tis

EXECUTIVE BRIEFING

CFOs in the Firing Line!

How to Improve Sanctions Screening and Compliance While Avoiding Personal Liability

Learn more at tis.biz »

THE IMPORTANCE OF GOVERNMENT-IMPOSED SANCTIONS

Government-imposed sanctions on who companies can trade with and how are changing almost daily. At the same time, CFOs are becoming personally responsible for sanctions violations relating to payments – and the size of fines imposed on errant organizations is snowballing. How, then, can finance leaders tackle these issues to minimize the risk of sanctions breaches, improve payments workflows, and ultimately, avoid severe legal consequences?

If the importance of sanctions compliance wasn't already on every CFO's mind, the case of Huawei's Meng Wanzhou brought the matter clearly into focus. In December 2018 1, Wanzhou, the CFO – and the daughter of the company's founder and its CFO – was arrested in Canada at the request of the US authorities for allegedly helping to cover up sanctions' violations relating to Iran.

Putting all of the intricacies of the Huawei case aside, it did shine a spotlight on the personal and professional consequences of sanctions violations. CFOs can and will be made examples of by the law – as members of the senior management team, they are responsible for compliance. Certain regulations, like those covering organizational negligence, also make individuals personally liable for company failings.

Non-compliance is often far more expensive than compliance itself

It is not just the US that is taking a hard line on sanctions violations, either. Across the globe, governments are cracking down on missteps made by individuals and organizations. In September 2017, for example, the Den Bosch Court in the Netherlands sentenced a former managing director of a Dutch company to almost two years' imprisonment, because he violated EU sanction regulations 2.

And the list of fines imposed on businesses, ranging from cosmetics to telecommunications and from electronics to banking, in recent years is eye-watering (see figs. 1 & 2).

In addition, companies also often suffer significant reputational damage as a result of sanctions violations. The negative impact on a firm's stock market price as a result of a compliance breach has been shown to be, on average, nine times the size of the fine imposed by the regulator 3.

Companies that breach sanctions may also find that buyers and suppliers no longer want to do business with them. Similarly, shareholders may turn their backs on companies seen to have been in violation of sanction rules. Bank funding arrangements are also potentially at stake. Breaches can result in banks terminating business relationships, cancelling loans, or leaving funds frozen in escrow accounts for long periods of time. In other words, non-compliance is often far more expensive than compliance itself.

Nevertheless, there is no need to panic. While the severity of sanctions violations may be increasing, much can be done to minimize compliance risks. The starting point is to understand where the exposures lie.

What are sanctions?

Sanctions are restrictive measures imposed by national or supranational governments to bring about a change in policy or activity by the target country, part of country, government, entities or individuals, in line with certain foreign policy objectives.

Common objectives include:

- Promoting international peace and security
- Defending democratic principles and human rights
- Preventing the proliferation of weapons of mass destruction
- Fighting terrorism
- Support of the national economy

What types of sanctions exist?

- Embargoes
- Trade restrictions, such as import and export bans
- Restrictions of free movement, such as visa or travel bans
- Financial restrictions
  - Prohibition of making available funds or economic resources
  - Freezing of funds and economic resources
  - Prohibition of providing financing or financial assistance related to certain goods or services

Figure 1
Recent US Sanctions Violations Penalties

Company	Sector	Year	Fines (in USD)
e.l.f Cosmetics Inc.	Cosmetics	2019	996,080 [4]
Ericsson	Electronics	2018	146,000 [5]
Zoltek	Materials	2018	7,772,102 [6]
Yantai Jereh Oilfield Services Group Co.	Oil & Gas	2018	2,774,972 [7]
Société Générale	Banking	2018	53,966,916 [8]
Zhongxing Telecommunications	Telecomms	2017	100,871,266 [9]
CSE Global Ltd	Technologies	2017	12,027,066 [10]

Figure 2
US Record Penalties

Company	Sector	Year	Fines (in USD)
Société Générale	Banking	2018	1,340,000,000 [11]
Commerzbank	Banking	2015	1,450,000,000 [12]
BNP Paribas	Banking	2014	8,900,000,000 [13]
HSBC	Banking	2012	1,900,000,000 [14]

[1] edition.cnn.com/2018/12/06/tech/what-is-huawei/index.html
[2] www.kneppelhout.com/news/hard-jail-time-for-a-substantial-period-after-violation-eu-sanction-regulations
[3] voxeu.org/article/financial-market-wrongdoing-fines-vs-reputational-sanctions
[4] www.wsj.com/articles/u-s-sanctions-compliance-fines-hit-decade-high-11564057920
[5] www.ft.com/content/1a588832-d2a7-11e8-a9f2-7574db66bcd5
[6] www.freightwaves.com/news/missouri-firm-fined-for-belarus-sanctions-violations
[7] www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20181212.aspx
[8] www.refinitiv.com/content/dam/marketing/en_us/documents/infographics/fines-for-banks-that-breached-us-sanctions-infographic.pdf
[9] www.treasury.gov/resource-center/sanctions/CivPen/Documents/20170307_zte.pdf
[10] www.straitstimes.com/world/united-states/singapore-tech-firm-cse-global-fined-us12-million-for-apparent-violation-of-iran
[11] www.straitstimes.com/business/banking/french-bank-societe-generale-fined-us13b-for-violating-us-sanctions
[12] www.refinitiv.com/content/dam/marketing/en_us/documents/infographics/fines-for-banks-that-breached-us-sanctions-infographic.pdf
[13] www.refinitiv.com/content/dam/marketing/en_us/documents/infographics/fines-for-banks-that-breached-us-sanctions-infographic.pdf
[14] www.refinitiv.com/content/dam/marketing/en_us/documents/infographics/fines-for-banks-that-breached-us-sanctions-infographic.pdf

PINPOINTING THE RISKS

In light of globalization, the majority of companies have exposure to international counterparties. Nevertheless, not all organizations have the same level of risk when it comes to sanctions violations. Certain industry sectors are much more vulnerable to breaches, given the nature of the work they undertake and the volume of international payments they process. The most at-risk sectors include:

Defence and security
- Banking
- Oil and gas
- Insurance
- Manufacturing

Of course, the countries where organizations operate also often pose threats. Each sanctions regime – US, EU, or another regional or national initiative – will have its own watchlist of 'high-risk countries'. For reference, examples from the Office of Foreign Assets Control (OFAC) in the US include (not exclusively):

- Belarus
- Cuba
- Democratic Republic of Congo
- Iran
- Iraq
- North Korea
- Syria
- Zimbabwe

Certain departments within a company are also more likely to be affected by sanctions. While it depends on the organizational structure of the business, alongside finance, those likely to be on the front line are: sales, trade (finance), procurement, and contract management.

WHY IN-HOUSE SCREENING MATTERS

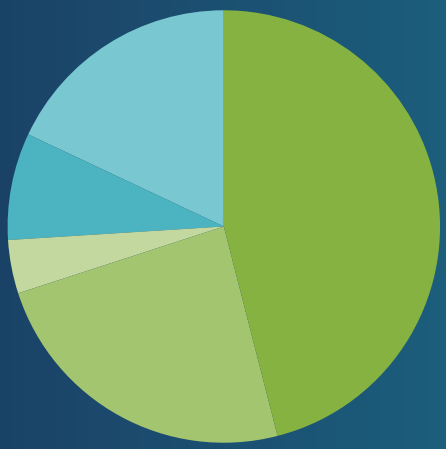
For finance, the most significant risk lies in payments processing. It is important that a company can flag potential violations against sanction lists before these payments are sent to their bank. Regulators consider a lack of adequate systems in place to run a sanctions compliance programme comparable to non-compliance and misconduct. So, even without a breach, the implications of not being on top of payments compliance are extremely serious.

On the other hand, a complex compliance system, which significantly impedes future compliance breaches, can lead to fines being reduced or even dropped in the event of a compliance breach.

Indeed, in this era of heightened risk and responsibility, all companies should be screening 100% of their outgoing payments against regulatory watchlists and in-house blacklists (customised to the company) – as a matter of routine. Performing the screening before the payment reaches the bank means that the organization remains in control and can deal effectively with any transaction that raises a red flag by e.g. contacting a supplier directly. This is an important distinction to make, because once a bank detects a sanctions breach, it is reported directly to the regulator – not to the payment originator and funds can be frozen, often for long periods of time. This removes any form of control over the situation for the corporate and can lead to tensions in the supply chain.

Screening in-house also prevents friction between the company and its bank(s) as banking partners increasingly expect companies to ensure their payments are compliant – and any 'bad behavior' may reflect poorly on the organization, negatively impacting the overall bank relationship. Auditors are also likely to be unimpressed by any breaches.

So, how can organizations go about screening payments in-house? What does best practice dictate and what are the common mistakes to avoid?



Source: 2019 TIS Sanction Screening Survey Report

Figure 3
What Proportion of outgoing payments does your company screen?

- 46 % All outgoing payments
- 24 % A large part of the outgoing payments
- 4 % Less than 60 percent
- 8 % Only a faction of the outgoing payments
- 18 % Do not know

STANDARDIZE AND DIGITALIZE

The first step is to standardize payments processing across the organization. This will help to minimize the risk that exists from various subsidiaries using different enterprise resource planning (ERP) systems, and / or different methodologies for screening. A standardized payments process brings with it visibility and control, which, in turn, enables screening of payments in a standardized environment. Some organizations still perform screening manually, but there are obvious risks here – ranging from the use of out-of-date sanctions lists to errors, oversights and inconsistencies. Resources in finance and IT departments (which often are responsible for maintaining the sanctions lists) are also diverted from more value-added tasks.

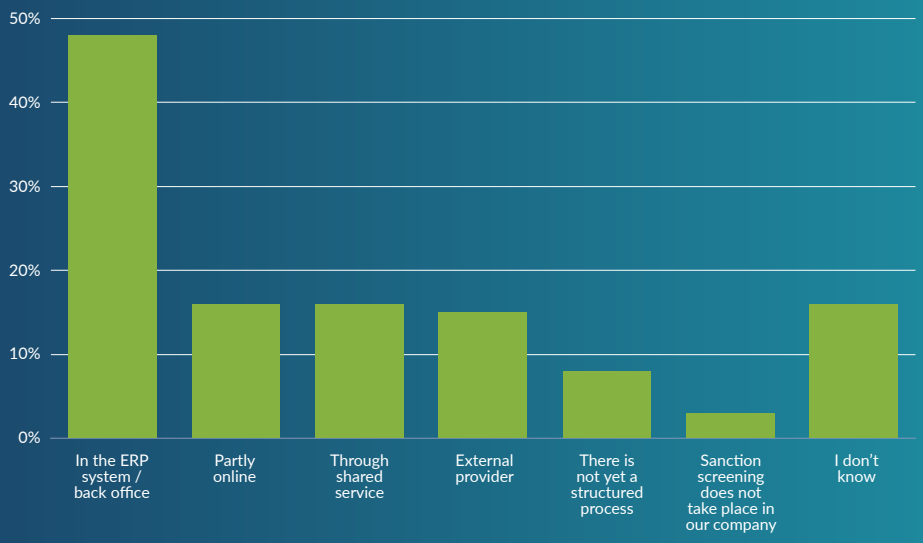
Technology is therefore the preferred route, with automation offering the power to enhance payment transaction screening. This ensures that more thorough screening takes place, without the limitations of manual processing. Companies take a variety of approaches to technology solutions (see fig. 4). Not all sanctions screening solutions are created equal, however. While many CFOs choose to use SAP and/or non-SAP ERP systems for this functionality, the majority of systems screen only circa 60% of outgoing payments.

What about the remaining 40%? This is most likely due to various ERP systems being used in large organizations and not all systems can be programmed to do the same things in the same way across the globe. Often smaller subsidiaries do not have the same level of sophistication in their ERP installations.

Systems integration is another concern – many organizations lack a proper interface or end-to-end connectivity for the entire payment processes. This includes everything from custom in-house systems to HR solutions, TMSs and ERPs – depending on each company's systems' infrastructure. By linking all systems that produce payment files seamlessly to a sanctions screening solution, compliance can be achieved, protecting organizations and individuals.

An essential ingredient of a successful sanctions screening solution is a fully comprehensive cloud-based platform. One that produces effective results, based on sanction- and black-lists updated in real time. Opting for a software-as-a-service (SaaS) solution will also mean that no intrusive IT project is required to implement the solution – which should help CFOs to build the business case for investment.

Figure 4
What Proportion of outgoing payments does your company screen?



Source: 2019 TIS Sanction Screening Survey Report

OPTIMIZING THE SET-UP

Making the most of any sanctions screening solution requires a standardized process to be defined from the outset. It is therefore wise to think about:

1. Defining a screening policy and procedure

What must be screened? How often should screening happen? How are alerts dealt with and by whom? How can alerts be resolved if information is unavailable or incomplete? How are suppliers notified? What happens if a breach occurs, in spite of screening? What remedial steps can be taken? How might the rest of the group be impacted?

2. Appointing a responsible and capable person(s)

The employee(s) in charge of monitoring sanctions requirements must have appropriate skills and experience in understanding the nuances, together with the technical capabilities to use any screening software. Moreover, the responsible person(s) should be screened themselves to ensure complete transparency.

3. Ensuring in-house communication

Companies must ensure in-house communication, so that a transaction can be stopped immediately in case of sanctions issues.

4. Provision of relevant resources

Relevant work materials and resources should be made available to employees. In particular, these should include relevant legal texts and sanctions screening guidelines. Such can also be official notices such as the Official Journal of the European Union and corresponding official national publications.

5. Building a culture of awareness

While technology plays a critical role in mitigating the risk of sanctions violations, so do people. The entire finance function should be aware of the importance of compliance and following proper processes and procedures. Regular trainings of employees can help improving sanctions screening skills and raising awareness. They should also be trained on the appropriate response to a breach scenario. Training results should be recorded in work instructions.

6. Stricter governance

Undertaking an overhaul of the company's approach to sanction screening presents a great opportunity to review the supplier selection process. Is stricter due diligence required? Are there any additional criteria that should be added given the growing focus on corporate social responsibility among regulators, auditors and investors?

7. Testing and reviewing performance

Regular monitoring of the chosen sanction screening solution should help to assess its effectiveness in managing the company's risks. Metrics, analysis and reporting may be useful – especially in larger organizations.

PEACE OF MIND

Taking the above steps should help CFOs to maximize the value of sanctions screening software and ultimately protect the organization against the financial and reputational damage of a non-compliance incident.

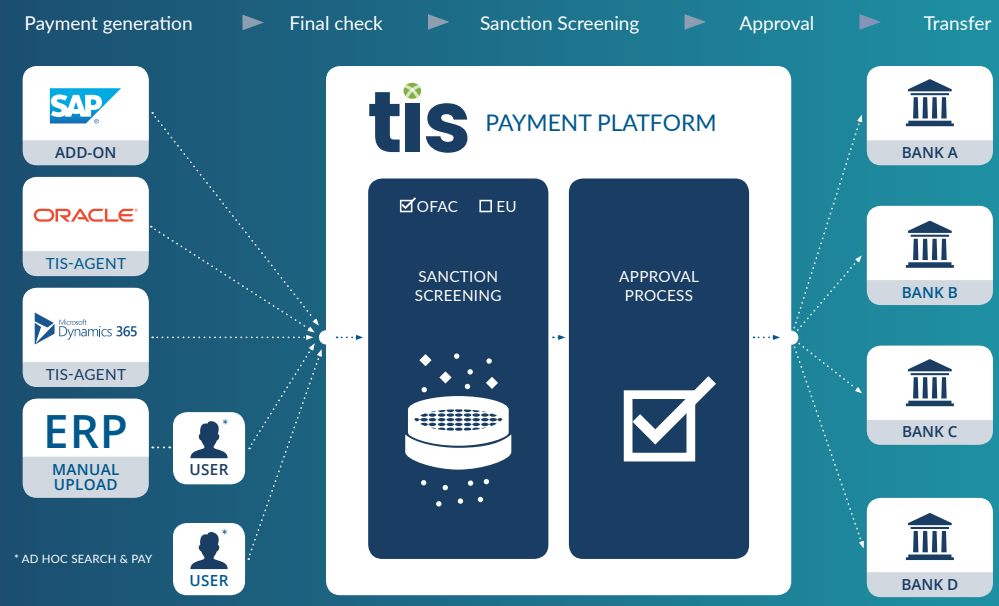
Following this roadmap should also help to demonstrate to regulators that everything possible has been done internally to minimize the potential for a sanctions breach – thereby protecting the CFO from personal liability.

THE TIS DIFFERENCE

TIS Sanction Screening reviews 100% of the payments, including manual items and those made by third parties such as payroll providers. The TIS solution makes this possible because all files are sent to the TIS platform to (format and) send to the company's designated banks. This risk-based, customizable, cloud solution gives end-to-end control over the payments process, from the ERP system (or e.g. TMS) to the bank (see fig. 5), and enables CFOs to be compliant – quickly, easily and reliably.

Find out more by downloading our comprehensive factsheet at:
www.tis.biz/en/portfolio/paygrid-simplify-sanction-screening

FIGURE 5
Standard payment flow to the bank



At TIS, we offer a secure, cloud-based platform which acts as a single point of contact for the entire finance function, allowing all payment transactions to be combined in a uniform way across the company. The platform offers a comprehensive Sanctions Screening solution – a customizable, cloud-based solution for payment screening and compliance management – visit www.tis.biz and request a demo.

Learn more at tis.biz »

ABOUT TIS

TIS is reimagining the world of enterprise payments through a cloud-based platform uniquely designed to help global organizations optimize outbound payments. Corporations, banks and business vendors leverage TIS to transform how they connect global accounts, collaborate on payment processes, execute outbound payments, analyze cash flow and compliance data, and improve critical outbound payment functions. The TIS corporate payments technology platform helps businesses improve operational efficiency, lower risk, manage liquidity, gain strategic advantage – and ultimately achieve enterprise payment optimization. Visit tis.biz to reimagine your approach to payment

Enterprise payments reimagined.

Learn more at tis.biz »

TREASURY INTELLIGENCE SOLUTIONS GMBH

Germany (+49 6227 69824-0) | United States (+1 (617) 955 3223) | info@tis.biz | www.tis.biz