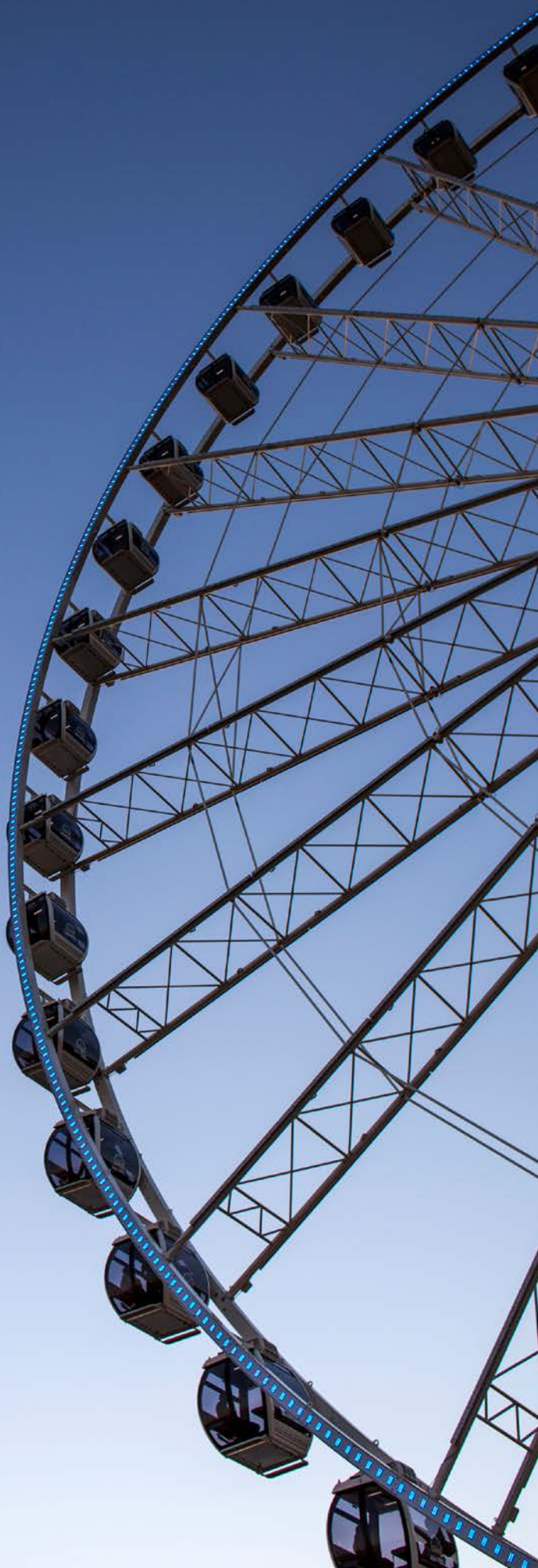
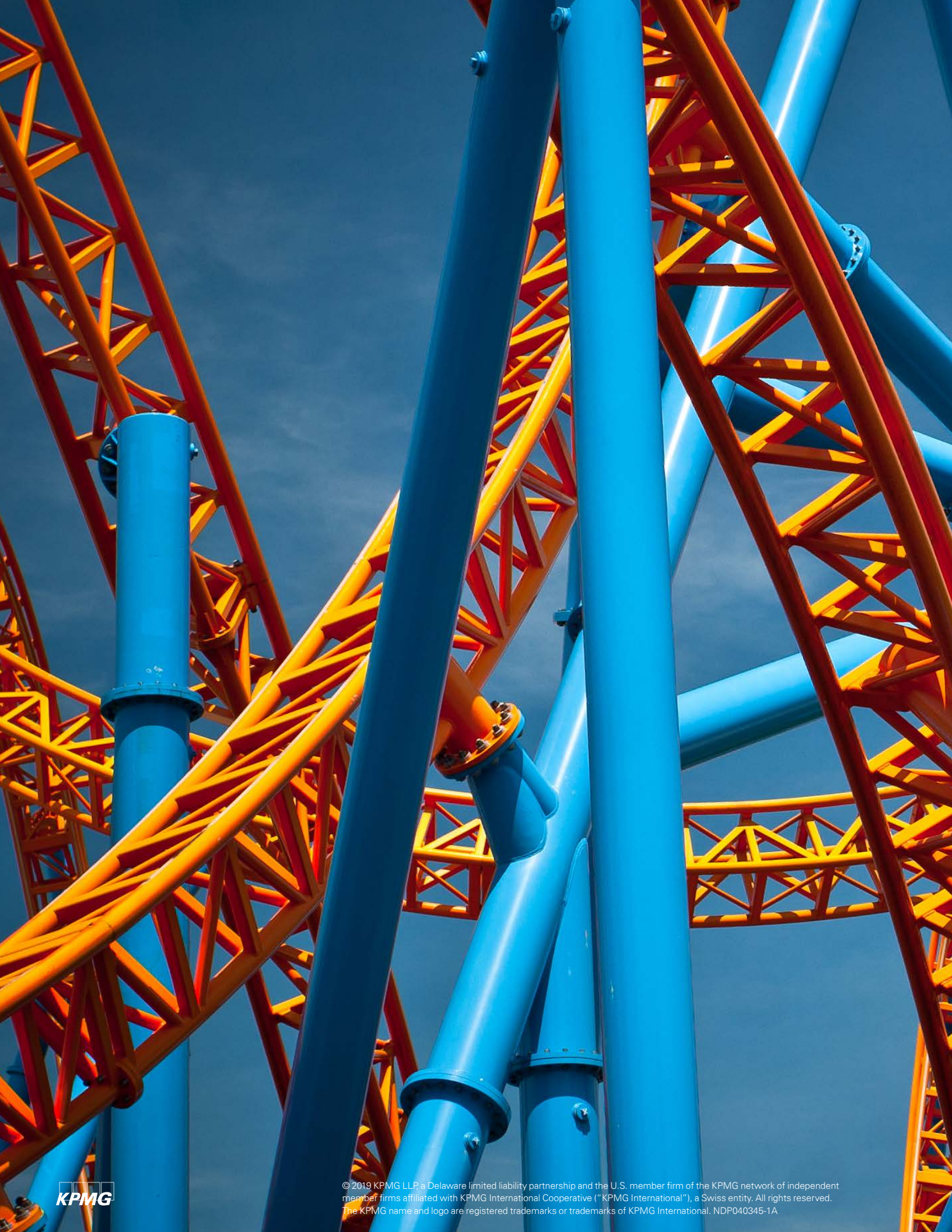
KPMG

Ten key regulatory challenges of 2020

Financial services risk across business imperatives



kpmg.com



Contents

Introduction

On behalf of KPMG's Regulatory Insights, we are delighted to issue the fifth edition of our annual Financial Services Ten Key Regulatory Challenges.

Regulators and public policy decision-makers are struggling with not only the pace of change within the financial services industry but also the interconnectivity of industries via data and technology. In 2020, we expect key regulatory challenges to be connected with the following core business imperatives:

— Technology transformation

— Customer interaction

— Payments modernization

— Market expansion

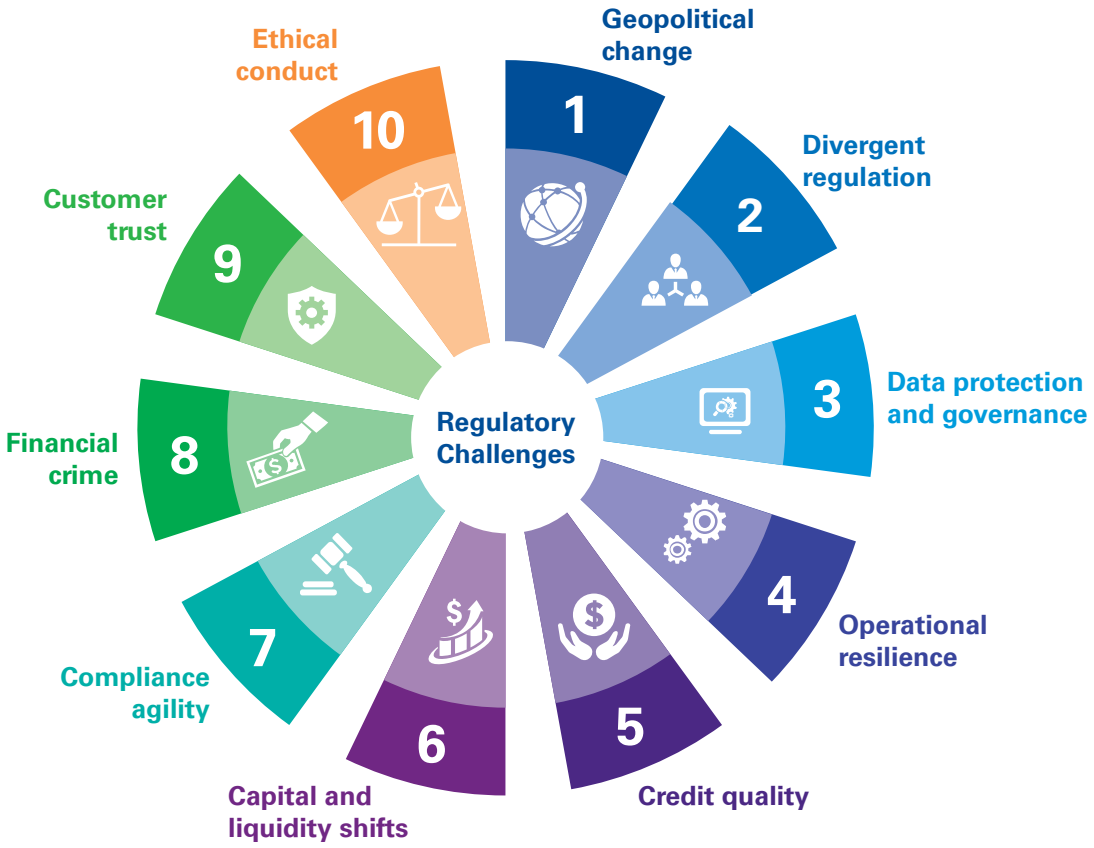
— Cost efficiencies

Geopolitical protectionism as well as divergent regulatory obligations across jurisdictions globally and between state and federal entities will continue to challenge financial services risk and compliance. Rapid and personalized customer experience and regulatory cross-industry focus on anti-trust and competition will drive additional challenges to enhancing operational resilience, data governance, fair markets, and customer treatment, while keeping all within ethical and sound conduct practices.

In the following pages, we evaluate how each of the Ten Key Regulatory Challenges aligns with and is influenced by the changes prompted by the core business imperatives. We hope this paper will provide you and your organization with valuable insights to consider throughout 2020, and would welcome the opportunity to assist you with developing strategies to meet this year's regulatory challenges.

Amy Matsuo
Principal and National Leader
Regulatory Insights

Ten key regulatory challenges



1 **Geopolitical change:** Expect disruption and embrace business change

2 **Divergent regulation:** "Merge the diverge" with both enterprise and localized needs

3 **Data protection and governance:** Protect your data as the asset that it is

4 **Operational resilience:** Plan for the unexpected operational impacts, they will happen

5 **Credit quality:** Apply the learnings from prior credit cycles

6 **Capital and liquidity shifts:** Easing buffers doesn't mean weakening risk management

7 **Compliance agility:** Solution now for agile and streamlined compliance

8 **Financial crime:** Innovate, but not at the cost of increasing risks of financial crimes

9 **Customer trust:** Remember that you are in the business of customer trust

10 **Ethical conduct:** Do the right thing, even when no one is looking

Geopolitical change

Geopolitical trends toward protectionism, sovereign rights, and anti-globalization prevailing in the U.S. and other countries introduce increased policy uncertainties and regulatory risks. U.S. financial services companies must expect that such uncertainty will create disruptions even as they continue to implement governance and controls to address divergent policies and regulations and regularly reassess operations to identify necessary business changes.

Geopolitical changes related to monetary policies, economic developments, trade agreements and sanctions, and specific regulations/requirements (e.g., KYC, beneficial ownership, GDPR, MIFID II, comparability determinations) will have the most impact near term. However, companies must also be alert to a heightened risk of fraud and financial crime, which can thrive in states of uncertainty, facilitated by innovative technologies that have made the world smaller and more connected and vulnerable to change.

Expect disruption and embrace business change

Technology transformation

— Multiple applications for digitization, including customer focus and operations focus (e.g., real –time monitoring of fraud/financial crime, and internal risk management)

— Cyber attacks can be fueled by geopolitical tensions; may be directed at a country's government, citizens, or businesses; and motivated by theft or vandalism

— Jurisdictional differences in the approach to regulation and supervision of technology innovations and technology firms may impact operational resiliency risks

Customer interaction

— The EU's GDPR is influencing customer expectations and legislative/regulatory actions in data privacy/security on a global scale

— The transition away from LIBOR in favor of new alternate reference rates will impact product offerings and pricing across multiple jurisdictions though the new rates are expected to better insulate jurisdictions from geopolitical risks

— Customer demand for personalization and seamless global access to products and services is driving risks related to technology development, third-party relationships, ESG policies, new products and services, and fraud/financial crimes

Payments modernization

— Policies and regulations in countries outside of the U.S. that are actively deploying real-time payments and "open banking" will likely influence customer expectations in the U.S. and potentially federal public policy

— Regulators are concerned that digital assets, including cryptocurrencies, could be used for illicit activities, such as cybercrime, tax evasion, and human trafficking, though not all jurisdictions require money transmitters to comply with Bank Secrecy Act-like obligations

KPMG

Market expansion

— Uncertainties in U.S. trade policies and the application of sanctions and tariffs impact financial services organizations' operations in the affected markets as well as the activities of its customers

— Financial services organizations should ensure that critical assets and the flow of sensitive information are adequately protected across international locations

Cost efficiencies

— The use of third and fourth parties to facilitate technology implementation, scale efficiencies, or business strategies must be monitored for compliance and reputation risks as well as geopolitical risk including tariffs, sanctions, and financial crimes

— Persistent world-wide interest rates will pressure firms to consider business model changes and may increase M&A activity across jurisdictions.

Additional KPMG perspectives

— Regulating virtual currencies

— Virtual assets and related providers—FATF recommendations

— Gaps in meeting BCBS risk data aggregation and reporting principles

— The FSOC Annual Report highlights areas of emerging risk and vulnerability

Have you heard? LIBOR ends 2021; Communicating the transition

Divergent regulation

Financial service companies will need to learn to "merge the diverge" with respect to regulation—anticipating continued differences in state, federal, and global regulations amidst protectionist and localized public policy agendas in the U.S. and abroad. Key areas of divergence will include:

- **Data privacy regulation, cyber security, student loan servicing and cannabis industry-related banking services**
- **Tailored regulatory and supervisory expectations to risk and complexity, diverging from global standards**
- **Innovative technology applications where new or refined regulations may evolve (e.g., payment processors, data aggregators, cloud service providers)**
- **Alignment with non-financial services federal regulators, including DOJ standards for compliance, FTC enforcement authority for data privacy, and DOL influence in fiduciary responsibilities.**

"Merge the diverge" with both enterprise and localized needs

Technology transformation

- While continuing to encourage innovation, federal regulators (banking and non-banking) are moving away from exploratory reviews and toward setting parameters for innovative technology applications through increased supervision, horizontal exams, and enforcement
- Regulators are expanding oversight to third-party vendors and other relationships that facilitate rapid deployment or scalability of technology applications for financial entities but may operate outside of prudential bank supervision (such as payment processors, cloud providers, data aggregators)
- Globally, regulators vary in their approach to encouraging and supervising the development and application of innovative technology

Customer interaction

- Throughout the election cycle, attention will be on federal standards for consumer protection in specific areas (e.g., affordable housing, student debt) and also in relation to innovative technology and supervisory easing.
- Individual states are enhancing their focus on consumer and investor protection, including state attorneys actions, and in some cases have "set the bar" nationally for customer expectations
- SEC's Regulation Best Interest did not set a fiduciary standard for broker-dealers but also did not preempt states laws; DOL and FINRA are each expected to release new fiduciary/suitability rules to align with the SEC

Payments modernization

- Regulations governing virtual currencies are evolving in the U.S. and abroad though public policy debate around regulatory safeguards, financial stability, and monetary policies continues
- Merchants and nonbanking financial services providers have a growing role in emerging payment channels and services, highlighting differences across banking and non-banking regulation and industry standards
- A private-sector real-time payments process is now available to U.S. markets and a public-sector process is being developed

KPMG

Market expansion

— State and federal regulators are each actively seeking supervisory authority over the proliferation of fintech firms

— Individual states continue to enact legislation and implement regulations where federal requirements are perceived to be insufficient, such as data privacy, data security, student lending, and banking access for the cannabis industry

— Business strategies to enter into new markets or products must address the expanded regulatory attention being given to anti-trust and sanctions compliance

Cost efficiencies

— Regulatory focus on cost efficiency (including talent and change management) has a positive impact on compliance culture and regulatory adherence

Additional KPMG perspectives

— Regulatory focus on technology risk

— OCC semiannual risk perspectives

— FSB consults on financial resources to support CCP resolution

— Regulatory capital requirements for insurance holding companies

AI | Compliance in Control

Driving Change | The California Consumer Privacy Act

Data protection and governance

Financial services providers recognize data as an asset that increasing needs protection via robust data governance and controls across their organization and through to third parties. Data is constantly collected, monitored, used, and shared though it is the quality of the data and its ethical uses that are key to protecting proprietary, operational, and customer information. Continued data breaches and data sharing incidents are influencing public and regulatory expectations for increasingly stringent data privacy and security requirements ensuring public policy and enforcement will continue at the local, federal, and global levels.

Protect your data as the asset that it is

Technology transformation

— Technology advances allow for more granular data classifications that permit tracking for sourcing, retention, access, use, and disposal via business functions and third-party relationships

— Dependence on third-party vendors for rapid deployment or scalability of technology applications can give rise to governance and accountability risks

— To keep pace with evolving technology, regulators expect cybersecurity strategies to be forward-looking and to address data protection, cloud security, threat simulations, and a layering of solutions.

Customer interaction

— Public policies and regulatory supervision and enforcement are focusing on strong data governance and controls, including KYC, suspicious activity, and fraud while customers focus on ownership and control, including collection, storage, use, disposal, and portability

— Some organizations, independent of regulatory requirements, are reconsidering policies regarding opt-in and opt-out procedures, the scope of data to be collected, how and by whom it is accessed, and how it will be used or shared

Payments modernization

— The push toward faster payments reduces the time available to detect fraud and suspicious transactions, potentially compromising data privacy/security and financial crimes compliance and increasing the need for strong third-party risk management

— Technology leveraging biometric authentication (i.e., fingerprint, face features, heart rate) may assist in establishing a more secure payments environment but may also carry new privacy and data security risks

KPMG

Market expansion

— Organizations must understand the source and content of data used to personalize customer experience, including data derived from social media sources or AI data sets, to proactively address unintended bias and reputation or strategic risk and abroad

— Increasingly, brands are differentiating based on transparency of data collection and use

— The threat of cyber-attacks is global in scope and can be motivated by theft, destruction, or disruption of proprietary or consumer data

Cost efficiencies

— Increased awareness, governance and reporting of reputational and third party risks in data privacy and data protection will influence business model, process and automation changes

— Data-reliant technologies, including AI and robotics, as well as relationships with third-party technology providers such as cloud servicers are increasing cost and process efficiencies

Additional KPMG perspectives

— Focus on data privacy policy and enforcement

— SEC privacy notice and safeguards policies

— Regulatory focus on technology risk

— FTC proposes amendments to the GLBA regulations

— FINRA report outlines cybersecurity practices

Operational resilience

Operational resilience will remain a key risk focus for regulators amidst ongoing business transformation that is increasing firms' vulnerabilities, including regulatory and operational change management, new technology and data governance strategies (e.g., cloud), expanded use of third parties (e.g., payments processors, data aggregators), enhanced risk management practices (including third party and reputation risks) and integrated risk, operations, and compliance. Regulators are taking an increasingly broad view of operational resilience, expecting firms to not only control for operational risk but also to manage disruptions when they occur with an eye toward preserving the continuity of key business services (inclusive of, but greater than, IT systems and cyber security).

As such, operational resilience integrates core elements of business continuity planning, operational risk (inclusive of third party) and concentration risk analysis. Further, firms must understand: the impact of critical system failures on their key businesses, counterparties, and markets; the systems that support their critical business activities; and the effectiveness of solutions and controls to protect those systems.

In today's interconnected business environment, firms must also consider that potential threats or disruptions to their operations may be generated from sources outside of financial services, such as cyber crimes, sociopolitical changes, or environmental risks.

Plan for the unexpected operational impacts, they will happen

Technology transformation

— Operational Resilience provides a useful lens for firms to prioritize investment decisions for modernizing legacy systems and strengthening technology infrastructure

— Dependencies and interconnectedness between internal and third party technology assets must be mapped, analyzed, and tested to validate the feasibility of stated recovery time objectives and achieve resumption of the end-to-end business service

— Heightened regulatory attention to competition and anti-trust, especially with regard to digital technology platforms and cloud services, must be considered when selecting/maintaining third-party relationships and/or acquisitions activity

Customer interaction

— Operational Resilience emphasizes the responsibility of financial services companies to maintain customer trust by delivering services consistently and with high quality, even when systemic shocks do occur

— Internal and external communications plans are needed to provide timely information to, and manage the expectations of, customers, other market participants, and regulators following a disruptive event; communications can help to restore confidence in the company and preserve its reputation

— Evaluate the firm's ability to meet evolving customer expectations for the continuity of financial services products and services, including mobile and web-based services that operate 24/7

Payments modernization

— Customer expectations for payments speed affects the resilience thresholds and tolerances for payments disruptions; disruptions in payment processing have the potential for serious financial harm to consumers and corporate clients

— Operational Resilience emphasizes the security of payments along the value chain, including during handoffs with third parties

KPMG

Market expansion

— When launching new products and services, articulate clear service level agreements and recovery time objectives to verify the firm's ability to deliver these services when there is an Operational Resilience event

— A clear understanding of business services and the people, data, systems, and processes on which they depend should enable a company to undertake M&A activity more efficiently and effectively or move more smoothly into new areas of business.

— A firm's ability to deliver services globally with high quality across the value chain, must consider third parties and partnerships across all geographies, including geopolitical and ESG risks specific to their locations

Cost efficiencies

— Balance effective risk management with operational efficiencies by concentrating investment in the assets that bolster Operational Resilience; invest and allocate resources based on the services that are most crucial for the continuity of critical systems and business objectives

— Understand the financial impact of service disruptions and establish impact tolerances; validate that insurance policies are appropriate from a Resilience perspective

— Establish penalties for third parties that fail to deliver services and develop exit strategies for each vendor

Additional KPMG perspectives

— Federal Reserve proposal on control determinations

— Operational Resilience in Financial Services

Data rich governance

Unlocking compliance analytic insights

Streamlining to create value

Credit quality

Apply the learnings from prior credit cycles

Financial institutions should apply the learnings from prior credit cycles and focus on potential risks related to:

- **Risk layering and leveraged lending**
- **Expanded delivery channels and payment options**
- **New products and services and technology applications**
- **Exposures via securities or trading activities, lending to non-depository financial institutions, or partnership arrangements.**

Credit challenges may also come in relation to GSE reforms, CECL implementation, LIBOR transition, and competitive pressures from nonbank financial services companies.

Technology transformation

- AI applications in credit scoring models can help organizations to more accurately model and price risk (and expand credit access to consumers) but increases potential risks from "unexplainable" credit decisions, learned bias, or other fair lending and consumer compliance risks.
- IT systems must be capable of incorporating new risk-free rates to accommodate LIBOR transition across loan pricing, deposits, and other products and services by the end of 2021

Customer interaction

- Credit quality remains strong, supported by the prolonged low interest rate environment, but a trend toward eased underwriting terms and expanded access for subprime borrowers is evident, primarily in retail (i.e., credit card and auto) and commercial leveraged lending, increasing debt service risks
- Regulatory supervisory priorities will consider credit risk trends, risk management practices, weakened credit underwriting, and concentrations of credit
- Automated systems are changing the role of traditional financial advisers and altering the way loan products are marketed, underwritten, delivered, and sold

Payments modernization

- Regulators have a heightened focus on payments, servicing, and collections across all loan products that is aimed at ensuring firms' practices are evolving to respond to related risks, including financial crimes/fraud, while ensuring consumer protections

KPMG

Market expansion

— Traditional financial services organizations are experiencing increased competition from nonbank financial firms and others (e.g., retail and real estate firms) that are expanding into financial products and services, including credit cards, short-term credit, and insurance as well as leveraged lending

— The use of alternative information to expand credit access, including under-banked and un-banked, is increasing

— The markets for collateralized debt obligations and commercial mortgage-backed securities have rebounded since the financial crisis while the markets for residential mortgage-backed securities and asset-backed securities have remained relatively flat

Cost efficiencies

— Efforts to address SCCL, CECL, and LIBOR will coincide and likely pressure allocations of resources (funds, staffing)

— Machine learning/AI may facilitate LIBOR transition at reduced expense

Additional KPMG perspectives

— Focus on leveraged lending risks

— Regulatory capital rules amended in response to CECL

— CECL modeling and accounting

— Single Counterparty Credit Limit—Key challenges and considerations

Capital and liquidity shifts

Although most U.S. financial services organizations will see an easing of regulatory capital and liquidity requirements, the regulatory focus on governance of such activities along with sound risk management will continue. Financial institutions should anticipate:

- **Forthcoming final rulemakings for banking entities related to the Stress Capital Buffer, the Net Stable Funding Ratio, and Total Loss Absorbing Capital**
- **Supervisory priorities highlighting governance over capital planning, model risk, cash flow forecasting, and liquidity risk limits as well as liquidity risks related to an uncertain interest rate environment, technology changes, and "untested depositor behavior"**
- **Building regulatory attention to capital and liquidity frameworks for insurance entities and central counterparties**
- **Forthcoming rulemakings for certain nonbank entities to complete the regulatory framework for U.S. OTC derivatives markets**

Easing buffers doesn't mean weakening risk management

Technology transformation

- Automated document ingestion and validation tools are reducing capital and liquidity stress buffers due to increased granularity of and confidence in model data
- Automated workflow management is increasing the efficiency and accuracy of transactions and controls testing programs

Customer interaction

- Digital payments networks permit customers to easily transfer funds, often in real-time, increasing a depository institution's liquidity risks.
- Regulatory initiatives, including LIBOR, FDIC 370, CECL, SCCL, and AML/KYC, are driving banks to gather additional data on, and in some cases connect with, customers.

Payments modernization

- Treasurers are monitoring the potential impact of real-time payments on intraday liquidity
- Regulators are increasingly pushing banks to integrate payments-related stresses into contingency funding and recovery plans

KPMG

Market expansion

— As banks expand beyond their traditional branch footprints, the absence of historical data for new customers and products is creating a need for increased management judgement and more active monitoring

— Regulatory tailoring is facilitating some M&A activity, increasing ability to add technology and services, and achieve scale economies

— Nonbanks are asserting competitive pressures and influencing customer expectations but may be challenged in a credit downturn.

Cost efficiencies

— Initiatives to integrate capital and liquidity reporting into the finance process are freeing up substantial resources across risk and finance

— Identifying lower-cost delivery models, such as offshoring and near-shoring, for repetitive manual processes and hard-to-source skill-sets, is creating additional efficiencies

— Even as regulatory requirements ease, firms must invest in skilled staff and maintain robust oversight to assure compliance.

Additional KPMG perspectives

— Simplification of regulatory capital rules

— SEC finalizes step in Title VII regulatory framework

— Proposed rule on TLAC debt investments

— Interagency framework for prudential standards, capital, liquidity, and resolution planning

— Regulatory capital requirements for insurance holding companies

Compliance agility

Business imperatives of change and efficiency will both drive and transform legal and compliance operations. The speed of change within financial services necessitates that companies anticipate and adapt to emerging risks and ongoing transformation across multiple fronts, including technology advances, process improvements, regulatory developments, new market entrants, and shifting consumer preferences. Regulatory focus on the technology sector will directly impact business strategy given attention to anti-trust, sanctions, and operational resilience risks; it will also spotlight customer protection risks, including bias, accessibility, and privacy especially with regard to machine learning, AI, and cloud services. Regulators will expect companies to understand and explain outcomes of new technology applications/ enhancements as well as the roles and responsibilities third-party service providers. Compliance challenges will remain in core areas of conduct/ ethics, financial crimes, customer protection, and evolving geopolitical risks.

Solution now for agile and streamlined compliance

Technology transformation

— The use of fintech incubators and partnerships, and ongoing adoption of AI and cloud services (in business, middle and back office) requires enhanced due diligence, compliance risk management, and monitoring and testing processes

— Evolving technologies, including data analytics and natural language processing, enable firms to evaluate pools of structured and unstructured data to proactively identify potential compliance risks

— Agile legal and compliance integration will facilitate ongoing adoption of technology advances; regulators will expect companies to understand and be able to explain outcomes resulting from applications of new or enhanced technologies

Customer interaction

— Integrated KYC/AML and compliance controls will enhance risk-based assessments and streamline processes from due diligence through monitoring, escalation and off-boarding

— Applications of innovative technologies, such as ML/AI and cloud computing, may increase certain customer protection risks including bias, accessibility, and data privacy though these applications are not yet fully covered by specific regulation

— Key areas of compliance for customer protections will include data privacy, UDAP/UDAAP, Best Interest, and CRA

Payments modernization

— As new payment channels and products are deployed, compliance concerns continue to focus on regulatory requirements in financial crimes and investor/customer protection, including data privacy, UDAP/UDAAP, fees and disclosures, funds availability, third party risk management

— Regulatory focus on crypto assets, non-bank and online processing, real-time payments, and crowdfunding is evolving, in some cases prompting a rethinking/reordering of certain compliance processes (such as "pre-validation") to facilitate faster technologies and transactions

KPMG

Market expansion

— The compliance program should include comprehensive due diligence of acquisition targets and prospective third parties, as well as ongoing tracking of identified red flags; M&A activity will drive continued legal and compliance operational integration

— Heightened regulatory attention on the technology sector will impact business strategy and may increase legal and compliance risks in the areas of anti-trust, sanctions, and conduct

— Compliance and ethics risk professionals must have the requisite skill set to understand, embrace, and execute evolving technologies and customer demands

— Customer demand is driving the development of new product and service offerings and new delivery channels that can expand compliance expectations such as the ADA's guidelines for web content and mobile applications

Cost efficiencies

— Companies are leveraging regtech solutions to reduce compliance costs and improve overall efficiencies in time and effort in areas such as KYC/AML, transaction monitoring and testing, regulatory reporting, misconduct; automation and AI applications can shift monitoring from reactive to proactive

— To optimize investments in automation and AI, organizations should first reassess their core processes and controls, assess data quality, and streamline governance in order to address potential reputation, brand, and ethics/conduct risks

— Operational integration of legal and compliance will increase cost savings through reductions in complexity and duplication and enhanced ability to respond to regulatory change

— Co-sourcing/outsourcing strategies in areas like contract management, client onboarding, investigations, and compliance monitoring and testing requires monitoring third parties for compliance and reputation risks as well as geopolitical risks, including tariffs, sanctions, and financial crimes

Additional KPMG perspectives

— DOJ expands focus on effective compliance programs

— OFAC Framework for Sanctions Compliance Programs

Streamlining to create value

Innovating compliance through automation

2019 Chief Compliance Officer Survey

Unlocking compliance analytic insights

Financial crimes

Technology innovations that are changing how companies operate and deliver value to customers is also changing the availability and use of technology and data for perpetrators of fraud and financial crimes. Regulators are placing intense pressures on companies to contain these misconduct risks, increasingly coordinating their efforts across multiple regulatory jurisdictions and bodies in the U.S. and abroad. Regulatory acceptance of and support for the adoption of innovations in financial crimes compliance, inclusive of co-sourcing/third party arrangements, adoption of fintech, and AI will continue. Yet, companies still struggle with navigating the volume of data, multiplicity of sources and systems, and data controls across systems and external parties.

Expanded controls will be needed to thwart and minimize misconduct, fraud, and financial crime risks in evolving areas, such as virtual assets, crowdfunding, and real time payments processing. Financial service providers will need to continue to enhance controls and monitoring with respect to conflicts of interest, anti-bribery, and corruption along with overall surveillance for potential misconduct.

Innovate, but not at the cost of increasing risk of financial crime

Technology transformation

— Although regulators encourage the use of automation/innovation pilot programs and initiatives to promote more effective BSA/AML compliance, they expect companies to employ proper governance to minimize risking additional exposure

— Cognitive technology and data analytics can greatly aid a company in identifying patterns of behavior that present a higher indicia of financial crimes or fraud risk as well as misconduct

— Technology investments to meet both short- and long-term needs, including automation pilots/initiatives or use of shared services, should be based on a strategic business plan and prioritized based on an assessment of risk and obligations

Customer interaction

— A risk based KYC program that refreshes customer information, re-evaluates customer risk ratings, and subjects all parties to negative news screenings, can help organizations to more proactively address and mitigate AML and TF risks and issues.

— Regulators are focused on identification of ultimate beneficial owners, encouraging companies to use multiple mechanisms to break through non-transparent organizational structures during KYC

— Customer demand for digital channels for all types of transactions increases anonymity and drives up fraud risk; transitioning to a customer lifecycle analysis may target activity that is more likely to be unusual

Payments modernization

— Validation of new or changed systems is needed to ensure data completeness and accuracy for transaction monitoring, reporting, and information sharing

— The execution of faster payments reduces the time available to detect fraud and suspicious transactions, potentially compromising financial crimes compliance; friction in the payments process could play a role to increase security

KPMG

Market expansion

— Regulatory AML and financial crimes attention is expanding beyond traditional financial services transactions into economic/trade sanctions and anti-terrorist financing compliance demanding that companies develop greater agility to defend against related risk

— The number of digital currencies, including cryptocurrencies, and decentralized markets continues to expand globally, frequently operating without stringent supervision, increasing financial crimes risk

— Metrics/ data analytics must account for activities in emerging markets to more holistically assess financial crimes risks; heightened due diligence should be applied to reviews of targeted acquisitions and third-party partners/ vendors.

Cost efficiencies

— Despite cost saving or automation initiatives, it is important to maintain sufficient SME resources, including in technology, to ensure a sustainable program; run systems in parallel

— It is possible to adjust business operations to realize efficiencies from managed service and still retain management ownership and SAR filing responsibilities

— Automation is driving down the costs of completing due diligence, especially on third-party vendors, suppliers, contractors, and customers

Additional KPMG perspectives

— FATF Report: Terrorist financing risk assessment guidance

— Agencies encourage innovation in BSA/AML compliance

— Virtual assets and related providers—FATF recommendations

Innovating compliance through automation

Streamlining to create value

Customer trust

To build a customer's trust and loyalty in the current environment, financial services companies must continue their strategy of customer-centric business: personalized experience, mobility between channels, reliable privacy protections, evidence of good corporate citizenship, and fair value. Competition from fintechs and other nonbanks borne out of the industry's digital transformation pose a persistent and increasing challenge to this strategy, prompting consideration of new business combinations (including partnerships, joint ventures, and acquisitions) and pushing all types of transactions to be delivered faster and more securely.

Ensuring the protection of customers' personal data will drive continued regulatory focus on consumer and retail investor protections as will privacy concerns regarding the sale or use of customer data for marketing purposes, customers' claims and complaints, and questions of data ownership and control. In this regard, state laws and regulations will likely influence developing federal policies; customer trust will be dependent on a transparent commitment to privacy. Election debate will draw attention to areas such as affordable housing, fair lending, student debt, elder financial protection, best interest, and retirement security.

Remember that you are in the business of customer trust

Technology transformation

— Regulators are focused on the implementation and outcomes of new technologies, including artificial intelligence and machine learning (particularly related to credit decisions and marketing), and digital platforms and channels (both in-house and through third-parties) with an eye toward fair treatment, best interest, data privacy, and transparency

— The shift toward automation and cloud solutions highlights the importance of authenticating and tracking customer data across the organization, including its origins and integrity, systems location, use or sharing, and governance

Customer interaction

— Election debate will draw attention to issues of affordable housing, fair lending/fair housing, student debt, consumer and elderly fraud/scams

— Data breach and data sharing incidents will drive public policy and regulatory supervision/enforcement

— SEC Regulation Best Interest will highlight fees and disclosures, conflicts of interest, and ethics/conduct

Payments modernization

— Complex and divergent regulations and/or standards (jurisdictional, public vs private) are moving toward real-time payments and "open banking"

— Cross-industry trend toward multiple channels, seamless navigation, and customer control of personal data

— Regulatory focus is on funds availability, fee disclosures, fraud prevention, error resolution, and technology controls

KPMG

Market expansion

— Complex and divergent regulations (jurisdictional and evolving state) are developing with myriad variation on protections and requirements

— Customer demand is driving the development of new product and service offerings and new delivery channels that can expand compliance expectations such as the ADA's guidelines for web content and mobile applications

— Participation/competition from nonbanks/fintech firms is increasing though customers cannot always distinguish between banks and nonbanks, which may not be subject to banking rules

Cost efficiencies

— Regulators encourage new technologies that expand access or and convenience for customers or bring greater efficiency, risk detection, and accuracy to operations; investments must be tempered by monitoring and controls for reputation and third-party compliance risks

Additional KPMG perspectives

— SEC Regulation Best Interest

— CFPB debt collection proposal

— Renewed focus on Fair Housing

— CFPB proposes amendments to Payday Lending Rule

Data rich governance

Ethical conduct

Regulators are focused on the efforts of financial services companies to identify and prevent misconduct at its root. Conduct risk frameworks will be expected to include enhanced monitoring and surveillance, inclusive of advanced technologies and data analytics, as well as ongoing metrics, reporting, and governance. In addition, the framework will be expected to be integrated throughout the operations of the company as part of a culture of ethics and compliance, including demonstrated support by senior management and the board and clear consequences for misconduct. Key areas of concern will include customer data privacy, sales/trading practices, and fair treatment in addition to conflicts of interest, market conduct, incentive compensation plans, and third-party oversight.

Do the right thing, even when no one is looking

Technology transformation

— Financial services companies are investing in tools and capabilities to identify patterns and trends that can proactively detect and prevent incidents of ethical misconduct, including market manipulation and financial crime; regulators and stakeholders are increasingly expecting investigations of ethical misconduct to help prevent misconduct through diagnosis of systemic weaknesses in control and risk trends

— Automation can enable data validation and aggregation, provide a more formalized reporting loop, and offer an integrated view of potential misconduct; technologies capable of culling data from supporting documents (e.g., pdfs, Word documents) can support investigations and inform multidimensional metrics, enhancing predictive qualities

— The expanding use of artificial intelligence is raising ethical conduct issues related to transparency and machine bias, customer data privacy and digital rights, and third-party data usage

Customer interaction

— Conduct risk management frameworks should be applied enterprise-wide to capture and assess relevant information on incentive compensation plans, customer sales practices,, trading activities, and market integrity in order to demonstrate proactive monitoring and prevention of misconduct and related customer harm

— Qualitative data, such as information gleaned from customer surveys, focus group outreach, complaints portals, and social media commentary, should augment quantitative/hard data statistics regarding ethical conduct and corporate culture

Payments modernization

— Across bank and nonbank participants and the scope of payment channels and delivered services, regulatory concerns and industry standards focus on fair treatment/access and customer protections, including data privacy, funds availability, fee disclosures, fraud prevention, error resolution, and technology controls

— Innovative and evolving technologies facilitate faster transaction screening to keep pace with payments modernization, but can also introduce new regulatory and customer protection risks and increase expectations for supplier and third party procurement and risk management

KPMG

Market expansion

— Conduct and culture issues might be exposed during efforts to expand market presence, such as cultural integration challenges when engaged in M&A activities; employee incentive/reward programs that promote integrity-related risks; and the presence of subcultures that do not align with the values, ethics, and risk culture of the company

— Continuing talent acquisition challenges will hinder firms' abilities to define and operationalize their conduct risk frameworks

Cost efficiencies

— Leveraging technologies to efficiently define relevant taxonomies at sufficient levels of granularity that aids in uncovering trends, patterns, and correlations in order to generate insight and identify root causes of misconduct

Additional KPMG perspectives

— DOJ expands focus on effective compliance programs

— Banking culture: supervisory priority on 'softer' measures

— Financial Stability Board releases toolkit for mitigating misconduct risk

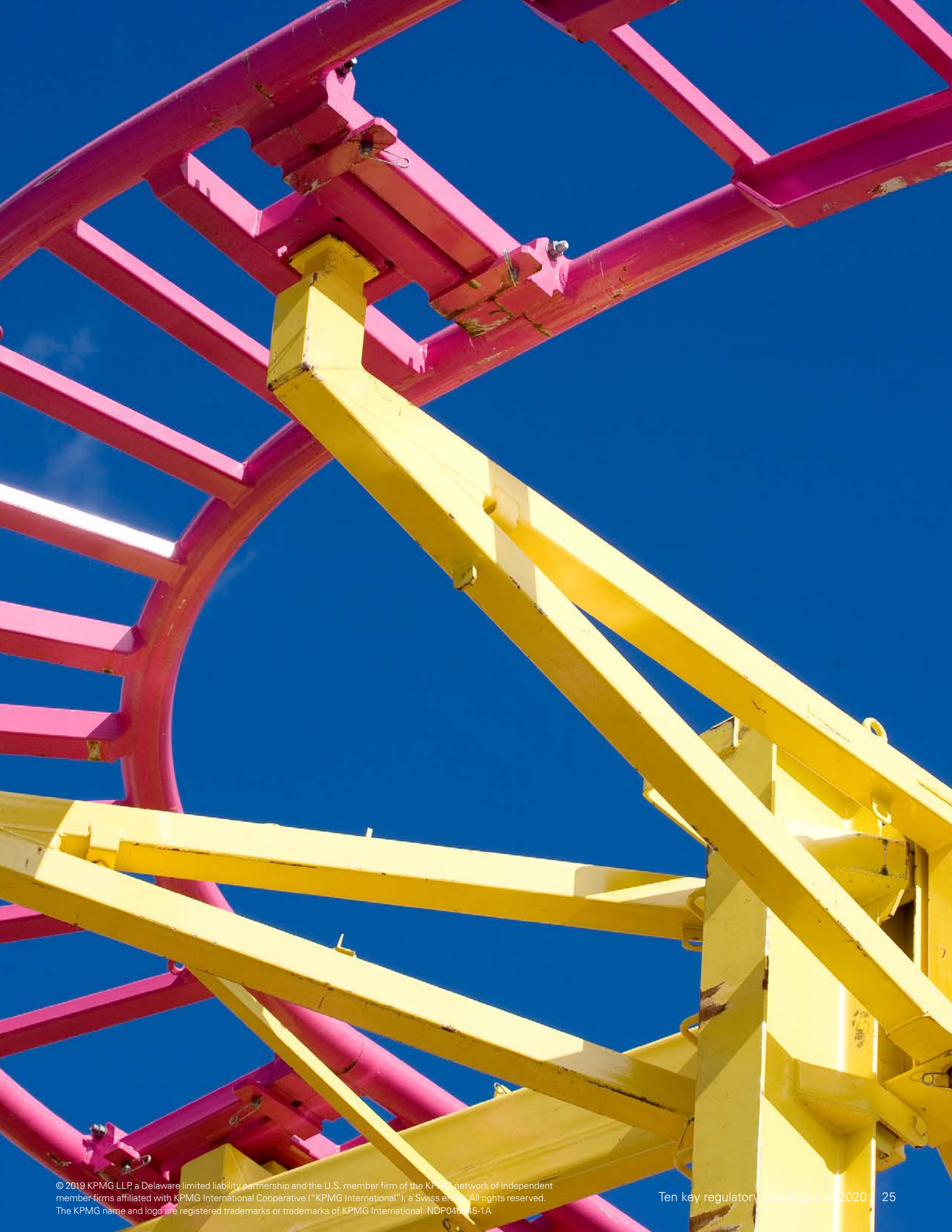
Revamping investigations: Future of ethics & compliance

Appendix

Defined terms and abbreviations

ADA	Americans with Disabilities Act
AI	Artificial Intelligence
AML	Anti-money laundering
BHC	Bank Holding Company
BSA	Bank Secrecy Act
CCPA	California Consumer Privacy Act
CECL	Current Expected Credit Losses
CFPB	Consumer Financial Protection Bureau
CFTC	Commodity Futures Trading Commission
DOJ	Department of Justice
DOL	Department of Labor
ESG	Environmental, social, and government
FINRA	Financial Institution Regulatory Authority
FRB	Federal Reserve Board
FTC	Federal Trade Commission
GDPR	General Data Protection Regulation
GSE	Government-Sponsored Enterprise
GSIB	Global Systemically Important Banks
HMDA	Home Mortgage Disclosure Act
IHC	Intermediate Holding Company
KYC	Know Your Customer
LIBOR	London Interbank Offered Rate
OCC	Office of the Comptroller of the Currency
SEC	Securities and Exchange Commission

KPMG



Acknowledgements

Contact us

Amy Matsuo
Principal and National Leader—Regulatory Insights
T: 919-664-7302
E: amatsuo@kpmg.com

Regulatory Insights Financial Services Steering Committee

Joseph Hargrove
Principal and Global Tax Leader—Financial Services
T: 212-872-5521
E: jhargrove@kpmg.com

David Reavy
Partner and National Sector Leader—Banking & Capital Markets
T: 212-909-5496
E: dreavy@kpmg.com

Jitendra Sharma
Principal, Americas Advisory Leader—Financial Services and Global Leader—Risk Consulting
T: 212-872-7604
E: jitendrasharma@kpmg.com

Authored by Amy Matsuo and Karen Staines

We would like to thank all of the following KPMG financial services professionals for their contributions and insights regarding the regulatory challenges for 2020: Deborah Bailey, Jeff Dykstra, Brian Hart, Orson Lucas, Frank Manahan, Greg Matthews, Lisa Newport, Todd Semanco, Anthony Sepci, Joe Slaninka, Nicole Stryker, Nicole Trawick

kpmg.com/socialmedia