



# Digital Age Compliance

The serial fraud cases in Japan in 2017 and the limit of Mura society

In September 2017, a major Japanese car giant announced that non-certificated employees had been conducting tests on their automobiles. A month later another industry giant also announced inappropriate automobile testing processes. Subsequently in November, two other Japanese major name manufacturers announced data falsifications. Investigations to date indicate the cause of these issues to have been a “lack of compliance”. However, an important question these incidents have raised in order to understand this issue for the future, is “why now?” and “why could they not hide these issues anymore?”

## Compliance Program Became a Dead Letter

“Fraud will never disappear” is a commonly said phrase in risk management. If this is true, it is a waste of time to take measures which aim to completely prevent risk. However, preparing strategies to minimise damage is of utmost importance for a company’s future prosperity, reputation and survival. To minimise the damage caused by fraud, it is critical to assess where the risks are, what the damages would be (risk assessment) and to prepare appropriate risk management measures.

It is not sufficient to just have a risk management system or a compliance program, it needs to be a system and a program that actually works as it was intended to. Even if a company has nicely worded and structured policies in place, it is always human error, a misjudgement or an individual wilfully exploiting an opportunity that results in violation. Risk management and compliance systems ultimately rely on each individual employee’s “awareness” as to whether or not fraud occurs. The crucial factor is whether the systems can have a strong influence on this “awareness”.

Although, there are several points that the serial fraud incidents revealed in 2017 have in common, the most notable uniqueness from the point of risk management is that all were listed companies which we automatically assume would have good compliance programs. Yet the fraud happened due to a “lack of

compliance”, which suggests that even compliance programs at the large international leading Japanese companies have become a dead letter.

At the related press conferences, we heard comments from executives which support this speculation. For example, one of the firms commented:

“We found the fraud more than a year before, but we did not announce it because there were no safety issues (of cars). However, we decided to announce this now, as there were postings (which leak the information on the fraud) on the internet BBS.”

They also commented that they would have not have announced the issue if one of the other firms had not disclosed their issue previously.

Another of the firms commented: “Thus far, problems were solved if we discussed them with customers” – a typical Japanese business practice when issues are discovered. However, this kind of comment from top management may give an impression of Japanese companies going backwards while compliance programs are aggressively progressing internationally.

The media responses from overseas were harsh. They pointed out the cause for the lack of compliance to be the tendency to hide

issues triggered by the seniority-based wages system in Japan, or serious cost reduction plans due to the economic downturn which created too much pressure on employees, or the harmful effects of quality supremacy which has been supporting the pride behind the “Made in Japan” slogan. These are all responses that are based on the so-called “fraud triangle” (opportunity, pressure and rationalisation).

The heavy sanctions on Japanese companies from the DOJ and EU commission regarding violation of Anti-trust or FCPA laws, and, as the bid-rigging incident regarding the linear Shinkansen (bullet-train) detected by the Fair-Trade commission in December 2017 indicates, have made it very clear that the traditional Japanese business style is no longer applicable.

Due to the overwhelming push for greater transparency and accountability on compliance around the world, the Japanese government and related agencies have been revising laws and policies. They have installed the leniency program and stock exchanges applied new rules and guidance. Responding to this many major Japanese companies set up a Compliance department, attempted to review existing compliance policies, and employees started to attend seminars held by law firms or consulting firms to learn what should be done and changed. Nevertheless, the series of fraud cases revealed in 2017 substantiates claims that these changes, assuming to catch up with global standards at major Japanese companies, were perhaps a formality only.

Company	Background
September 2017 <b>Japanese Motor Co. #1</b>	<ul style="list-style-type: none"> <li>Issue reported by Whistle-blower</li> <li>The Ministry of Land, Infrastructure and Transport (“MLIT”) conducted a surprise inspection</li> <li>Fraud was identified</li> <li>Public announcement</li> </ul>
October 2017 <b>Japanese Motor Co. #2</b>	<ul style="list-style-type: none"> <li>After the above announcement, MLIT notified car manufacturers to conduct internal investigations</li> <li>#2 conducted investigations</li> <li>Fraud was identified</li> <li>Public announcement two weeks after fraud was found</li> </ul>
October 2017 <b>Japanese manufacturer #1</b>	<ul style="list-style-type: none"> <li>Conducting check-ups on their entire manufacturing process</li> <li>A factory reported an issue</li> <li>Head office confirmed the fraud</li> <li>An announcement was not made for several years</li> </ul>
November 2017 <b>Japanese manufacturer #2</b>	<ul style="list-style-type: none"> <li>A subsidiary found fraud during their quality control checks</li> <li>No action was taken</li> <li>It was reported to the parent company about six months later</li> <li>Public announcement</li> </ul>
November 2017 <b>Japanese manufacturer #3</b>	<ul style="list-style-type: none"> <li>Fraud was discovered in July 2016 during their internal survey</li> <li>No initial announcement</li> <li>Announced a year and half later following BBS postings</li> </ul>

## Current Situation of Whistle Blowing

It is said that the large companies with perfunctory compliance programs have created a “Mura” society. “Mura”, which means “village”, is a very closed society/organisation that has a strong fellowship. They prioritise Mura rules over rules outside of the Mura. The Mura rules are only applicable within the specific Mura. People in the Mura would not have reacted even if fraud was hidden within the Mura. It becomes easy to understand why such incidents happen if we apply the Mura theory to the major companies’ fraud cases.

As an example, a Mura society within Company A had unwritten Mura rules such as “there is no choice but to ship out our product even if there was fabricated data, as long as there is no change to the safety of the product. Above all, there is no need for us to disclose the internal (Mura/family) issue to the public (while there is no harm to customers)”. This Mura rule takes priority over any global law. As long as people follow this Mura rule, individuals are protected and no one gets hurt. Further to this the key players of Company A have strong connections with politicians and government officials – they know the new regulations. They will update their dead letter compliance program which will look fine to regulators. What the A Mura people are most afraid of is “Mura Hachibu” which they will be exposed to should they violate Mura rules rather than the rules set out by the authorities.

The below data reflects this tendency.



<sup>1</sup> [http://www.caa.go.jp/planning/koueki/chosa-kenkyu/files/chosa\\_kenkyu\\_chosa\\_170104\\_0003.pdf](http://www.caa.go.jp/planning/koueki/chosa-kenkyu/files/chosa_kenkyu_chosa_170104_0003.pdf)

“No chance of change even if I reported” indicates there are Mura rules prioritised over other rules.

“Afraid of retaliation” indicates that they have seen retaliation actually happen or might have heard of the rumour or threat of retaliation.

In addition, according to the following data, 62 percent out of all whistle-blowers were actually retaliated against.

<b>Number of contacts between 2010 to 2016</b>	<b>178 cases</b>	
<b>Actually reported the issue</b>	<b>63 cases</b>	<b>35%</b>
<b>Retaliated or disadvantaged after reporting</b>	<b>39 cases</b>	<b>62%</b>

(Tokyo Bar Association- Whistle-blower Statistics)<sup>2</sup>

The total number above is from less than 200 cases researched by the Tokyo Bar Association; however, it becomes evident that the “Mura Hachibu” system still exists within Japanese companies when you view these research results together with the Consumer Agency’s data.

There are two systems for internal reporting; one is to have a hotline directed to an internal function, the other is to have it outside the company. It is difficult to decide which function should be the receiver of the hotline calls when setting up internally.

HR or the audit department, which are supposed to be neutral and independent, also consist of company employees which make whistle-blowers worry about whether their performance evaluations may be impacted, or whether their speaking out may lead to demotion or reputational damage and repercussion.

Having an external hotline raises concerns for whistle-blowers about disclosing the issue as the receiver may not know anything about the company, the industry or the culture of the organisation, or there are concerns about whether anonymity and privacy is actually protected even through a third party.



It has now become very difficult for large companies to maintain and hide lack of clarity and fraud due to the development of the internet.



Out of 35 percent of Mura people who finally overcame their anxiousness and reported the issue, more than half were retaliated against. Under these circumstances, it is understandable and natural to believe that whistle-blowing is a highly risky thing

to do with a high likelihood of some personal damage and with little being done in response to the reporting anyway.

For these reasons the whistle-blowing system in Japan which was implemented within compliance programs along recommended advice from the authorities became a system that no one ever uses.

### “Internet Accusation”

It is not easy to understand exactly how fast and to what extent information can be spread through the internet unless you have actually used and experienced internet tools such as Twitter, Instagram or BBS (so-called Keijiban). Whatever the content the posted, information will be shared, disseminated globally, and infiltrated (or saved) **in an instant**. There are many convenient and effective tools for whistle-blowers even if a company has tried to hide their issues, or has a corporate culture which does not encourage employees to speak out



The “AI Industry Revolution”<sup>3</sup> generated by rapidly developing AI technology promises efficiency and accuracy of work. However, the core issue will still be human error, as it is humans, not machines that commit wrong doings.



Executives at Japanese companies who have never used such internet tools may still think “people will not believe unreliable information on the internet”. However, the credibility of information on the internet is not always questioned and it has notably improved over the last decade. People tend to believe information on the internet more than ever. Many executives at foreign companies use LinkedIn or Facebook to disclose their profiles. We are all aware that even a country president will now have an account on Twitter through which he can openly criticize media or other countries through “tweeting”. This is because they know that using these tools is the most efficient and effective way to assume transparency, communicate, win trust and be influential.

Japanese companies need to disclose information more proactively in internet society. It has now become very difficult for large companies to maintain and hide lack of clarity and fraud due to the development of the internet. It is also worth noting that the new generation who will soon enter the business society were born after the year 2000 and grew up with smart phones. Their understanding is that information is disclosed and shared, or even if it was not disclosed someone will leak or tweet it.

<sup>2</sup> [https://www.toben.or.jp/know/iinkai/koueki/news/post\\_11.html](https://www.toben.or.jp/know/iinkai/koueki/news/post_11.html)

<sup>3</sup> 日経新聞 2018年1月16日

The “AI Industry Revolution”<sup>4</sup> generated by rapidly developing AI technology promises efficiency and accuracy of work. However, the core issue will still be human error, as it is humans, not machines that commit wrong doings.

While the digital medium is becoming the nest of fraud, it is also digital tools that search out fraud. In the near future, it will be main stream that part of compliance will be simplified through widespread AI monitoring technology.

It is likely that this new generation will not blend in with the traditional Mura society and will pose various kind of questions on the nature of companies which have not been addressed up to now. Companies have to get ready for the new generation as soon as possible.

*Author: Sayaka Kobayashi*

---

<sup>4</sup> 日経新聞 2018 年 1 月 16 日

The views expressed herein are those of the author(s) and not necessarily the views of FTI Consulting, Inc., its management, its subsidiaries, its affiliates, or its other professionals

Ben Fouracre  
Japan Representative  
+81 3 5369 3939  
ben.fouracre@fticonsulting.com

Ryo Fujita  
Director  
+81 3 5369 4145  
ryo.fujita@fticonsulting.com



## About FTI Consulting

FTI Consulting is an independent global business advisory firm dedicated to helping organisations manage change, mitigate risk and resolve disputes: financial, legal, operational, political & regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centres throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities. Connect with us on Twitter (@FTIConsulting), Facebook and LinkedIn.