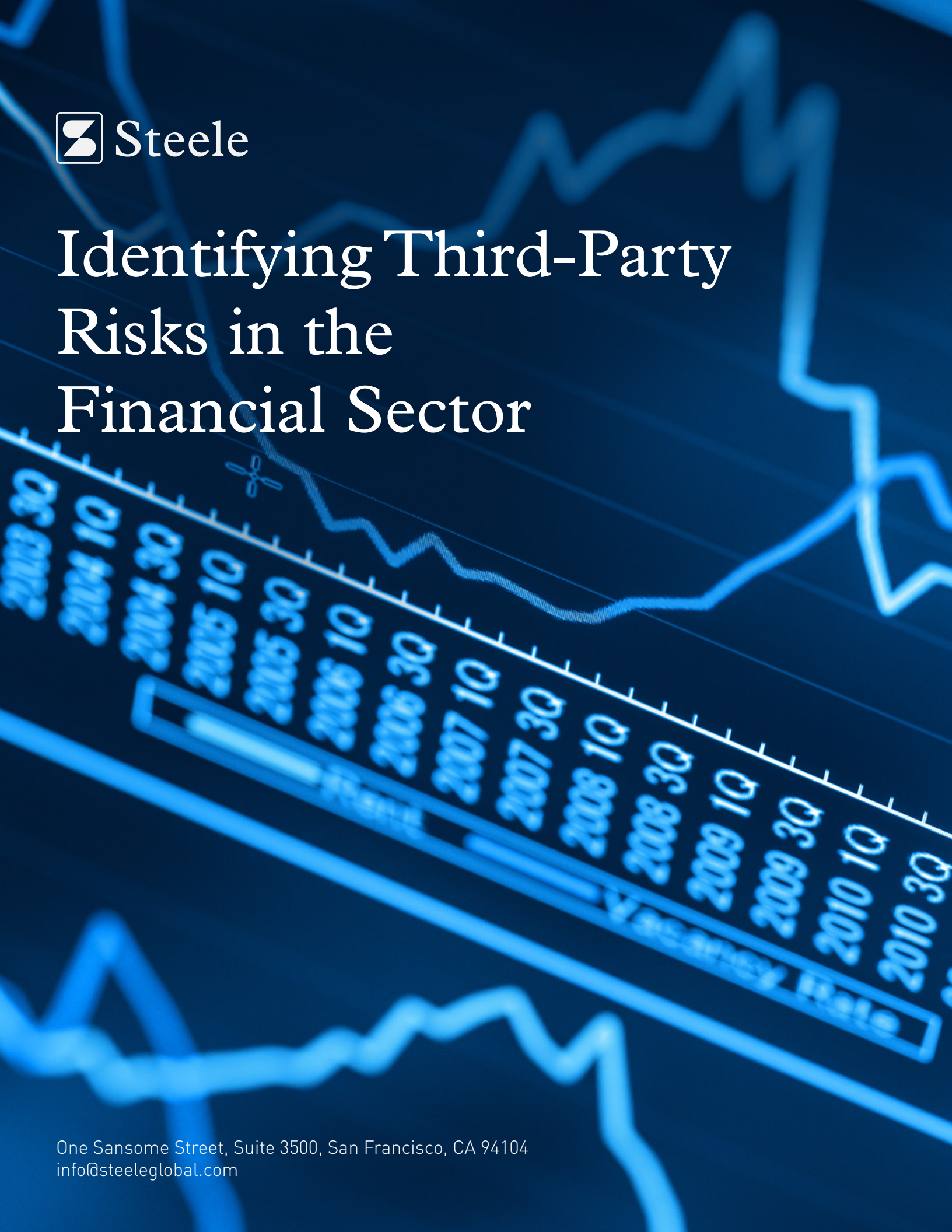
Steele

Identifying Third-Party Risks in the Financial Sector



One Sansome Street, Suite 3500, San Francisco, CA 94104
info@steeleglobal.com

INTRODUCTION

Third-party risks in the financial sector are a breed unto themselves. Or, more precisely, they are two related breeds: third-party risks from customers, and third-party risks from vendors. A financial firm's compliance function must somehow address them both.

Yes, at a conceptual level, those risks exist in non-financial sectors, too: anti-bribery, data security, fraud. Businesses in any type of industry do worry about them. But in no other sector are third-party risks as heightened as what we see in the financial sector. Hence the pressure to implement sufficient oversight of third parties is immense.

The financial sector faces so much third-party risk for two reasons. First, financial firms are the circulatory system of the economy as a whole, pumping credit and cash from one party to another; they touch an immense number of players in the economic and business worlds. Second, many participants in the financial system want to exploit the system for some other nefarious purpose: money laundering, tax evasion, terror financing, and the like.

Taken together, those threats can cause extreme damage to innumerable other parties: a banking system crashed, sensitive data stolen for tens of millions of people, drug cartels funded or terror campaigns sustained.

Moreover, most financial firms now operate on a global scale. They interact with more customers of uncertain origin; they allow more third parties onto their data systems. They also encounter more regulators, vigorously policing against the risks the firms pose to their own financial systems.

For example, in 2016 the U.S. Financial Crimes Enforcement Network (FinCEN) adopted enhanced customer due diligence requirements that require firms to identify the "beneficial owners" of every new business client. Those rules expand the range of due diligence that firms must perform on third parties; and firms must complete all updates to their policies, procedures, and operations by May 2018.

Meanwhile, the federal government also designates the financial services sector as "critical infrastructure." That means a host of regulatory agencies (Securities and Exchange Commission, Treasury Department, Federal Reserve, and more) are pressuring firms to increase their management of cybersecurity risk.

Financial firms, especially large banking businesses, face a double-barreled threat with cybersecurity: they are under constant attack, *and* routinely use thousands of vendors across their enterprises. Those vendors can be conduits for attack, driving up the need for third-party oversight even more.

Those regulatory pressures neatly bookend the third-party risks from customers (the FinCEN example) and from vendors (the cybersecurity example). Let's examine specific risks in each of those categories more closely, and what they mean for a firm's compliance program.

"No other sector are third-party risks as heightened as what we see in the financial sector. Hence the pressure to implement sufficient oversight of third parties is immense."

RISKS FROM CUSTOMERS

In one form or another, all third-party risks from customers revolve around *people masking their true intentions*. Some specific examples include:

- **MONEY LAUNDERING.** Customers might want to use the financial system to "launder" money from illicit business activity: drug dealing, human trafficking, or similar crimes. They mask where their money came from.
- **TAX EVASION.** Customers might try to hide financial assets in overseas accounts, so their tax authorities at home won't know their true wealth. They mask where their assets actually are.
- **TERROR FUNDING.** Where money laundering attempts to "clean" money from illicit activity, terror funding seeks to divert legitimate money to terrorist organizations shut out of the financial system. It masks where money is going.
- **SANCTIONS.** Some customers might try to do business with parties in countries such as Iran, North Korea, Venezuela, Russia, or other countries in violation of trade law. They try to mask the true identity of the other party.

To fight these abuses, governments have enacted a host of laws that all drive toward the goals of knowing who a financial firm's customers actually are, and what transactions those customers are undertaking.

For example, the United States enacted the Bank Secrecy Act and the PATRIOT Act to fight money laundering and terror funding. It also adopted the Foreign Account Tax Compliance Act (FATCA) to crack down on U.S. citizens evading taxes by hiding financial assets overseas. The European Union adopted the EU Fourth Anti-Money Laundering Directive to fight money laundering. FATCA became the basis for the Common Reported Standard, an effort endorsed by the G-20 to fight tax evasion globally.

Financial firms' compliance obligations under these laws are commonly known as Know Your Customer (KYC) programs: customer information to collect, policies to enact, data to report, and due diligence to perform.

RISKS FROM VENDORS

Third-party risks from vendors, in contrast, are more about exposing a financial firm to business interruption, litigation, or regulatory enforcement. Consider:

- **CYBERSECURITY.** Financial firms hold troves of valuable personal data about customers. That makes them enormously lucrative targets for thieves, who try to steal that data and sell it or use the data to empty customers' accounts. As financial firms use third parties for business processes (data storage, payroll processing, accounts payable; even compliance services to collect customer data), each of those third parties becomes another possible entry point attackers will exploit.
- **BUSINESS CONTINUITY.** Modern financial firms must run nonstop, every day of the year. Vendors managing websites, data storage, or even the physical plant at bank branches must provide needed reliability; or their failures could disrupt your business.
- **FOREIGN BRIBERY.** The United States, Canada, Britain, and many other countries now have laws that prohibit companies from bribing foreign government officials to win business. Those laws extend to a third-party working on the company's behalf—so like all global businesses, large financial firms must police their third parties for anti-bribery risk, as well.

As mentioned earlier, all these vendor risks exist in other business sectors as well—but the financial sector is different. Because it plays such a crucial role supporting other business sectors, and must be available essentially at all times, many of its vendor risks—particularly cybersecurity and business interruption—are magnified. That means the importance of governing those vendor risks is magnified as well.

Now, with that sweeping range of third-party risk that financial firms must worry about—how does a compliance officer begin to tame them?

THE FOUNDATION: DUE DILIGENCE AND MONITORING

The specific risks from customers and vendors are quite different, and the allies a compliance officer will need to enlist across the firm will differ as well. The fundamentals of effective third-party risk management, however, cut across both categories.

First, financial firms must perform *due diligence* to determine the identity and reliability of the third party in question. That's true whether the third party is a customer, where you must comply with KYC obligations; or a vendor, posing other regulatory and operational risks. If the third party's bona fides can't be confirmed, the financial firm needs to revisit the wisdom of doing business with that party at all.

Second, after a third party is "onboarded," the financial firm needs to perform *monitoring* to ensure that the third party remains a reliable business partner. Customers might start conducting much larger financial transactions; a vendor might be acquired by a parent company with ties to foreign governments. Neither of those events would automatically require a financial firm to cut ties, but they *might*—and for your firm to decide that question, first it must know that those changes in circumstance have occurred, and require attention.

Due diligence for customers and due diligence for vendors are not identical. They do, however, require similar steps.

- **BACKGROUND CHECKS**
  Third parties should be screened to assure that neither they, nor their beneficial owners, raise any concerns. For example, vendors should be screened to confirm whether any of their executives or owners are "politically exposed persons" (PEPs) who might bring higher levels of anti-bribery risk. Customers should be screened to confirm whether any of them are "specially designated nationals" who could trigger terrorism or drug cartel concerns.

- **INTEGRATION OF POLICY AND PROCEDURE**
  Compliance obligations force financial firms to have policies for background checks and customer due diligence; those policies must then be embedded into procedures so employees can meet them. For example, procedures to open new customer accounts should be updated to capture data necessary to fulfill FinCEN's enhanced due diligence on beneficial owners.

- **DOCUMENTATION**
  You can require vendors to sign forms certifying that, for example, they will not subcontract storage of your data to some other service without your permission. You can (and must) obtain evidence from customers that they are who they claim to be.

An important point to remember is that due diligence should be *risk-based*—an appropriate amount of due diligence for the amount of risk a third party poses. For example, a U.S. citizen with no foreign bank accounts, and a long history of financial transactions under $10,000, might only need standard identity verification procedures: two forms of government-issued identification. A Russian national who owns businesses and bank accounts around the world, with transactions that routinely top eight figures, would need much more.

Likewise, monitoring of third parties is crucial—and it, too, should be risk-based. A firm might require its mission-critical vendors to disclose any change in ownership, and perform annual "adverse media checks" to identify other possible trouble. Audits of data security controls might be necessary, especially if the vendor has any access to your financial firm's payment systems or to customers' personal data.

Monitoring of customers is even more complicated. AML regulations obligate firms to report suspicious activity to the authorities. What constitutes a "suspicious" activity? Any transaction that seems *unusual* for the customer, and suggests some nefarious intent. So again, monitoring must be risk-based.

GOING FORWARD

Given the sheer volume of due diligence and monitoring that financial firms must perform, automating these tasks is crucial. Thankfully, KYC regulations do acknowledge the importance of automation, and even encourage it.

The implication, however, is that financial firms must understand their business processes—customer onboarding, vendor review, cybersecurity, mission-critical reliability, and many more—and then *embed third-party risk oversight into those processes*. Trying to "bolt on" third-party risk management at the end of those processes is a fool's errand.

BACKGROUND READING

Banking regulators and other federal agencies have numerous pieces of guidance to help financial firms understand their duties around third-party risk. Some of them include:

1. The U.S. Sentencing Guidelines, which address what an effective compliance program should look like for all companies;
2. The "Evaluation of Compliance Programs" guidance published by the Justice Department in February 2017, which includes a section on oversight of third parties;
3. OCC Bulletin 2016-32, "Risk Management Guidance on Foreign Correspondent Banking;"
4. Federal Reserve Supervisory Letter 13-19, "Guidance on Managing Outsourcing Risk;"
5. FinCEN, "Customer Due Diligence Requirements of Financial Institutions;"
6. FinCEN, "Geographic Targeting Requirements."

ABOUT STEELE COMPLIANCE SOLUTIONS, INC.

Steele Compliance Solutions, Inc. is a global compliance intelligence firm offering comprehensive third-party due diligence and software-as-a-service (SaaS) solutions that help organizations comply with regulatory third-party compliance requirements. With more than 26 years of experience, due diligence engagements in more than 190 countries, covering more than 40 languages, Steele provides Fortune 1000 companies with pragmatic solutions. Our suite of products and services include regulatory due diligence, third-party program advisory services, program management services, and a secure, automated third-party management software platform.

Steele
Worldwide Headquarters
One Sansome Street
Suite 3500
San Francisco, CA
94104 USA

+1 (415) 692-5000
info@steeleglobal.com
www.steeleglobal.com