CSI

2020 SANCTIONS COMPLIANCE REPORT

A Roadmap
for Compliance in 2020

Collision Course

Are you prioritizing sanctions compliance?

Today's technology empowers organizations to engage a global pool of customers. But with this digital reach comes increased scrutiny to ensure your organization remains compliant with the latest sanctions regulations. Those who negate this responsibility are unnecessarily setting themselves on a potential collision course with regulatory agencies.

Indeed, regulators are prioritizing sanctions compliance at all U.S. organizations and their foreign subsidiaries, and by their domestic and foreign employees.

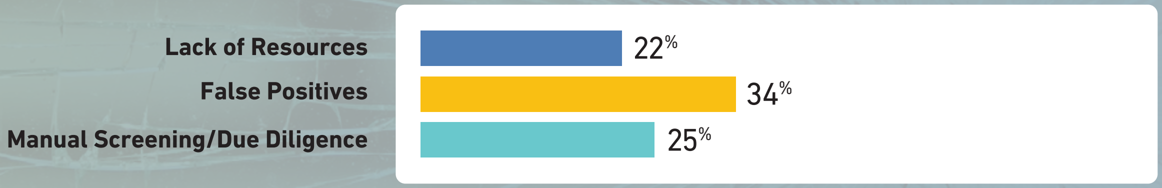
CSI's 2020 Priorities for Compliance Leaders survey reveals that those on the receiving end of this scrutiny are routinely frustrated by obstacles hindering their compliance, and they're demanding solutions to streamline them.

In response, this paper outlines a resource-maximizing roadmap that will help your organization navigate sanctions screening and bolster your overall compliance.

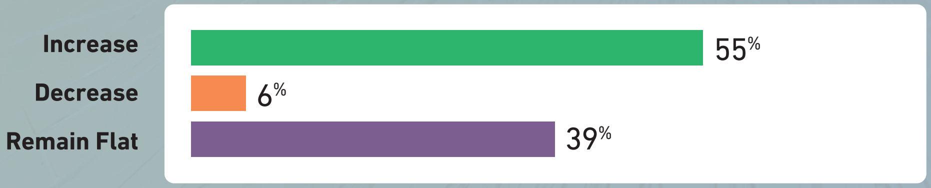
The 224 compliance leaders who participated in the survey represent organizations of all sizes (less than $250 million up to more than $5 billion in revenue) and a variety of industries, including financial services, healthcare, technology, business services, non-profits and more.

The consensus of that group is that false positives, manual screening and lack of resources are the biggest hindrances to their sanctions compliance. Furthermore, the majority (55 percent) plan to increase spending on compliance initiatives this year.

What is the biggest hindrance/obstacle to your sanctions screening program?



What are your plans for spending on compliance initiatives for 2020?



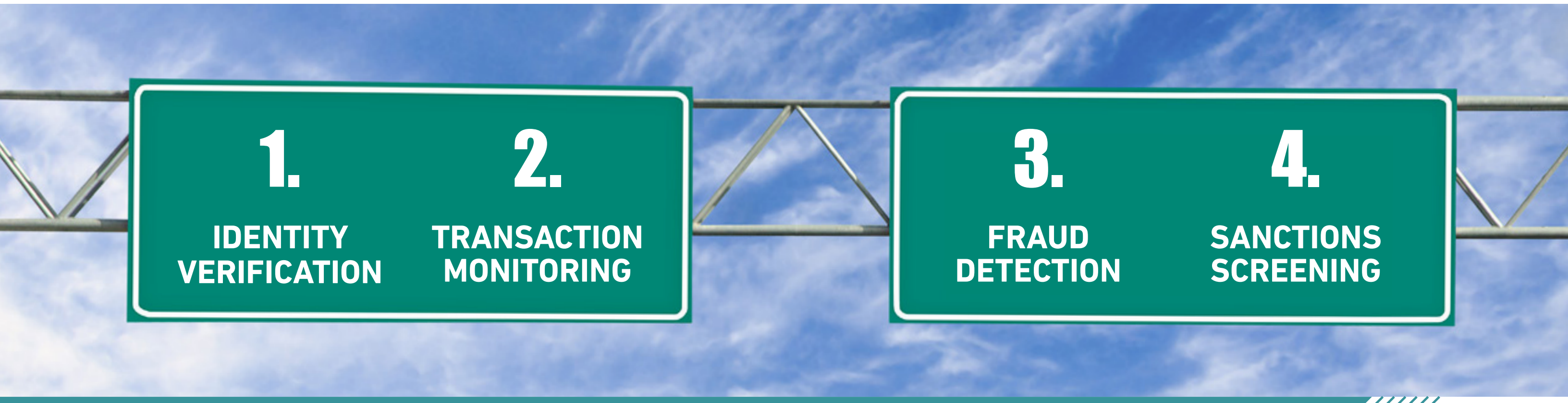
Current Road Conditions

Are you at higher risk for sanctions violations?

FinCEN considers the following industries and businesses as financial institutions because they are at higher risk for sanctions-related violations:

- Depository institutions
- Credit card companies
- Credit unions
- Securities and commodities dealers/brokers
- Currency exchanges
- Investment banks
- Insurance companies
- Money Service Businesses (MSBs)
- Casinos
- Real estate firms
- Travel and tourism operators
- Importers and exporters
- Jewelry, precious gem and metal dealers
- Vehicle, boat and aviation dealers
- Non-profits and charities

As such, they are required to establish a program that encompasses four main functions for preventing and detecting financial crimes:



3.1/5

★★★☆☆

Sanctions Screening was ranked on our survey as one of the most important (3.1/5) of these functions, making it the focus of this roadmap.

Zeroing in on Sanctions Screening

The United States has used sanctions to promote national security and foreign policy goals throughout its history. Today, however, national and international sanctions regulations are more complex than ever. This makes it extremely difficult for U.S. organizations to keep track of sanctions changes and, ultimately, to comply with them.

As a result, between 2006 and 2019, the Office of Foreign Assets Control (OFAC) issued more than $5.66 billion in sanctions-related enforcement actions.

Notably, these sanctioned entities were not limited to FinCEN-defined financial institutions. In fact, significant fines were levied against a variety of large international organizations as well as small local firms. In particular, the enforcement actions reveal these industries at high risk for sanctions violations:

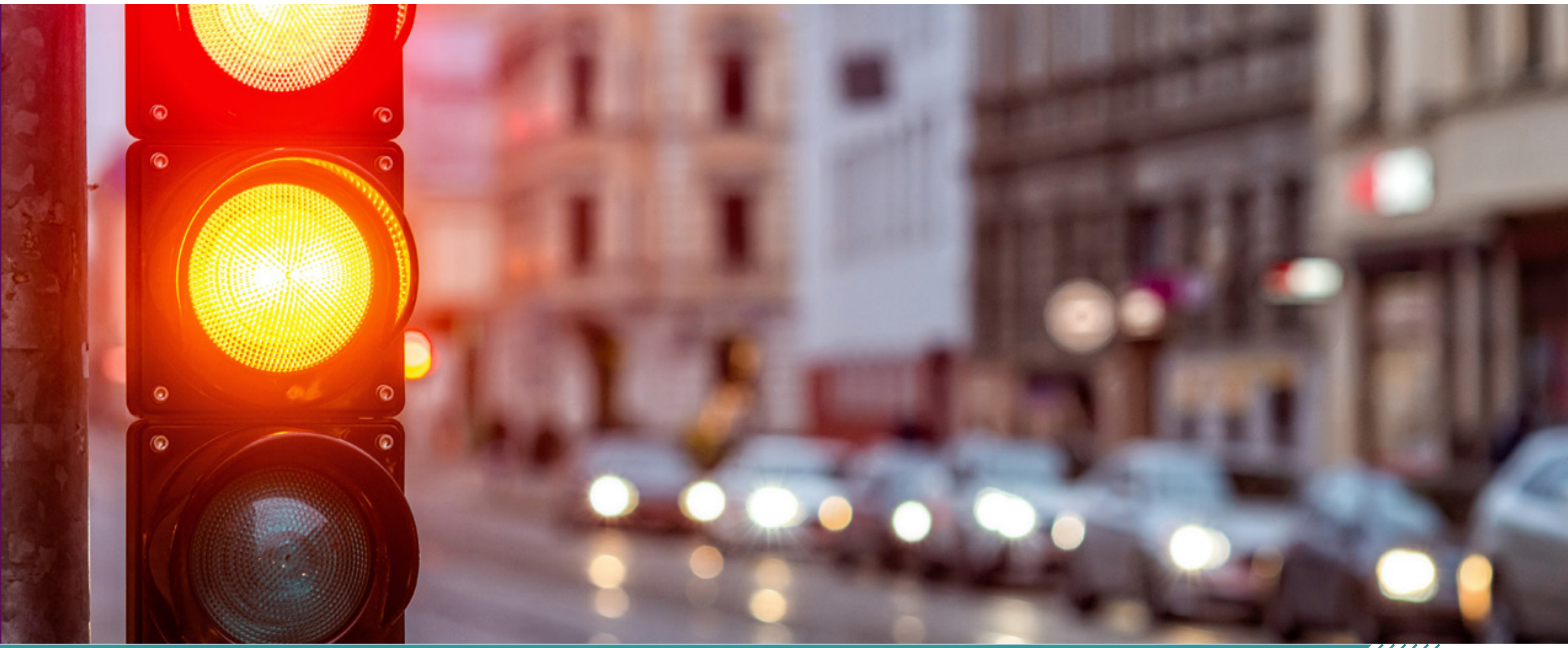
- Energy and fossil fuel
- Technology and data processing
- Electronic payments and trading entities
- Transportation and logistics
- Retailers and distributors
- Suppliers and manufacturers

Warning Signs

Why is sanctions screening important?

Public accounting and consulting firm Crowe advises that due to a growing set of economic, geopolitical and counter-terrorism challenges, “sanctions have become the policy tool of choice for world governments, particularly in the West.”

Because sanctions are a governmental tool used to deal with international problems, many fail to connect it directly to their organizations, especially those who conduct most of their business entirely in the United States, like 77 percent of our survey respondents.



Relating the macro strategy of sanctions to your organization boils down to understanding the need to protect three vital and interconnected interests through a sound sanctions compliance program:

1

UNITED STATES
Terrorist attacks, drug trafficking and other criminal activity can affect the physical safety of all citizens and harm the economic security of every organization.

2

U.S. FINANCIAL SYSTEM
When criminals use U.S. banks and other entities to facilitate their illicit or terrorist-related activity, it jeopardizes the entire financial system.

3

YOUR ORGANIZATION
Failure to have an effective sanctions compliance program puts you at greater risk of being used for financial crime, which can hurt your reputation and lead to expensive regulatory enforcement actions, both of which can negatively affect your business success.

Route Guidance

Which route do regulators recommend?

Survey respondents expressed the most confidence (3.6/5) in the risk management of their sanctions screening, over that of their transaction monitoring, case management or fraud mitigation. However, recent guidance suggests regulators have far less confidence.

3.6/5

CONFIDENCE IN RISK MANAGEMENT

OFAC and DOJ Offer Compliance Guidance

The Department of the Treasury's A Framework for OFAC Compliance Commitments and the Department of Justice's Evaluation of Corporate Compliance Programs both outline similar themes and signify a heightened prioritization of risk-based, comprehensive corporate compliance.

Specifically, OFAC's Framework strongly encourages all U.S. organizations "to employ a risk-based approach to sanctions compliance by developing, implementing, and routinely updating a sanctions compliance program (SCP)."

It also states that OFAC will now take the existence of an organization's formal SCP into consideration when investigating potential sanctions violations. Moreover, the lack of one may be used to deem a case as egregious, which can significantly increase its fine.

Summarizing OFAC's Framework

Beyond an occasional check or even the dutiful screening of organizational databases against OFAC's Specially Designated Nationals (SDN) list, the Framework envisions a formal and comprehensive SCP that includes five key elements:

1. MANAGEMENT COMMITMENT

- Review, approve and promote the written SCP
- Appoint a dedicated OFAC sanctions compliance officer who directly reports to senior management and has appropriate authority, autonomy and resources (human, IT, etc.)
- Understand the weight of violations and implement measures to reduce them

2. RISK ASSESSMENT

- Consider the potential risks to "inform the extent of the due diligence efforts at various points in a relationship or in a transaction," including on-boarding and mergers and acquisitions
- Develop a methodology to identify, analyze and address identified risks

3. INTERNAL CONTROLS

- Design, communicate, implement and enforce appropriate policies and procedures
- Ensure information technology aligns with them
- Develop adequate recordkeeping policies
- Appoint staff to fully integrate Internal Controls and address any weaknesses in them

4. TESTING AND AUDITING

- Create an independent audit function, accountable to senior management, which is conducted by someone with sufficient authority, skills, expertise and resources
- Use testing procedures that produce comprehensive and objective results
- Take immediate action to mitigate confirmed weaknesses identified through testing

5. TRAINING

- Provide adequate and regularly scheduled employee training, plus tailored training for high-risk employees
- Adapt training based on the scope of products, services, customers, partners and geographic locations
- Update material and/or retrain employees in the event of negative testing results
- Make training materials easily accessible and available to staff

Known Hazards

What are the obstacles hindering sanctions compliance?

Both OFAC's Framework and CSI's survey provide valuable insight into the key hindrances of sanctions screening compliance:

LACK OF A FORMAL SCP

The Framework notes that, "OFAC regulations do not require a formal SCP." As a result, many overly burdened and resource-limited U.S. organizations do not develop or implement one.

Even some financial institutions, which typically have more robust corporate compliance, "do not effectively document their programs or update documentation on a periodic basis," according to ABA Risk and Compliance.

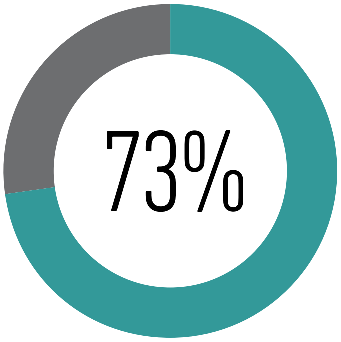
It is noteworthy that even before the Framework officially recommended a formal SCP, enforcement actions were citing the lack of a formal program as an aggravating factor in determining fines.

MISJUDGING ORGANIZATIONAL RISK

Nearly 77 percent of our survey respondents conduct most of their business in the United States. Among them, there may be an incorrect assumption that this automatically decreases potential risk. That could explain their high level of confidence in sanctions screening. **In truth, as global connectivity increases—in both obvious and subtle ways, so does the risk of sanctions violations.**

The Framework remedies this by recommending a risk assessment, which "should generally consist of a holistic review of the organization from top-to-bottom and assess its touchpoints to the outside world," including:

- Customers
- Supply chain partners
- Intermediaries
- Counter-parties
- Products and services
- Networks
- Systems
- Geographic locations of all offices, customers, supply chain partners, intermediaries and counter-parties



OF BUSINESSES CURRENTLY SCREEN AGAINST OFAC

LIMITED LIST SCREENING

Based on CSI's survey, only 73 percent of businesses currently screen against OFAC. Although U.S. organizations are not specifically required to screen the OFAC SDN list, they are blocked from doing business with anyone on it. Screening is the only way to ensure compliance with that prohibition.

A risk assessment gauges the peril of not screening, determines how often to screen and identifies which lists to include.

Denied Party Lists

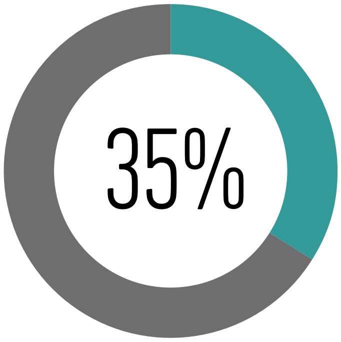
Based on jurisdiction and industry, organizations could be blocked from doing business with a variety of denied parties on one or more of these lists:

- OFAC SDN
- UN
- Department of State
- Sectorial Sanctions
- Interpol
- European Union
- Accountability & Divestment Act of 2010
- BIS
- HM Treasury Department Sanctions
- Healthcare Exclusions
- Debarments

Risk-Based Lists

Based on its risk profile, an organization could reduce certain risks by screening these lists:

- Politically Exposed Persons (PEPs)
- Adverse Media
- Medicare/Medicaid Opt-Outs

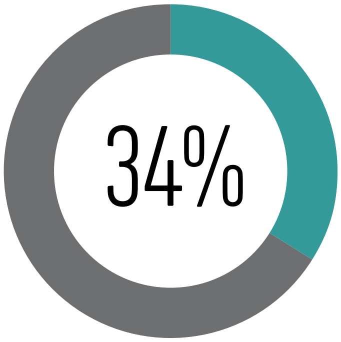


PRIORITIZE REDUCING MANUAL SCREENING PROCESSES

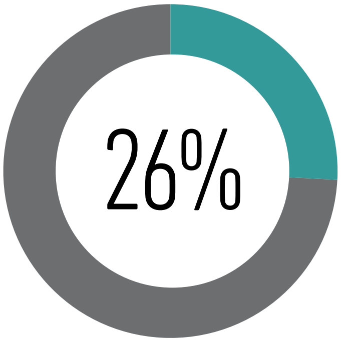
RELIANCE ON MANUAL OR INADEQUATE AUTOMATED SCREENING

The top compliance priority for more than a third (35 percent) surveyed was reducing manual processes. Although some manual intervention is necessary, the more an organization does manually, the more expensive and ineffective it is.

Dealing with false positives—which itself increases manual intervention—was noted as the biggest hindrance to sanctions screening by almost 34 percent. Outdated or inadequate automated screening solutions contribute to unnecessary, resource-wasting and time-consuming false positives.



SAY FALSE POSITIVES ARE THE GREATEST HINDRANCE TO SANCTIONS SCREENING

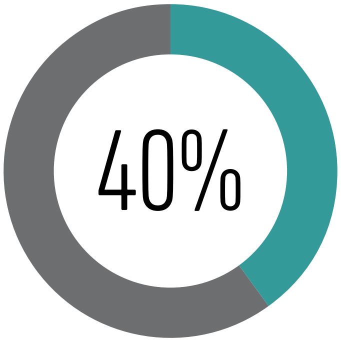


STATED MANUAL SCREENING/DUE DILIGENCE WAS THE SECOND GREATEST OBSTACLE TO SCREENING

INADEQUATE CUSTOMER DUE DILIGENCE

Likewise, the combination of manual screening/due diligence was rated the second biggest obstacle by 26 percent. This results in definite consequences:

Various administrative actions taken by OFAC involved improper or incomplete due diligence by a company or corporation on its customers, such as their ownership, geographic location(s), counter-parties, and transactions, as well as their knowledge and awareness of OFAC sanctions.



SPEND TOO MUCH TIME DEALING WITH SCREENING WITHIN THEIR CASE MANAGEMENT SYSTEMS

NON-INTEGRATED FUNCTIONS OR DATA

Although 40 percent of businesses in our survey stated they spend the majority of their time in case management systems, there is still a lingering lack of functional and data integration.

The OFAC Framework states:

> *"... several organizations subject to U.S. jurisdiction have committed apparent violations due to a de-centralized SCP, often with personnel and decision-makers scattered in various offices or business units."*

According to legal firm Gibson, Dunn and Crutcher LLP, "Taken together, the DOJ and OFAC guidance supports our oft-given warnings against a siloed approach to compliance for multinational companies."

This lack of integration also affects data cleanliness, leading to:

- More unnecessary false positives
- Limited employee access to needed data
- Delays in notification and/or resolution of potential matches

Technology Bypass

How can you achieve an effective sanctions compliance program?

Whether your organization is part of the 55 percent of businesses that plan to spend more on compliance initiatives in 2020, or the 39 percent that hope to keep it the same, the latest technology advancements offer viable and realistic ways to maximize every dollar spent on sanctions compliance.

AUTOMATED SCREENING

Machines can accurately analyze large volumes of data much faster than humans, and artificial intelligence is continually widening that gap. The most effective automated screening solutions allow your organization to conduct real-time, recurring and retroactive screening of any of your internal databases against any number of pre-selected lists simultaneously and seamlessly.

The key benefits:

- Zero disruption to pending transactions
- Automatic alerts to possible matches
- Decrease in duplicate efforts
- Single and batch lookup capability

COMPLETE LIST ACCESS

When choosing an automated solution, look for one that provides access to a wide range of continuously updated denied party and risk-based lists so that your organization can screen against all the appropriate lists identified in its risk assessment.

For maximum results, make sure it includes:

- Global Database Checks (GDC) to search for negative profiles on criminal, civil litigation, credit and compliance databases
- Open Source Investigations (OSI) to complete enhanced due diligence on high-risk third-parties

CASE MANAGEMENT INTEGRATION

52 percent of those surveyed use an in-house case management system or one that was developed by a third party. That system cannot perform as intended if it is unable to quickly and easily interact with your chosen automated screening solution.

Leading-edge solutions come equipped with application programming interfaces (APIs) that allow them to fully integrate with an existing case management system within your organization.

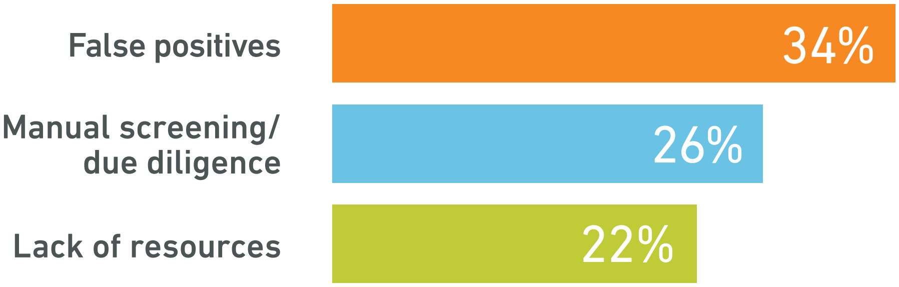
Enhanced and streamlined user experience:

- Watch lists enter your organization in one comprehensive, immediately available data feed
- Screening processes and information work seamlessly with all your relevant technology, including customer onboarding, transaction payment and vendor-related systems
- Consistent, real-time screening against multiple internal databases is always available
- Appropriate parties have access to all the information needed to perform any sanctions screening function
- Easy sharing of alerts, status reports, assignments and record-keeping related to all functions, no matter the organizational structure or physical location of them related to all sanctions screening functions

ADVANCED, CUSTOMIZABLE ALGORITHM

The algorithm of your automated solution is a vital key to reducing three of the biggest sanctions screening obstacles identified in our survey: false positives—34 percent; manual screening/due diligence—26 percent; and lack of resources—22 percent.

What are the biggest sanctions screening obstacles?

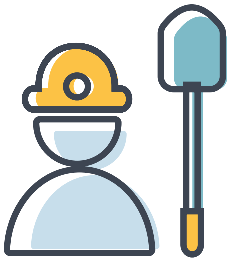


More sophisticated algorithms zero in on true matches, reducing the time spent investigating and resolving false positives. The efficiencies increase exponentially the bigger your data set of customers, transactions or relationships.

Must-have efficiency features:

- Advanced name search using a variety of name-matching methodologies based on risk
- Tolerance threshold that lets you choose how closely a single or batch lookup must match:
  - Lower tolerance (less similar match threshold) for higher-risk subjects, or
  - Higher tolerance (closer match threshold) for lower-risk subjects

DISQUALIFICATION TOOLS



False positives can be further weeded out when your automated solution features an array of disqualification tools. When selected, they automatically provide valuable information for quickly confirming or disproving a potential match.

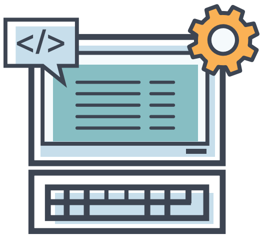
Extensive disqualification markers:

- Name
- City
- Country
- State postal code
- Year of birth
- Birth date range
- Street address
- Assigned watch lists

Plus, exact matching:

- Social security number against SSA Death Master File (DMF)
- User ID against National Plan and Provider Enumeration System (NPPES)

ADDITIONAL USER FUNCTIONALITY



The ease and efficiency of your organization's sanctions screening depends on how much other functionality is available in its automated solution.

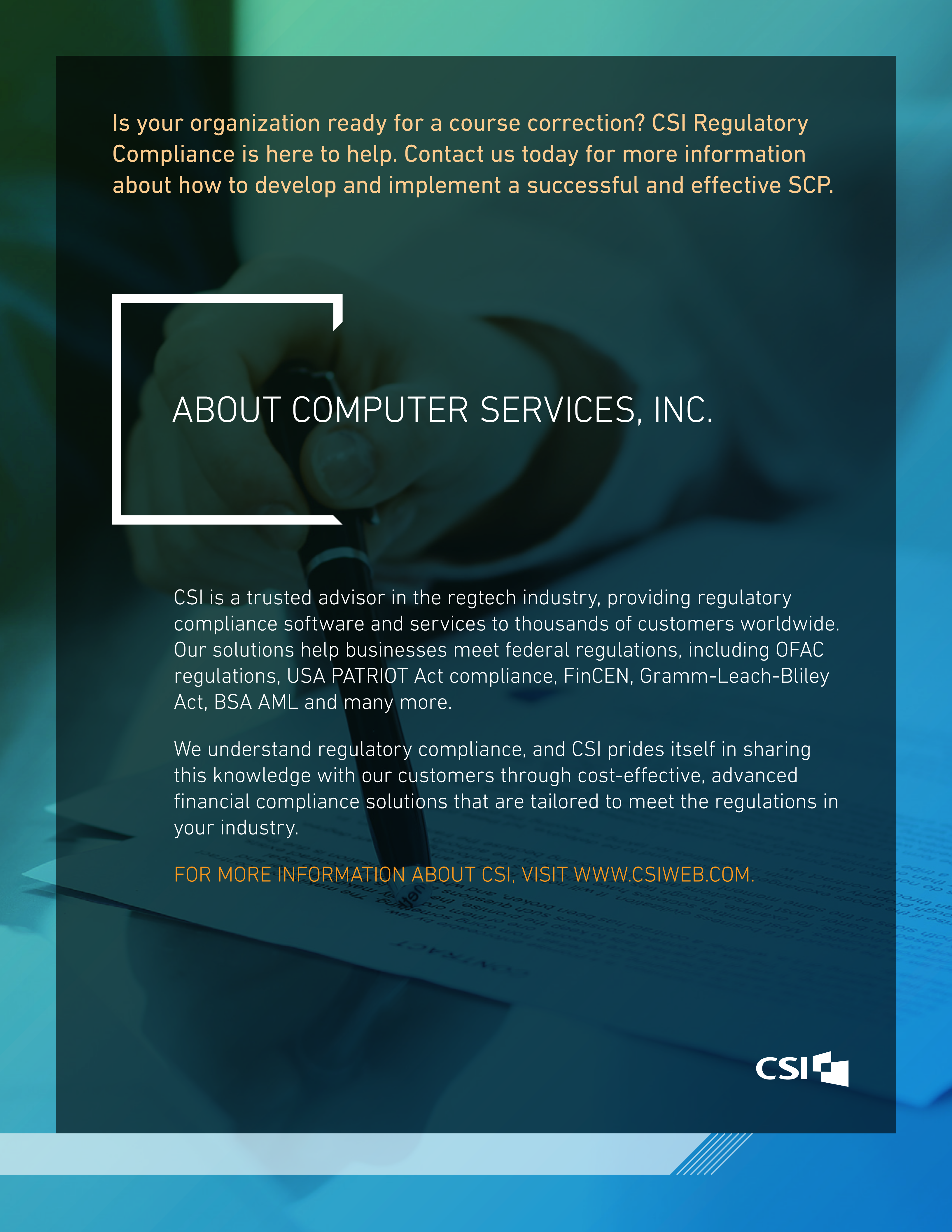
The advantages of more:

- Easy deployment
- Translation and transliteration of all major languages and alphabets
- Good customer lists that flag previously reviewed, investigated and eliminated matches
- Blocked customer lists that flag previously identified true matches
- Extensive report capability for testing, auditing and proof of compliance

Course Correction

Are you ready to put your sanctions compliance on the right path?

The OFAC Framework—coupled with CSI's 2020 Priorities for Compliance Leaders research—gives U.S. organizations the clearest picture to date of what a sanctions compliance program should look like. According to the framework: "Given the dynamic nature of U.S. economic and trade sanctions, a successful and effective SCP should be capable of adjusting rapidly to changes published by OFAC."



Is your organization ready for a course correction? CSI Regulatory Compliance is here to help. Contact us today for more information about how to develop and implement a successful and effective SCP.

ABOUT COMPUTER SERVICES, INC.

CSI is a trusted advisor in the regtech industry, providing regulatory compliance software and services to thousands of customers worldwide. Our solutions help businesses meet federal regulations, including OFAC regulations, USA PATRIOT Act compliance, FinCEN, Gramm-Leach-Bliley Act, BSA AML and many more.

We understand regulatory compliance, and CSI prides itself in sharing this knowledge with our customers through cost-effective, advanced financial compliance solutions that are tailored to meet the regulations in your industry.

FOR MORE INFORMATION ABOUT CSI, VISIT WWW.CSIWEB.COM.

CSI