed, bad character, or competition. The leading cause of regulatory violations by financial institutions is probably the business cycle.

The American financier Warren Buffet famously said that it is only when the tide goes out that you learn who has been swimming naked. He meant that frauds and other misconduct come to light only at the end of an economic boom. This is an astute observation, well documented by recent experience.

We may expand one his observation by adding that it is only when the tide is *coming in* that people start to remove their bathing suits. In other words, economic booms provide opportunities and effective cover for misconduct.

Compliance 2.0 has nothing to do with the business cycle. It doesn't even take explicit account of the incentives for misconduct that economic booms can cause.

As yet, human beings have not learned how to repeal the business cycle. Until we do get control over booms and busts, we face an ever-present threat of economic conditions that induce misconduct by financial institutions and that no amount of compliance reform can prevent.

In offering these words of caution, I don't mean to dismiss the value of the new compliance approach, but only to offer a word of caution that neither Compliance 2.0 nor any other iteration of the system that might be devised in the future is going to solve the problem of corporate misconduct.

The best we can do is to deter and punish a sufficient amount of misconduct. Compliance 2.0 appears to do a reasonably good job along these lines.

Thank you for your attention.