# BUSINESS COMPLIANCE

## Governance – Compliance – Ethics

## 03-04/2014

**EDITOR-IN-CHIEF:**
**ANTHONY SMITH-MEYER**



Baltzer Science Publishers

ERICH SCHMIDT VERLAG

# THE ROUND TABLE DEBATE:
# WHISTLEBLOWING – LOVE IT OR LOATHE IT …

Chair: *Sharon Ward,*
Panelists: *Philip Brennan, Andrew Buckhurst, Scott Killingsworth, Pedro Montoya & Klaus Moosmayer**






Welcome to the Journal of Business Compliance Round Table. This is an opportunity to gather highly experienced thought leaders to discuss questions raised by the compliance community, to consider evolving trends in the field and to identify emerging topics for the future.

Today we are discussing whistleblowing, a term and activity that has risen in prominence over the past decade and one which poses challenges, dare we say conundrums, for many. There are many opinions expressed on the role and use of whistleblowing programmes, both internal and external. Some jurisdictions actively encourage their use, some legislate against it. Particularly in Europe, some view them with suspicion, even distaste. As we contemplate this topic from our many different perspectives and with a variety of experience, we have gathered a highly qualified group to ponder the issues of trust, integrity, legal considerations, anonymity and protection from retaliation that lie at its heart, all matters for ongoing deliberation by employers and employees alike.

**Sharon Ward:** Before getting to grips with the practicalities of whistleblowing programmes, let us try to clear up any remaining doubts concerning the moral rights and wrongs of "encouraging" whistleblowing. Are we now past this "good" or "bad" debate regarding their existence? Are whistleblowing programmes here to stay?

---

* **Philip Brennan** is Chairman of the Association of Compliance Officers in Ireland and Founder and Managing Director of Raiseaconcern.com. The remaining panelists are all members of the Editorial Board of the Journal of Business Compliance. Their respective biographies may be found at the end of this issue.

## WHISTLEBLOWING – LOVE IT OR LOATHE IT

**Scott Killingsworth:** Yes, that ship has sailed. There is no longer any doubt that confidential reporting mechanisms serve as a crucial, incremental early warning system for misconduct. And when global groups like the International Chamber of Commerce, the World Bank, the Electronic Industry Citizenship Coalition and the World Economic Forum are all advocating the use of such systems, and large company Supplier Codes of Conduct are requiring their business associates to implement whistleblowing systems, we can be sure that the trend will not reverse itself.

**Philip Brennan:** I agree, whistleblowing programmes are here to stay. However, there is still a long way to go before the majority of employers regard having a whistleblowing programme in place as something that is positive and sensible to do from a moral or even a business perspective. Only the better employers 'get it'. Many others are putting programmes in place merely because they feel this is something they are expected or required to have in order to be seen as satisfying legal or governance requirements.

**Andrew Buckhurst:** That's certainly true, but even then, viewed positively, whistleblowing schemes will remain in a company's compliance programme because it can be partly seen as a "defensive tool" against possible sanctions for non-compliance with anti-corruption laws like the UK anti-bribery Act or the FCPA. Furthermore, companies may also promote the existence of a whistleblowing scheme to demonstrate and signal their commitment against violations of laws, regulations and ethical breaches. In some European countries, the topic is seen from a data protection perspective, such as recently introduced in Hungary. The Luxembourg data protection authority[1] is currently working on the issuance of a specific note on this issue as well. However, it is more about clarifying procedure than legislating against whistleblowing arrangements.

**Pedro Montoya:** But there is still significant resistance in most of

1 *Commission nationale pour la protection des données.*

## WHISTLEBLOWING – LOVE IT OR LOATHE IT

*There is no longer doubt that confidential reporting mechanisms serve as a crucial, incremental early warning system for misconduct*

Continental Europe to the promotion of whistleblowing programs. As you say, particularly from data protection agencies, albeit that they are becoming more receptive to company requests for approval to put in place such a system. In some instances we even see recent regulations encouraging, even demanding the implementation of whistleblowing systems in areas like public policies against discrimination or harassment in the workplace. What we have not seen yet in Europe is the rewarding system we have seen developed in the United States.

**Scott Killingsworth:** I believe that the remaining cultural barriers or reservations are mainly relevant to the details of implementation and to the overall effectiveness of the programs, which is sensitive to the attitudes of potential whistleblowers and of their co-workers. In the big picture, whistleblowing systems are a necessary part of a comprehensive approach to compliance management.

**Sharon Ward:** That change in perception you refer to is clearly having practical consequences, not least on the attitude within firms themselves. It is said though that whistleblower schemes act as a safety valve, a mechanism that would be superfluous if the organisational culture is right. Do you think the existence of internal whistleblower schemes builds trust between employer and employed, or is it a harbinger of mistrust and intrigue?

**Scott Killingsworth:** Many things would be unnecessary if the organisational culture were perfect, but I don‘t think anyone has spotted that unicorn yet. As long as we are dealing with human imperfection, we are likely to find micro-cultures of misconduct within our organisations. An honest individual in the midst of such a pocket of toxicity will be uncertain who they can trust, or how far they have to go to find a sympathetic ear, and so this whistleblowing safety valve is really important.

**Philip Brennan:** Absolutely. No matter how positive the corporate culture is, some employees will always be nervous about raising concerns. This is perfectly understandable, particularly if the issue being reported involves malpractice or wrongdoing by a line manager or colleague. Human nature being what it

*Employees raising concerns about wrongdoing should not be expected to expose themselves to the risk of reprisal in return for doing the right thing*

is, those accused – whether rightly or wrongly – have a history of retaliation against the accuser. It can be very subtle, or downright blatant. Employees raising concerns about wrongdoing should not be expected to expose themselves to the risk of reprisal in return for doing the right thing, and so they need to be satisfied that measures are in place to ensure that will not be the case.

**Klaus Moosmayer:** It is all about communication. If Management on all levels openly discusses with the employees the advantages and risks of a whistleblowing system, this will certainly help to build trust. Employees have a very good sense about authentic behavior and leadership, so the implementation of such a system is not only a technical and legal challenge but requires also a thoughtful communication plan.

**Andrew Buckhurst:** I couldn't agree more Klaus. Communication and transparency are essential. It is up to the compliance team to explain the purpose of whistleblower schemes. Employees need to be informed about the existence, purpose and handling procedures of reporting mechanisms. It is necessary to demonstrate on the one hand that the whistleblower will be protected thanks to the non-retaliation principle and the confidential handling of his/her report and then, on the other hand, assuring the rights of the individual being the "reported person" – as in "innocent until proven guilty".

**Philip Brennan:** Communication on purpose and procedure is important. Primarily though, in my view the question of whether or not a scheme builds trust or mistrust largely depends on how the employer chooses to address wrongdoing that is escalated. Where there is a tendency to concentrate on who raised the issue, or the fact that it was raised using the whistleblowing process, rather than on the issue itself – well then, invariably, it gives rise to both mistrust and intrigue amongst across the work environment. Where, however, employers concentrate on discretely investigating the alleged wrongdoing itself and do not get involved in identifying the whistleblower or trying to determine their motive, the likelihood is that a more positive culture and attitude to whistleblowing will evolve. At the end

## WHISTLEBLOWING – LOVE IT OR LOATHE IT

*Whistleblowing… is about doing the right thing for the right reasons*

of the day the attitude of employees, and indeed middle management, to whistleblowing will largely be determined by whether or not the Board and senior management are demonstrably supportive of the programme and act promptly and decisively on matters escalated.

**Scott Killingsworth:** Certainly in the US we have a different attitude towards confidential reporting than is prevalent in much of Europe, as a result of different historical experiences. But we find that a whistleblower system can enhance trust if several conditions are met: the program must be administered impartially in a genuine effort to detect misconduct; confidentiality must be preserved to the maximum extent possible; verified misconduct must be addressed decisively; and the company must have a strong, effective anti-retaliation policy. These factors have all been positively linked to employees' willingness to report internally, as well as to the overall incidence of misconduct. In this realm, confidence in the ethical character of the company's top management, and confidence in the whistleblowing system, are known to reinforce one another. People are more likely to report if they trust senior management. If they have positive experiences with reports and investigations of misconduct, their trust in senior management and the company grows. That's a virtuous cycle we should work to take advantage of.

**Sharon Ward:** And indeed one that we should all be keen to contribute to. So it rather looks like we're agreed on the vital importance of transparency and communication for the effectiveness of these schemes within a firm, but what are your thoughts on internal versus external whistleblower schemes themselves? How do you distinguish between their impact? As Pedro already alluded to, the US SEC has effectively offered a bounty on external whistleblowing, rewarding those coming forward with significant cash rewards – do you think this is helpful to integrity in business, or do you see it as a destructive force that entices employees not to speak up at work, but to the regulator instead?

**Philip Brennan:** I think external whistleblowing schemes have a place, but I do not agree with the concept of external schemes rewarding those who

## WHISTLEBLOWING – LOVE IT OR LOATHE IT

come forward. Whistleblowing, or rather I prefer to talk about raising concerns about wrongdoing, is about doing the right thing for the right reasons. At its simplest, this should be a subordinate casually mentioning to their boss that they have a concern about something. Employers should provide various alternatives for escalation where an employee is not comfortable raising an issue with their line manager, ranging from a senior, trusted party within the firm to an independent, external third party service provider acting for the firm, but who will also protect the employee's identity. In all cases, the employer will have the option to investigate the matter and take appropriate action. And if the employee is not satisfied with the outcome, they should have the option to go externally – whether to regulators or law enforcement agencies – who, equally, should provide a professional and confidential reception for those raising a concern.

**Andrew Buckhurst:** Personally, I would always prefer that employees feel able to speak up at work first and only if the outcome is unsatisfactory (or the issue subsequently repeated) to then take this to a regulatory or supervisory body. No one likes to have dirty washing uncontrollably aired in public and most companies would probably want to avoid this if they could. However, where an employee feels there is an in-grained problem, which includes the corporate culture, then the external system clearly has significant benefits. Naturally, in some circumstances, it is only possible to raise a concern outside the company, given the nature of the violations being raised.

**Pedro Montoya:** These external whistleblowing channels are very seldom available in Europe. We have even seen cases where the whistleblower "threatens" to report a case being ignored to the SEC, even if the case is unrelated to this regulator! In my experience, the majority of employees regard external reporting with distrust and express more sympathy for those reporting through the company's hotline, as this is consider as "internal", even if it's outsourced.

**Philip Brennan:** I'd like to continue for a moment on the theme of raising an issue for reward; I believe this risks changing the dynamic totally. Sure, it

## WHISTLEBLOWING – LOVE IT OR LOATHE IT

*Law enforcement agencies do not pay witnesses to come forward with information; they rely on their goodwill to do so*

will yield some results, but how many of these could have been achieved anyway – and how much collateral damage is caused? External schemes are much more likely to build distrust and give rise to poorly motivated disclosure. The risk is apparent: are regulators and employers not much more likely to find themselves on the receiving end of frivolous or vexatious issues, as employees become motivated by reward to go outside the organisation rather than using internal processes. This creates a negative and distrustful culture. It is no longer about doing the right thing – it is about getting paid. Processes for dealing with criminal law which have evolved over several centuries are an interesting parallel. In general, law enforcement agencies do not pay witnesses to come forward with information; they rely on their goodwill to do so. Even the concept of offering a reward for specific information that is known to be out there (i.e. the identity of the perpetrator of a serious crime such as murder) is very rarely seen. This is because law enforcement agencies have tried and tested such processes over the centuries and found them to be unsuitable to an appropriate outcome.

**Scott Killingsworth:** Evidently a US topic! Well, there is concern about this, and in the US part of it is focused on the unresolved question whether whistleblowers who go to the government may be entitled not only to bounties, but to *stronger legal protection,* than those who report internally. But in general, the fear that the Dodd-Frank Act would open the floodgates to a massive wave of bounty-hunter whistleblowing may have been overblown. The most telling fact about internal versus external reporting is that, in US companies that have no whistleblowing mechanisms, an employee is three times more likely to forgo reporting internally and go directly to the government. It might be something of a surprise for many that the number of whistleblowers who circumvent their company channels, and report directly to the government is an order of magnitude smaller than the number who circumvent their supervisors in order to report *internally* through company channels – the point being that if you have a credible internal whistleblowing channel, people are much more likely to use it than to go outside the company. As to bounties, an Ethics Resource Center study assessed the effect

of seven different motivating factors on the decision whether to report externally; the availability of a substantial monetary award was the least influential of all. By contrast, the top reason employees gave for failing to report internally is that they didn‘t believe anything would be done about the misconduct. All this suggests that most whistleblowers are reporting for the right reasons and that the better your internal whistleblowing channel is, the less you have to worry about being the last to hear about a problem – and hearing about it from the government.

**Klaus Moosmayer:** You make a very interesting point Scott, and an important one as it addresses a real concern of encouraged “false reports”. A fair process is clearly the key, for complainants and for companies. Of course, once a concern is raised with an external authority then it is the duty of the authority to assess the allegation properly and decide if an investigation is necessary. But here there is a considerable burden of responsibility on the authority in question not to punish the company if there is a sound internal reporting system in place, which at least offered a confidential internal channel and protection from retaliation. Regarding financial awards for complainants, I personally believe this sets the wrong tone internally and externally. Companies should clearly encourage their employees to report instances of misconduct in good faith – not as a financially rewarded “special task”, but as a part of their trustful employer-employee relationship. And the authorities should be mindful of this and not set the wrong tone.

**Sharon Ward:** Not to mention perhaps that the receipt of financial reward for reporting might detract from the credibility of the whistleblower? However, back to the proverbial drawing board. We have agreed that the form and nature of an internal whistleblower, or concern raising arrangement is crucial to credibility and effectiveness if it is to be a contributor to trust within the organization. However, there is the risk that employees will view such initiatives as “box-ticking” to comply with external expectations rather than a genuine initiative to encourage employees speaking up. What advice would you offer to the firm in order to make this as effective and inclusive a process as possible?

## WHISTLEBLOWING – LOVE IT OR LOATHE IT

*The fear that the Dodd-Frank Act would open the floodgates to a massive wave of bounty-hunter whistleblowing may have been overblown*

**Andrew Buckhurst:** Don't rush the implementation! Be as inclusive and transparent from day one to make sure everyone is on-board. Hold lots of meetings with employee representatives to fully explain the scheme. Only roll it out once fully satisfied that all data protection issues / clearances have been received – potentially a long process for multi-nationals. Make sure all compliance officers have been trained on the scheme and how to handle and report cases. Oh, and follow the data protection rules!

**Scott Killingsworth:** So just a short list then! I agree, there is much to consider, but the main thing of course is that the company must show by its actions that it takes whistleblower complaints seriously, that it is committed to finding the truth wherever the investigation may lead, and that when misconduct is discovered, it will take decisive steps to correct the problem. Credibility is everything. A more prosaic, practical challenge comes from the fact that a large proportion of whistleblower calls turn out to be minor workplace dissatisfactions, personality issues, etc., risking cynicism on the part of management. You have to crush tons of ugly rock to get a few ounces of gold, but it's worth it.

**Philip Brennan:** Getting this right is of course a matter of many of the above, as well as correct application in the organisation, taking into account its culture, environment and circumstances. I have a long list here for you Sharon (Philip waves a paper in his hand), I'll circulate it for you afterwards as I don't think we have time to discuss each of them! (Ed: We have published Philip's list at the end of this Round Table transcript).

**Klaus Moosmayer:** OK! But let me emphasize the matter of size and proportionality. Global companies certainly need a sophisticated system – able to comply with many different data privacy regimes globally; offering toll-free access in many languages around the world and so on. This is certainly not the right approach for an SME.[2] Here, a trustworthy "go to person" or external ombudsman would normally be sufficient. But one thing both have in

2 Small and Medium sized Enterprise.

## WHISTLEBLOWING – LOVE IT OR LOATHE IT

*The company has to clearly prohibit any retaliation against whistleblowers and treat such acts as violations of the Compliance rules which will not be tolerated*

common: any implementation will fail if top and middle management are not supporting the whistleblower system.

**Andrew Buckhurst:** Most importantly, the process should be on-going and not stopped once the whistleblower scheme has been implemented. It should be integrated in the company's Code of Conduct and employees trained, both in speaking up and in receiving "bad news".

**Pedro Montoya:** That's crucial. The company needs to explain that the whistleblowing system is built to protect the company interests and not to substitute a culture of transparent dialogue in the workplace. On the other hand, if the hotline is presented as the "last recourse", then it may be less effective, as employees may understand that they should not use it unless all other options are closed for them. The difficulty lays in the right balance when communicating on this topic. The other aspect to be underscored is the importance of providing sufficient feedback to the whistleblower and even going public within the Company on some of the investigations, when it is feasible.

**Sharon Ward:** We could discuss the difficulties, and the appropriateness of guaranteeing or promising best endeavors in assuring anonymity for those using such programmes. However, this is principally a concern only to protect the whistleblower from retaliation. Experience and studies seems to speak to at least a very significant minority experiencing retaliation. How should companies deal with situations where trust between colleagues appears to have gone past reparable levels?

**Philip Brennan:** Very few, if any, legal systems offer *actual* protection from retaliation. Many call it 'protection', but in reality it is redress after the event, normally by application to the court for protection or reinstatement. This in itself is often a significant deterrent to whistleblowers and one of the key reasons they choose to stay silent, unless the right environment is created by their employer.

**Andrew Buckhurst:** Clearly, the code of conduct (and by default the whistleblowing scheme) must set out very clearly that retaliation is absolutely

## WHISTLEBLOWING – LOVE IT OR LOATHE IT

not acceptable where someone has made a claim in good faith. They must be protected. However, they must also accept that realistically they cannot be put in a protective casing making them "untouchable" as an employee. We are dealing with ongoing personal relations and trust after all. Allegations made in good faith (even if the investigations do not conclude that there has been a violation) should be acceptable and the non-retaliation principle fully applies. If anonymity is impossible, people are required to "forgive and forget" and continue a normal working relationship – not an easy expectation.

**Klaus Moosmayer:** This is indeed a difficult topic, especially where the whistleblower was himself involved in the alleged scheme of misconduct. I would advocate for a clear and transparent guidance as part of the mandatory set of Compliance policies: the company has to clearly prohibit any retaliation against genuine whistleblowers and treat such acts as violations of the Compliance rules which will not be tolerated. On the other hand, reporting in bad faith is also a breach of the Code of Conduct and must be sanctioned equally, this has nothing to do with retaliation, but with the credibility of the Compliance system and is necessary to maintain the trust of employees and managers in a fair and due internal process.

**Scott Killingsworth:** With our preference for splintered, issue-specific regulatory solutions, the US has around 60 different whistleblower protection laws at the federal level alone, so companies operating in the US are well advised to adopt a broad-based, zero-tolerance anti-retaliation policy. There are undeniable difficulties: in particular, zero-tolerance means responding to minor incidents of retaliation before they escalate, but minor incidents can be very ambiguous as to whether retaliation is going on or not. And a whistleblower who has been "outed" is likely to interpret the actions of coworkers through a somewhat colored lens, which will produce some false positives. It's impossible to manage these situations perfectly but that is also true of many other personnel management problems.

## WHISTLEBLOWING – LOVE IT OR LOATHE IT

**Philip Brennan:** Essentially, and just as with the anonymity aspect we have just been discussing, boards and senior management must be absolutely clear and unequivocal that they will not tolerate retaliation by line bosses or colleagues. Where it occurs (and they must consciously guard against it) the response must be short, sharp and public.

**Sharon Ward:** As ever, the attitude of the board and senior management is critical to implementation. But it is soon time to bring our discussion on whistleblowing to a close. What though, does the future bring? How do you see best practice and technology changing the nature of whistleblower schemes going forward? Are there any utopic solutions waiting to be applied?

**Philip Brennan:** Looking to the future, best practice is slowly moving in the direction of whistleblowers being regarded as the good guys, rather than as 'snitches'. Compliance Officers have a major role to play in spreading the positive business and cultural case, as well as the legislative one (where it applies). In many cases, what is off-putting for those raising concerns is the fear and hassle of having to confront a superior on an issue where the superior is likely to be questioning or even defensive. Employees often base their concerns on observations and inclinations, rather than on hard evidence. But they are often right.

It is now possible to design highly secure web based technology for reporting. This is likely to be increasingly used as a medium for raising concerns. Rather than confronting a line manager face to face, employees can now have the opportunity to raise concerns on secure websites, from the comfort of their own homes. They can attach document, pictorial or video evidence obtained using their mobile phone for example and substantiate their case with a considered report rather than being interrogated or intimidated in face to face contact with their boss. This process too, is going online.

**Pedro Montoya:** I tend to agree, Philip, that technology may help to report more easily, but we have to be aware that it may also increase the risk of malicious whistleblowing. The use of colleagues who act as "ethics ambassadors" in

## WHISTLEBLOWING – LOVE IT OR LOATHE IT

*What is off-putting for those raising concerns is the fear and hassle of having to confront a superior on an issue*

proximity to the whistle-blowers may offer alternative ways to enable employees to speak up either openly or confidentially depending on the circumstances. The web may offer new tools, but the effort must be made in developing the environment in which those tools will be used. Like in most cultural issues, there are no magic formulas, but the need to be consistent and tenacious in building a culture of integrity and transparency is still the most important one.

**Klaus Moosmayer:** Technology apart, how do we encourage people to speak up? I think I've already made it clear that I am not in favour of financially incentivizing whistleblowing, but there might be other ways to think about rewarding whistleblowers differently: by a personal "Thank you" from the CEO or CCO, or by granting special Compliance awards. This puts the case in the positive light of recognized value added for the firm and tells a powerful story, an approach that might well be worth pursuing.

**Sharon Ward:** In summing up what has been a spirited and varied discussion, Andrew, the last word goes to you. Any final thoughts?

**Andrew Buckhurst:** Only to bring us back to our starting point: whistleblowing schemes seem set to be with us for good. Unfortunately there is no such thing as a perfect corporate culture and though a good one will certainly help reduce the use of a whistleblowing system, it will never fully take away the need for one. But if the scheme is implemented in a fully transparent way by those who are respected and trusted within the organisation, then the scheme will build traction with the employee base. There is a balance to be found, which will be different on a case by case basis and probably only learnt from experience.

**Sharon Ward:** Thank you everyone. We may like it or loathe it; but used correctly and applied with intelligence, whistleblowing and the organized schemes to support it looks here to stay.

## WHISTLEBLOWING – LOVE IT OR LOATHE IT

# TEN STEPS TO MAKING A WHISTLEBLOWER SCHEME AS EFFECTIVE AND INCLUSIVE A PROCESS AS POSSIBLE:

1. Demonstrable and unequivocal support from the Board and Senior Management is key. If there is any sense or post implementation evidence that a scheme is not taken seriously by either party it will fail. The Board and Senior Management should use clear unambiguous language along the lines of *"we support and encourage employees to raise concerns about wrongdoing and we will protect those who do from retaliation"*.

2. For employees who want to protect their identity, take all necessary steps to accommodate and support them.

3. As well as providing internal reporting channels, offer employees an alternative of reporting to a trusted external intermediary – a professional who works for the employer, but is not part of the firm. Some employees just won't take the risk of reporting internally.

4. The internal confidential recipient should not be from Human Resources. Employees will be fearful that their action in coming forward will form part of their HR record or at least be known by those with influence over reward and promotion.

5. Include employees in scheme design/ redesign. Launch the scheme like a new product. Provide training and information aids to both managers and employees. Managers must be ambassadors for the scheme rather than be in fear of it.

6. Refresh awareness frequently by training and feedback. Survey employees on their views. Address identified shortcomings.

7. Where concerns are about senior management, particularly the CEO, an avenue to the Senior Independent Director on the Board, whether directly or through a third party service provider, should be provided.

8. Concerned employees should be kept as informed as possible. Where this is not done, they are likely to use alternative channels or take alternative action to reiterate their concern. Give as much feedback as practical and legally possible at the end of the investigation to those who raise concerns. Include an appeal process.

9. Collect as much management information on the operation of the scheme as possible. Ensure it is discussed at senior management and board level and that lessons learned are acted on. Raising concerns must be positioned as a value adding activity. Do not hide the results. Share them and actions taken with employees and other stakeholders.

10. The scheme must always be portrayed as a collaboration between board, management and employees to eliminate wrongdoing and malpractice and create a better place to work.

# SUBSCRIPTION INFORMATION

## Subscription prices international*

| FTE's | Corporate | Universities |
|---|---|---|
| Personal subscription | | |
| 1 Hard Copy (6 issues) | € 195 | € 195 |
| 1 Online user | € 255 | € 255 |
| Institutional subscription | | |
| 3 Online users +1 Hard copy | € 450 | € 450 |
| 5 Online users + 5 Hard copies | € 550 | € 450 |
| 10 Online users + 10 Hard copies | € 750 | € 450 |
| >10 | To be negotiated | € 450 |

Online access includes the complete archive

Please go to our website for the general information regarding our journal subscriptions. http://www.baltzersciencepublishers.com

### New Subscriptions
Subscriptions start with the first announced issue of the calender year. If subscriptions are started in the course of the calender year the full subscription rate applies, and the subscriber will get full access to the archive of the journal.

### Change of address
Please mail your change of address to the address mentioned on the contents page, or consult the website.

### Terminating a subscription
Subscriptions can only be cancelled, by email or letter, until 1 December of the present subscription year. After this date subscriptions will be automatically renewed for the following year.

### Subscription Information
Details on subscription rates and offers are available on request from the publisher.



## Journal of Business Compliance

**Baltzer Science Publishers BV**
Amsterdam - Berlin
+31 6 53 88 1602
+49 30 679 60 435
info@baltzersciencepublishers.com
www.baltzersciencepublishers.com
ISSN 2211-8934
E-ISSN 2211-8942

*** For distribution and subscription in Germany, Austria, Switzerland and Liechtenstein please contact:**

**Erich Schmidt Verlag GmbH & Co. KG**
Genthiner Str. 30 G, 10785 Berlin, Germany
phone +49 30 250085 227
fax +49 30 250085 275
IBAN DE31 1007 0848 0512 2031 01
BIC (SWIFT) DEUTDEDB110
Vertrieb@ESVmedien.de
www.BUCOdigital.de
E-ISSN 2198-803X**

** This ISSN number is applicable for D, A, CH and FL

## Advertising Rate Card
2014 prices, excluding applicable VAT.

Full page
1x € 1000
5x € 750 (per page)

Half page
1x € 600
5x € 450 (per half page)

For technical instructions please contact the marketing/sales department: info@baltzersciencepublishers.com