



**INSIDE THIS PUBLICATION:**

As compliance evolves, so do accounting and finance

Government says FinTechs can compete with banks

If robots report to compliance

Data sharing, AI: antidote to failing AML efforts?

How AI is driving better risk and reward at AmEx

Is AI ready for financial compliance?

# Keeping compliance on track in a **High-tech world**

## About us

### COMPLIANCE WEEK

Compliance Week, published by Wilmington plc, is an information service on corporate governance, risk, and compliance that features a weekly electronic newsletter, a monthly print magazine, proprietary databases, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has become the go to resource for public company risk, compliance, and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance executives. <http://www.complianceweek.com>



Dun & Bradstreet helps customers improve business performance through the power of data and analytics. The Dun & Bradstreet Data Cloud delivers the world’s most comprehensive business data and analytics and provides unparalleled depth and breadth of business information that accelerates growth, reduces costs, manages risk, and transforms your business. Comprising over 300 million business records and thousands of attributes, our data is curated from tens of thousands of sources—both online and through our World-Wide Network of data partners around the globe—and is updated five million times each day. It encompasses the companies that make up the majority of the world’s GDP—meaning the companies you are most likely to do business with.

From the Data Cloud we derive our Live Business Identity, which delivers a comprehensive and continually updated view of any company in the Data Cloud. Live Business Identity starts with our universal identifier, the Dun & Bradstreet D-U-N-S® Number. The D-U-N-S Number is a unique nine-digit business identifier that is assigned once our patented identity resolution process, part of our DUNSRight methodology, identifies a company as being unique and distinct from any other in the Data Cloud. Consider Dun & Bradstreet’s unique Live Business Identity as a living, breathing descriptor of nearly every business on earth. Our data and analytics are delivered through the Data Cloud, which customers can access through our comprehensive solutions, APIs, and partner solutions.

Companies of every size around the world—including 90 percent of the Fortune 500™—rely on Dun & Bradstreet to improve business performance.

## Inside this e-Book

As compliance evolves, so do accounting and finance	4
Government says FinTechs can compete with banks	9
If robots report to compliance	12
Data sharing, AI: antidote to failing AML efforts?	15
How AI is driving better risk and reward at AmEx	18
Is AI ready for financial compliance?	20





# As technology evolves, so do accounting and finance

Robert Half and the Financial Executives Research Foundation reveal how evolving technology is rapidly enhancing the accounting and finance functions. **Jaclyn Jaeger** more.

**T**he pace at which technology is driving change in today's accounting and finance functions is accelerating at a rapid clip, resulting in boosted efficiencies, better collaboration with the business, enhanced compliance, and more.

Such was the theme from this year's accounting and finance benchmark report, developed jointly by Robert Half and the Financial Executives Research Foundation (FERF), the non-profit research affiliate of Financial Executives International. Based on survey responses from more than 1,700 financial leaders at public and private companies in the United States and Canada, the report also features insights gathered di-

rectly from interviews with financial executives.

"We have been tracking the automation trend closely as part of our benchmarking research for the past several years and, year in and year out, one thing emerges pretty clearly: Accounting and financing organizations throughout North America are only expanding their embrace of automation and, even more so, cloud computing," Dave Pelland, research consultant at FERG, said during a Webinar on the findings.

The intent of the report, Pelland said, is to help accounting and financial leaders assess how their accounting and finance functions operate relative to

their peers and provide insight on how to adjust management strategies to align with leading practices.

Key themes and trends discussed in this year's report include:

- » How accounting and finance functions are keeping pace with the evolving compliance landscape;
- » How technology trends are impacting accounting and finance functions, including driving the need for new skills; and
- » How accounting and financial leaders are managing everyday operations in response to heightened business expectations and a skills shortage.

Adoption of cloud-based solutions among accounting and finance leaders in North America continues to rise. In this year's survey, 75 percent of U.S. financial executives and 73 percent of Canadian financial executives said they either are currently using cloud-based solutions or plan to do so in the future.

The desire to boost efficiencies is a primary reason why accounting and finance leaders are moving to automation and the cloud. According to the report, accounting and finance leaders are using automation for routine tasks—such as data collection, management report generation, and document storage. "That gives accounting and finance teams more time to devote to analysis, collaboration with other business units, and help with decision support," said Paul McDonald, executive director at Robert Half.

Automating business processes, however, creates its own set of challenges. "A lot of organizations have processes with workarounds," Pelland said. "Those workarounds are probably a little bit trickier to automate and, so as financial leaders are thinking about automation, in some cases, they may need to clean up those processes before they can automate them."

Many respondents said they do not have plans, however, to automate processes that require strategic judgment, such as financial decision making and project management. For example, 26 percent of companies with less than \$500 million in revenue and 35 percent with more than \$500 million in revenue said they don't have plans to, or won't, automate financial

decision making.

Another trend changing the operations of many accounting and finance functions is "digital transformation" efforts, aka "digitization," which the report broadly defines as the application of technology "to create new business models and processes; drive innovation and revenue; and, in some cases, disrupt entire markets and industries." As such, digital transformation is an umbrella term that can include process automation, cloud-based solutions, data analytics tools, internet of things (IoT) devices, AI, and machine-learning technologies, the report states.

Winnie Leung, CFO at Canadian financial technology firm Moneris, said during the Webinar that one benefit of digitization is that it helps companies make risk-based decisions faster. Some solutions on the market enable firms like Moneris to reduce credit risk, for example, by taking information that the company may have on a client and layering in public data to help decide whether to advance credit to a certain customer, or whether it poses a risk to the firm.

Another firm in the early stages of automation as it moves toward digital transformation is Titan International. Jim Froisland, chief financial officer and chief information officer at Titan and one of the financial executives interviewed in the report, offered insight on starting the digital transformation journey: "You need to pick the right technology, of course, but before you do that, you need to define the business case and get the right resources behind it," Froisland said. "Define your business needs. Then, get the right skill sets. And then, get the right technology."

## Skills shortage

As companies pursue digital transformation efforts, demand for different skills among accounting and finance leaders is growing. According to the report, 17 percent of respondents at U.S. companies and 22 percent of Canadian companies have plans to expand their accounting and finance teams in response to digital transformation efforts.

As such, respondents listed several technical and non-technical skills that are becoming more important. Top technical skills that are in demand include,

“We have been tracking the automation trend closely as part of our benchmarking research for the past several years and, year in and year out, one thing emerges pretty clearly: Accounting and financing organizations throughout North America are only expanding their embrace of automation and, even more so, cloud computing.”

Dave Pelland, Research Consultant, Financial Executives Research Foundation

for example, experience with ERP systems and experience in data analytics.

Soft skills, like communication and creativity, are also high in demand—often even more so than technical skills. One reason for this, the report states, is that “accounting and finance professionals need a broader range of communication skills to work effectively with others across the organization because digital transformation efforts often require, as well as enable, extensive cross-departmental collaboration.”

Few respondents cited “knowledge of AI and robotic process automation” as a necessary skill. This is likely to soon change, however, as use of these technologies grows, McDonald said.

Companies that do decide to expand their teams likely will face a skills shortage. For example, 49 percent of companies with more than \$5 billion in revenue said they are either somewhat or severely understaffed. Meanwhile, the U.S. unemployment rate for accountants and auditors is just 2 percent.

Many companies are overcoming the skills gap by using interim staff, the report found. This year, 33 percent of U.S. respondents said they are using interim professionals, up from 28 percent in 2017. In Canada, 41 percent of companies said they are using interim professionals, up from 32 percent in 2017.

“We know from our interviews with finance executives that new mandates are adding to the compliance burden for many accounting and finance functions,” McDonald said. Thus, financial executives are increasingly turning to interim professionals to not only

support new initiatives, like digital transformation efforts, but also to meet evolving regulatory demands.

“For example,” the report states, “as accounting and finance functions have worked to implement revenue recognition and lease accounting standards, many have brought interim resources into their departments for extra support, either to lend expertise in those areas or to take on everyday tasks while full-time staff members focus on standards adoption.”

As the regulatory landscape continues to evolve and place more demanding compliance burdens onto accounting and finance leaders, those leaders “can add value by staying on top of what’s happening in the industry of accounting and finance,” Joan Cox, CFO of educational non-profit Head Start of Greater Dallas, said during the Webinar. Prudent accounting and financial executives today can stay on top of the latest trends in accounting and finance by participating in peer-to-peer forums, for example, to exchange knowledge and ideas, hear what challenges others are encountering in their companies, and how they are approaching those challenges, she said.

Financial executives have a key role to play in adding value to the business beyond just making sure that the company keeps accurate books and records. Leung challenges all financial executives to keep this one important question in mind: “How do we help the business grow and succeed, and where does the finance team play a role in that?” ■

## ACCOUNTANTS, AUDITORS TURN TO TECHNOLOGY TO COPE WITH CHANGE

Like other areas of the business, accounting and auditing are in something of a transformation as part of a digital mega-trend that is driving technological advancement. The digitizing of information has been going on since about the early 2000s, says Will Bible, audit innovation leader at Deloitte & Touche. Using a variety of different tools and approaches over many years, companies have been converting their information on products, services, and customers to digital data, developing new processes for how they do business along the way. That sets the stage for the next phase of technological advancement, which is automation and analytics, says Bible.

“Once you have information that’s digitized, how do you connect your systems to business processes so that it becomes automated?” says Bible. Technology is emerging to enable systems to interface with one another—robotics process automation, or RPA, as one example of such automation.

“RPA is essentially coding bots to act as if people were acting in a routine way,” says Bible. “Bots interface with the system like a person to process information systematically from one system to another. It saves people from having to copy and paste information from one system to another.” A new lease accounting standard has demonstrated for many companies where they could better leverage technology to not just achieve accounting compliance, but to improve their management of leases. At many companies, lease contracts have been signed and managed using various different methods at various locations literally all over the world.

Now companies are using various types of tools to centralize leases into single systems, read the

contracts for abstract terms that are important to the new accounting, enter data into accounting systems, and perform the new lease accounting calculations. “Anywhere you have systems that don’t talk to each other, one option is to build a bot to do that for you,” says Bible.

Cloud technology is another means of interfacing that is transforming accounting processes. Stacey Gilbert, senior vice president at KeyBank, says its cloud solution is proving critical to the implementation of and compliance with major changes in accounting standards.

Public companies adopted pervasive new requirements for how to recognize revenue at the start of 2018, and now they’re sprinting to the finish line to be ready for equally sweeping rules on how to recognize leases in financial statements. For financial institutions, an even more critical change takes place the following year is how to recognize credit losses, adopting the “current expected credit losses” model for projecting and reporting where a company may have risk in its portfolio.

New accounting standards are not only major changes for the accounting office, but they represent major changes for virtually every other area of the organization as well. A cloud approach connects people throughout the organization and allows them to work together more effectively, accessing and sharing information more efficiently and more confidently. That has been important in assessing the impact of new accounting standards, gathering and sharing data, and documenting every step of the journey. “As accounting experts, we’re relying on information coming from other people,” says Gilbert. As they

rely on that information to develop accounting policies, establish judgments and estimates, and assert proper control over financial statement assertions, accountants need to document that they've done their due diligence.

Using a cloud application enables not only the collaboration necessary to establish accounting policies and arrive at critical estimates and judgments, but it also documents the entire process, says Gilbert. As the Public Company Accounting Oversight Board has come down especially hard on auditors for their review of management review controls, the cloud platform with its documentation features has been "a huge win," says Gilbert.

Despite the potential of such applications to automate in a way that improves compliance, not all companies have embraced it as readily. A recent survey from consulting firm Protiviti says time and money spent on SOX compliance continue to rise, but corporate adoption of technology tools to automate the process is still lagging.

Only one-third of organizations, for example, are automating workflow approvals or access controls, and two-thirds are not using technology to test controls to demonstrate SOX compliance. Only 11 percent said they were using RPA, "the holy grail of having real-time, 24/7 monitoring," says Brian Christensen, executive vice president focused on internal audit at Protiviti.

Technological tools could remove some of the "monotonous, recurring work" associated with SOX, says Christensen, while also providing visibility into larger or even complete data sets rather than samples. The encouraging side of the poll result, he says, is that companies are trying

to get there. Roughly half said they are planning to deploy new technology specific to SOX in the next year.

Given the pace of change and the massive new opportunities created by technology, it can be difficult for companies to figure out where to invest their next dollar. The decision should start with an inventory of what's already in place, both from a systems and data perspective, says Dan Sunderland, chief auditor for the audit practice at Deloitte.

If a firm has a single platform that forms the basis of its Enterprise Resource Planning process, for example, that creates a different set of opportunities and challenges compared with a company operating multiple disparate systems. "Understand how accessible and uniform the data is within the organization, so you can start to see what is feasible to work with in the short run," says Sunderland.

The analysis can then identify intersections of complex accounting judgments and data supporting those judgements, or areas that are typically most problematic, to identify where perhaps manual steps could be replaced with automated processes, or where data could be better mined and analyzed, says Sunderland.

It's a difficult process, in part because the business and the external environment are always changing, he says. "To enable folks to really utilize technology, you have to get down into the details," he says. "What is truly data that I can analyze to inform my decision-making processes and not just data for data's sake?"

—Tammy Whitehouse



## Government says FinTechs can compete with banks

In separate developments announced in July, the U.S. Department of Treasury and the Office of the Comptroller of the Currency paved the way for FinTech firms and other non-banks to more easily compete with traditional banks. Once again, opponents are threatening legal action. **Jaclyn Jaeger** explores.

The U.S. Department of Treasury and the Office of the Comptroller of the Currency each announced developments that pave the way for FinTech firms and other non-banks to more easily compete with traditional banks.

The first development came on July 31 from the U.S. Department of Treasury in the form of a 222-page report, "identifying improvements to the regulatory landscape that will better support nonbank financial institutions, embrace financial technology, and foster innovation," the Treasury stated. It is the fourth report issued by Treasury, under the direction of Secretary Steven Mnuchin, in response to Executive Order 13772.

(Issued by President Trump in February 2017, the executive order called on the Treasury Depart-

ment to identify laws and regulations that are inconsistent with the Core Principles it set forth for financial regulation.)

"Creating a regulatory environment that supports responsible innovation is crucial for economic growth and success, particularly in the financial sector," Mnuchin said in a statement. "America is a leader in innovation. We must keep pace with industry changes and encourage financial ingenuity to foster the nation's vibrant financial services and technology sectors."

In drafting the report, Treasury said it consulted extensively with a wide range of stakeholders focused on consumer financial data aggregation, lending, payments, credit servicing, financial technology, and innovation.



Treasury further said its recommendations “are designed to facilitate U.S. firm innovation by streamlining and refining the regulatory environment. These improvements should enable U.S. firms to more rapidly adopt competitive technologies, safeguard consumer data, and operate with greater regulatory efficiency.”

Treasury’s report identifies just over 80 recommendations that are designed to:

- » Embrace the efficient and responsible use of consumer financial data and competitive technologies;
- » Streamline the regulatory environment to foster innovation and avoid fragmentation;
- » Modernize regulations for an array of financial products and activities; and
- » Facilitate “regulatory sandboxes” to promote innovation.

The second development came from the Office of the Comptroller of the Currency (OCC), which announced on the same day as the Treasury report that it will begin accepting national bank charter applications from FinTech firms. “The federal banking system must continue to evolve and embrace innovation to meet the changing customer needs and serve as a source of strength for the nation’s economy,” Comptroller of the Currency Joseph Otting said in a statement.

“The decision to consider applications for special purpose national bank charters from innovative companies helps provide more choices to consumers and businesses and creates greater opportunity for companies that want to provide banking services in America,” Otting added. “Companies that provide banking services in innovative ways deserve the opportunity to pursue that business on a national scale as a federally chartered, regulated bank.”

The OCC said its decision follows extensive outreach with many stakeholders over a two-year period, and after reviewing public comments solicited following the publication of Exploring Special Pur-

pose National Bank Charters for Fintech Companies in December 2016 and Comptroller’s Licensing Manual Draft Supplement: Evaluating Charter Applications From Financial Technology Companies in March 2017.

#### Charter details

In announcing the decision, the policy statement and Comptroller’s Licensing Manual Supplement stress that “every application will be evaluated on its unique facts and circumstances.” The OCC also said that FinTech firms that apply and qualify for, and receive, special purpose national bank charters “will be supervised like similarly situated national banks, to include capital, liquidity, and financial inclusion commitments as appropriate.”

Additionally, FinTech firms “will be expected to submit an acceptable contingency plan to address significant financial stress that could threaten the viability of the bank,” the OCC said. “The plan would outline strategies for restoring the bank’s financial strength and options for selling, merging, or liquidating the bank in the event the recovery strategies are not effective.”

The expectations for promoting financial inclusion will depend on the company’s business model and the types of planned products, services, and activities. New FinTech firms that become special purpose national banks will be subject to heightened supervision initially, like other de novo banks, the OCC said.

The OCC further stressed that it has the authority, expertise, processes, procedures, and resources necessary to supervise FinTech firms that become national banks and to unwind a FinTech firm that becomes a national bank if it fails.

The OCC said qualifying FinTech firms may also apply for federal charters under the OCC’s authority to charter full-service national banks and other special purpose banks—such as trust banks, banker’s banks, and credit card banks.

“A national bank charter is only one option among many for companies engaged in the business of banking,” the OCC said. “Other options in-

clude pursuing state banking charters, appropriate business licenses, and partnerships with other federal or state financial institutions.”

In a statement, Otting said, “Providing a path for FinTech companies to become national banks can make the federal banking system stronger by promoting economic growth and opportunity, modernization and innovation, and competition. It also provides consumers greater choice, can promote financial inclusion, and creates a more level playing field for financial services competition.”

#### Industry reaction

The Treasury and OCC developments elicited both cheers and jeers. The Conference of State Bank Supervisors (CSBS), which last year filed a lawsuit opposing the OCC’s national bank charter, is expected to legally challenge it again. “An OCC FinTech charter is a regulatory train wreck in the making,” CSBS President John Ryan said in a statement.

“Such a move exceeds the current authority granted by Congress to the OCC,” Ryan added. “FinTech charter decisions would place the federal government in the business of picking winners and losers in the marketplace. And taxpayers would be exposed to a new risk: failed FinTechs.”

The CSBS also challenged certain recommendations in the Treasury report. “We do not support creation of new federal rules or unauthorized federal charters that would seek to compromise the ability of state officials to apply and enforce state laws and, so, we disagree with Treasury’s recommended changes to the valid-when-made doctrine and the true-lender doctrine, and the creation of an OCC special purpose bank charter for FinTech companies,” the CSBS stated.

Other critics include advocates at the National Consumer Law Center, Americans for Financial Reform, the Center for Responsible Lending, the Consumer Federation of America, and U.S. PIRG. Like the CSBS, these groups argued that this move is outside the authority of the OCC.

“The OCC does not have the legal authority to hand out ‘national bank’ charters to entities that do

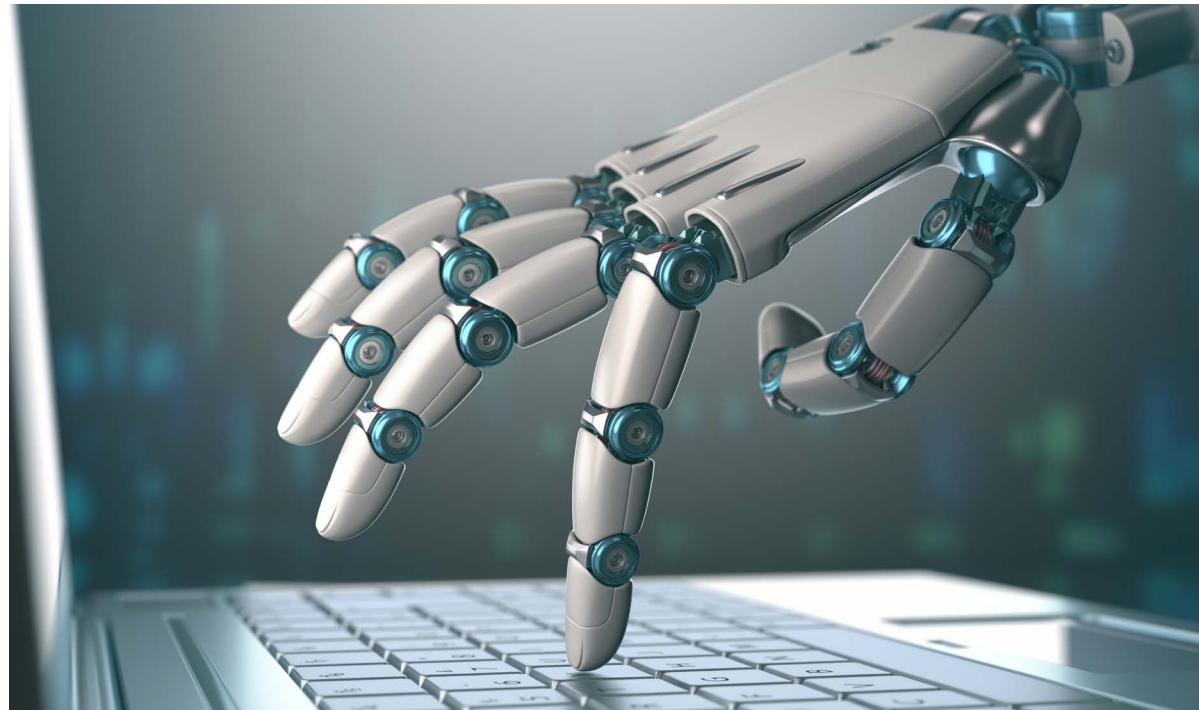
not take deposits,” said Linda Jun with the Americans for Financial Reform. “I expect the courts will stop this power grab by the OCC.”

“Giving ‘national bank’ charters to non-bank lenders could open the floodgates to a wide range of predatory actors making loans at 100 percent APR or higher,” said Lauren Saunders, associate director of the National Consumer Law Center. According to a report conducted last year by the National Consumer Law Center, two-thirds of states cap a \$2,000 loan at 36 percent or less, but a non-bank charter could allow lenders to avoid those limits, Saunders said. In 2017, more than 250 organizations sent a letter to the OCC opposing a FinTech national bank charter.

The New York Department of Financial Services (NYDFS) expressed similar concerns, stating that it “strongly opposes” the OCC’s efforts. “DFS believes that this endeavor, which is also wrongly supported by the Treasury Department, is clearly not authorized under the National Bank Act,” NYDFS said. “As DFS has noted since the OCC’s proposal, a national FinTech charter will impose an entirely unjustified federal regulatory scheme on an already fully functional and deeply rooted state regulatory landscape.”

Additionally, the NYDFS said it “fiercely opposes” Treasury’s endorsement of regulatory “sandboxes” for FinTech firms—which allow firms test out new products, services, or business models under a regulator’s supervision. “The idea that innovation will flourish only by allowing companies to evade laws that protect consumers, and which also safeguard markets and mitigate risk for the financial services industry, is preposterous,” Superintendent Maria Vullo said in a statement.

Others, however, praised the changes. Jason Oxman, chief executive of the Electronic Transaction Association, applauded the OCC for creating a “consistent and uniform regulatory framework for FinTech companies.” Oxman added, “This type of clarity benefits everyone by ensuring that industry, customers, and regulators are operating from the same rules and expectations.” ■



# If robots report to compliance

Experts at CW's innovation summit had some helpful advice on adopting new technologies. **Jaclyn Jaeger** reports.

At Compliance Week's Technology Innovation & Compliance Summit, held June 26 in Boston, compliance officers and audit professionals gathered to discuss how data analytics—such as artificial intelligence (AI) and robotic process automation (RPA)—is advancing the role of compliance and audit, what challenges they create, and what benefits are being realized.

"Technologies around artificial intelligence exist. It's finding the use cases and the practical applications of how that's going to be implemented at companies to derive meaningful insights that's the challenge," said Scott Szalony, an audit and assurance partner at Deloitte & Touche, speaking at the Summit.

Some companies are already making strides. In a poll conducted by Compliance Week, 50 percent of respondents said they have already begun to integrate, or are well on their way to integrating, data analytics technologies within certain compliance and audit

functions, whereas the other 50 percent said they are likely to.

A few examples of new technologies that companies are starting to employ include:

**Robotic process automation:** In its simplest form, RPA is the automation of repetitive tasks and business processes that mimic human computer activities—things like logging into a system, entering data, and copying and pasting data across many systems and departments. Processes automated through RPA must be rules-based—be it in finance, customer service, or operations. As just one example, RPA can enhance the accounting close process by gathering and consolidating transactions recorded in journals and reconciling them in an ERP system.

**Artificial intelligence (AI):** One limitation of RPA is that you can only input structured data, like spreadsheets and databases. In this way, AI complements RPA by taking unstructured data—like e-mails, phone

calls, meeting transcripts, contracts, bank checks—and putting them into a structured format. The capabilities it affords are also "smarter" than RPA in many ways. As just one example of this, certain cognitive AI technologies can read signatures to help find forged documents. Also, unlike RPA, AI provides for more sophisticated data models that help companies to enhance their decision-making processes.

**Data visualization.** Data visualization essentially is the art of data, presented through charts and graphs. Just as AI complements RPA, data visualization complements AI by turning large amounts of complex data into attractive visuals that make it easier to interpret the data.

Companies that have had early success with automation generally start with low-hanging fruit. They first find an area where they can perform a proof of concept to prove the value of automation before moving onto larger projects. "Generally, the best use cases are use cases where data is readily available," said Jennifer Gerasimov, a managing director at Deloitte Advisory.

Accounts payable data is a good starting point for data that most companies have readily available. General Electric, for example, "has a data lake that our IT team has put together for all our AP systems," said Thanh Tsoi, director of compliance—digital transformation at General Electric. "We are looking for outliers and patterns and trends to identify risk." Specific examples might include high employee spend in certain customer accounts, or high spend in a certain region of the world.

GE has independent data scientists that analyze data for trends to identify risk factors, Tsoi added. Those data scientists understand what risks the business is trying to mitigate, "but also I understand what they need to do to get their job done," she said, adding that the partnership is invaluable.

On the machine learning side, "our analysis and monitoring team can now focus on high-risk transactions," Tsoi added. "That's been effective in mitigating a lot of risk."

Another consideration is what actions to take once the business has gathered and analyzed the data.

"Data visualization is pretty, but are you actually taking action on it?" Tsoi said.

Looking at the broader picture of data analytics, automation is intended to enhance—not replace—human intelligence. "There is value in individual knowledge and experience, and that should not be forgotten," Gerasimov said. There is always going to be the need for humans to translate what the data means in relation to the risks that the business faces, and what predictive modeling can be garnered from it.

The ownership and accountability piece is another important factor, Tsoi said. Who will advocate for automation? Who understands the process? Who will take accountability and will want to improve it? This individual—typically, the end user—should be included in the early stages of the process to help define requirements.

Just as important as the human element is the security and privacy side of automation. It's important to be critical about the reasoning behind why the business is keeping data. "What are you going to use that data for? Don't just pull it because you might use it later," Tsoi said.

On the assurance and audit side, technology innovations are also on the radar of accounting and auditing firms. "Many don't think of the auditing field as a tech-driven industry, but if our clients are going there, then the auditors have to go there," said Catherine Ide, managing director of professional practice and member services at the Center for Audit Quality (CAQ). "Our clients are going to expect us to modernize and become more effective and efficient as they are making investments in their own companies."

Thus, audit firms are making major investments in cognitive technology, like machine learning and pattern recognition, she said. Internal auditors are looking to employ new technology, like data visualization, in their audits as well.

Continued strife over new lease accounting standards taking effect next year only adds to the incentive for audit to move further along the technology continuum. "Companies and audit firms alike are thinking about using this as an impetus to monitor how they track their leases in terms of both inventory, as well as

accounting,” Ide said. The opportunity is there to use document-extraction software and machine learning to pull out key terms in a contract, she said.

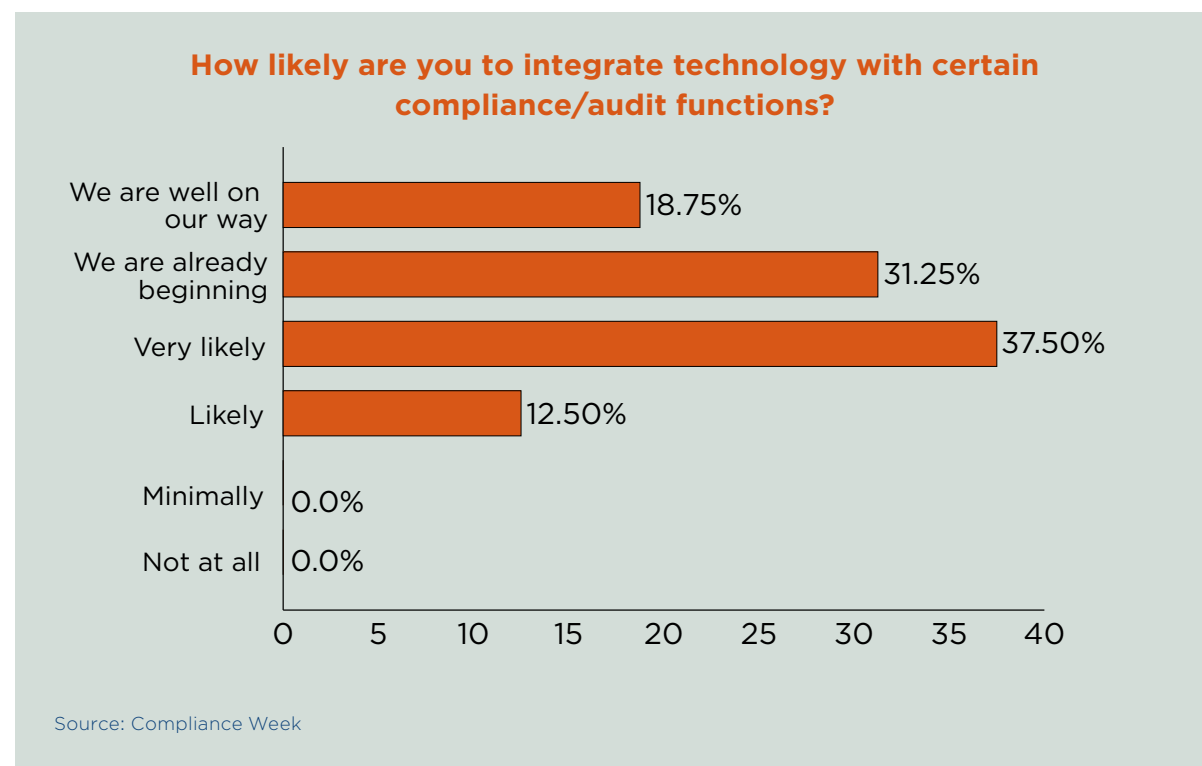
Also key will be the ability of accounting oversight bodies—like the Public Company Accounting Oversight Board and the Financial Accounting Oversight Board—to keep up with the pace of technological change. In terms of auditing standards promulgated by the PCAOB, for example, “there’s likely an opportunity for additional guidance for auditors about implementing these types of more sophisticated risk analysis tools and data analytics,” Ide said.

Most agreed. Specifically, when asked about the regulatory approach to cutting-edge tech, 62.5 percent said it should be treated like any other risk factor that requires rules and oversight.

There’s also more work to be done as preparers look to the Securities and Exchange Commission for guidance on how to adopt these technologies. From a

financial accounting standards perspective, Ide noted that “significant accounting and auditing questions” remain as it concerns companies that utilize technologies like bitcoin, for example. As the SEC ramps up its interest in this area, “the regulatory umbrella will have an impact,” she said.

As the adage goes, “a picture is worth a thousand words,” but in the world of compliance and audit, that picture is worth a thousand words only if you can understand the data, Ide said. That’s applicable to not just auditors using data analytics, but also management seeking to understand more about the risks their companies face and audit committees seeking to better understand what risks they should be thinking about from an oversight perspective. “These tools and technologies are enabling not just the auditor,” Ide concluded, “but [giving] everybody in the financial reporting supply chain a better lens into the risks associated with the business.” ■



## Data sharing, AI: antidote to failing AML efforts?

Big data may revolutionize anti-money laundering efforts, but privacy concerns and preserving a human element to compliance programs may get in the way. **Joe Mont** explores.

In an age of political impasse, the need to update the Bank Secrecy Act and Anti-Money Laundering regulatory regimes has become a bipartisan cause. Among the ideas: resolving the privacy roadblocks to data sharing and using modern technology, including artificial intelligence and machine learning, to do the detective/grunt work.

To that end, Rep. Ed Royce (R-Calif.) introduced the Anti-Money Laundering Modernization Act of 2017 last September. “Our nation’s anti-money laundering and countering terrorism financing regime has been a 40-year work in progress, and there is increasing recognition that it needs to be modernized,” Royce said of the bill’s introduction. “Our regulatory infrastructure must keep pace with the times. Criminal syndicates, rogue nations and terrorist networks are not sitting idly by, and neither can we.”

The bill would also expand the ability of financial

institutions to share suspicious activity reports within their organization to improve enterprise-wide risk management and require Treasury to improve qualitative feedback for financial institutions and Federal financial regulators on their AML/CTF efforts.

Importantly, the legislation would also require Treasury to explore the potential for artificial intelligence, machine learning, and other technologies to help detect and prevent money laundering and terrorist financing.

The prospect of applying AI and other technological advances to AML programs was also a recurring theme at a Jan. 9 Senate Banking Committee hearing.

At the hearing, Greg Baer, president of the Clearing House Association, laid out the many problems currently facing the nation’s AML regime.

“Our AML/CTF system is broken,” he said. “A core problem is that today’s regime is geared toward com-



pliance expectations that bear little relationship to the actual goal of preventing or detecting financial crime ... Fundamental change is required to make this system an effective law enforcement and national security tool, and reduce its collateral damage.

The regulatory regime, he said, “is a system in which banks have been deputized to act as quasi law-enforcement agencies and where the largest firms collectively spend billions of dollars each year, amounting to an annual budget somewhere between that of the ATF and the FBI.”

Large banks, Baer said, have been pushed away from risk-based approaches, because their performance is not graded by law enforcement or national security officials, but rather by bank examiners.

“Those examiners focus on what they know and control: policies, procedures, and quantifiable metrics—for example, the number of computer alerts generated, the number of SARs filed, and the number of compliance employees hired,” he added. “This means that a firm can have a program that is technically compliant, but is not effective at identifying suspicious activity, or is producing adverse collateral consequences.” As a result, he said, banks are filing SARs that are in less than 10 percent of cases followed up on in any way. For certain categories of SARs, the yield is close to 0 percent percent.

Baer said that one AML director recently testified that his firm employs 800 individuals worldwide fully dedicated to AML/CFT compliance, detection and investigation work, as well as economic sanctions compliance. Today, a little over half of these people are dedicated to finding customers or activity that is suspicious. The remainder—and the vast majority of employees dedicated to these efforts in the business and operations teams that support the firm’s AML program—are devoted to perfecting policies and procedures; conducting quality assurance over data and processes; documenting, explaining, and governing decisions taken relating to their compliance program; and managing the testing, auditing, and examinations of their program and systems.

By point of reference, the more than 800 is greater than the combined authorized full-time employees in

Treasury’s Office of Terrorism and Financial Intelligence and FinCEN.

Baer urged officials and financial institutions to consider the potential for the use of AI and machine learning to improve AML systems.

“AI does not search for typologies but rather mines data to detect anomalies,” he explained. “It gets progressively smarter; it would not be easily evaded; and different banks with different profiles would end up producing different outcomes. The current system is not progressing from typology to anomaly, however, because there has been no signal whatsoever from the regulatory agencies that dollars can be shifted from the existing, rules-based system to a better one.”

But there are obstacles, Baer said. AI strategies require feedback loops, which do not exist in the current system. In addition, there are barriers to cross-border information sharing of suspicious activity for global financial institutions.

Baer also encouraged the exchange of AML/CFT information between the government and the private sector as well as between and among financial institutions. He applauded the FinCEN Exchange program, launched on December 4, in which FinCEN will meet with law enforcement and financial institutions every six to eight weeks to exchange information on priority illicit finance threats, including targeted information and broader typologies. This is intended to enable financial institutions to better identify risks and focus on high-priority issues.

“Such sharing not only makes financial institutions’ programs more effective and efficient, it assists in focusing their resources on important matters,” he said.

“Strong public-private partnerships and two-way information sharing is a crucial component of our efforts to combat the sophisticated money laundering methods and evolving threats we face today,” said Sigal Mandelker, Treasury Under Secretary for Terrorism and Financial Intelligence.

Private-sector participation in FinCEN Exchange is strictly voluntary, and the program does not introduce any new regulatory requirements.

“Improving information sharing is not limited to the exchange of information between the public and private sectors. We welcome efforts by financial institutions to share information with each other,” Mandelker said.

“We know that some banks have started forming consortia to share information more dynamically under Section 314(b) of the USA PATRIOT Act,” he added. “By working together, these groups of financial institutions have provided substantial insight into illicit finance threats that otherwise may be invisible to a single institution. We are highly encouraged by the private sector’s willingness to engage in this type of exchange, and we appreciate the amount of time and effort that is going into these projects.”

Heather Lowe is legal counsel and director of government affairs at Global Financial Integrity, an organization dedicated to curtail illicit financial flows. She

supports greater information sharing among banks and with the government, but adds a caution.

“While we generally support greater sharing of information in the AML area, it must be done with appropriate privacy safeguards,” she says. “Where it may result in a person being denied banking services at all, there must be a system for redress for people to be able to restore that access if they can demonstrate that they are involved in legitimate activity.”

“Transferring raw banking data from banks to FinCEN to analyze (with appropriate privacy safeguards) is not a bad idea,” Lowe added. “However, it is essential that we do not absolve banks of the responsibility to carry out their own analysis as well, which they have the ability to review within the context of the additional client information that they have, because they are the gatekeepers to the financial system. The federal government cannot do this alone.” ■

## War on money laundering

Another imperative in the fight against money laundering is ensuring boards of directors also make the crime more of a priority. Even though financial institutions are aware of risks related to money laundering- and sanctions-related investigations, many of them may be “de-risking”—disassociating themselves, perhaps needlessly, from otherwise-profitable businesses and relationships,

That’s according to a survey of financial services executives and boards of 361 financial institutions around the world recently released by AlixPartners, a global business advisory firm. At the same time, a significant number lack both adequate AML and sanctions compliance budgets and training for their boards.

According to the survey, nearly two-thirds of respondents have experienced de-risking in one form or another—a trend that could actually in-

crease institutions’ AML and sanctions risks, as customers seek other avenues for conducting their business with the institution, such as creating “nested” relationships in the case of correspondent banks. This could be even more difficult to detect and subsequently report potentially suspicious activity and/or sanctions violations.

Meanwhile, 32 percent of respondents say they consider the AML and sanctions-compliance budgets at their firms to be “inadequate” or “severely inadequate.” And, in what the survey’s authors say may be a sign that an understanding of AML and sanctions risks hasn’t fully permeated the upper reaches of many financial institutions, 20 percent of respondents say their board is not receiving AML and sanctions training and regular briefings, despite many new compliance standards having recently been implemented around the world.

—Joe Mont



## AI driving better risk & reward at AmEx

**Bill Coffin** talks with American Express Chief Risk Officer Paul Fabara, about the company's proprietary artificial intelligence-driven data management system.

For much of last year, “artificial intelligence” and “machine learning” were buzzwords that got thrown around a lot in the compliance world. And while many CCOs could readily imagine how an AI-driven data management system—one that could take the data it already handles and learn how to make increasingly relevant correlations between that data and new, incoming data—there remained few examples of how such a system might look in practice.

Thankfully, such examples are beginning to emerge, and one that is especially interesting is a proprietary system currently up and running at American Express. Amex handles a staggering number of financial transactions each day, and as such,

it needed a smarter, faster, stronger data management system to address not just the company's vast compliance needs, but also to help drive better overall risk management. And that is where Paul Fabara, American Express's chief risk officer comes in.

Compliance Week had the chance to speak with Paul a few times last year as American Express brought its new system online. The system was born from the need American Express recognized internally that its risk oversight largely was backward-looking. “Management, action plans from internal audit, complaints, regulatory notices, MRAs provided by the government...all that plus independent compliance testing results in a lot of lag indicators,” Fabara said.

What Fabara wanted was a system that could produce a report of how his ERM program was performing in the context of fulfilling American Express' promises made to customers clients on a daily basis, as well as the company's commitment to its regulatory obligations. That was the catalyst, as Fabara calls it, for him to challenge his group to find the best way to meet these needs. The way forward, it was decided, was a next-generation, real-time monitoring system that captured as much of the company's operational data as possible.

“We wanted to go upstream and monitor the entire life cycle of an account,” Fabara explained. “From the time we onboard the account, to the pre-screening of possible personal or commercial cardholders, all the way to the end of life of an account.”

The system American Express has previously used captured up to 300 key risk indicators on any given account. The new system captures more than 1,000 KRIs per account, and that number is continuing to increase. The KRIs are not just driven by control and compliance, Fabara said, but by safety and soundness as well.

KRIs also define the risk appetite framework. At what point does an alert become something to work through? That's important, Fabara says, because he wants his human operators to focus on investigating true issues, not false positives. So there needs to be levels of tolerance built up so that by the time the system tolerance has been breached on a particular item, there is a necessity to investigate. To handle it all, the system uses a case management engine that enables Fabara's team to file, store, query and fulfil a particular alert. Any time an alert is generated, it also creates an obligation to investigate the issue. “When there is an alert, it's not a thing of where there is smoke, there is fire,” Fabara said. With this system, “now, for a fact, we know there is fire.”

That all works thanks to an AI-driven system that can forecast issues before they actually become issues. Fabara likens it to in the aerospace industry, when companies can tell a part is about to fail based on data for how often it's used before a stress fracture emerges. “With us, indication comes in differ-

ent forms, such as customer calls and writing, so we can see common denominators to detect if there is a defect in the system or not,” Fabara says. This capability still in early stages, he adds, but AI-driven monitoring is handling the bulk of work done in real-time monitoring, and the results have been positive thus far.

The most important thing, however, is the human element; specifically, arming compliance professionals with specialized tools to enhance their quality of compliance dialogue. “Most of the time, the discussions you have with the compliance officer will be about events that already happened,” Fabara said. “At American Express, we want compliance officers to be part of the growth strategy, but they need the tools to make sure out operating units are working safely.”

Unfortunately, Fabara can't provide examples of specific cases handled by the system because a lot of it involves confidential information. What he can say, however, is that many events the system highlights are considered to be “operational opportunities.” Those are data correlations the system identifies that merit investigation by the teams who generate new products and services. The system isn't just about controlling governance across American Express. It's also about improving the customer experience by providing actionable data to marketing, customer service, and other departments.

Historically, chief compliance officers and lead operational risk officers discussed lag indicators from the past to try to improve the future,” Fabara said. “Now, we are using real-time data from the system to allow compliance officers to have more substantive dialogue, with empirical data, to speak to the health of a particular business unit. It gives risk and compliance officers a seat at the table when we are creating new products because they already have an in-depth knowledge of how products are already performing. It's changing the dialogue. Businesses are not coming to us. Now they know they have a true partner that wants to help them do things better.” ■

# Is AI ready for financial compliance?

**Daniel Fernandez** has more on how to incorporate “artificial intelligence” and “machine learning” into the compliance function.

Like many industry buzzwords, artificial intelligence (AI) has become a hot topic that RegTech technologists often write about, but also an overloaded and misused term, often mistaken for Machine Learning (ML). How does one clarify the two?

In simple terms, artificial intelligence enables computer systems to perform tasks that require human intelligence. Intelligence is the key word. In contrast, Machine Learning refers to a computer system that has the ability to learn how to do specific tasks and, in some instances, can use past data to make future decisions or predictions without being explicitly “told” (programmed) how to do so. Machine learning is a key building block of artificial intelligence.

**Contextualizing machine learning.** AI and ML are often confused because the terms are used interchangeably. Today, ML is used in many narrow compliance applications, including risk detection models, and other event classification use cases. A narrow ML application, however, does not constitute artificial intelligence in the context of compliance.

That being said, a combination of systems and programs (based on ML) could constitute an Artificially Intelligent System, although no such systems truly exist in the compliance realm today.

Most artificially intelligent systems use a combination of machine learning applications and techniques along with rule-based systems (to be fully interactive). For example, phone-based smart assistant applications (such as Google Now, Siri, Cortana, and Alexa) use a set of application components mostly powered by machine learning. These include: language identification, translations, transcriptions, natural language understanding, etc. In these interactions you can perform tasks such as booking a cab (“Siri, I need to hail a taxi cab to get me from 129 Portland Street to South Station”), where the following steps are performed behind the scenes: understand your com-

mand of requesting a car service and your destination; detect your location and determine your optimal pickup location; reach a nearby driver and agree with this driver on taking this trip; and communicate back to you with an estimated fare for final confirmation.

Interacting with a smart assistant in this manner can be considered Artificial Intelligence because the smart assistant fully replaces a human (the taxi dispatcher), who would normally perform these tasks. Thus, human interaction is bypassed altogether.

**Why compliance needs hybrid intelligence.** While taxi dispatchers can be replaced by AI, the same cannot be said for compliance analysts. And this is a good thing, because while smart machines and complex algorithms can process a lot of data to automate and perform some human tasks, faster, there are limitations. For example, the current machine learning models and advanced statistical techniques can process far more messages, trades, and records than humans can, but today humans are still needed to review, apply judgment, and make decisions about compliant communications. Why?

First, such decisions involve substantial operational and financial risk and potential severe legal consequences and reputational damage. Secondly, true AI systems need to learn what is good (compliant) and bad (non-compliant) behavior, and there simply aren't enough instances of non-compliant communications in a firm's data for an AI machine to learn this and make reliable decisions.

So, when it comes to financial communications compliance, while technology can eliminate the time-consuming tasks entailing large data analysis, it is no substitute for the decision-making abilities of the compliance analyst, at least not today.

**The data integration/aggregation challenge in machine learning technologies.** Adoption of ML technologies is accelerating across many industries

thanks in large part to a renewed focus on applied problems and sharing of research findings. Still, one of the biggest challenges of ML remains unsolved. Machine learning relies on data.

Most advanced analytics projects devote a large portion of time to identifying and curating the necessary data to feed advanced algorithms. But are the analytics engines themselves flexible enough to handle all of these data inputs? In some cases, the answer is no as some ML systems are constrained to accepting only certain types of data in certain types of formats.

This exact concern was highlighted in a recent research report by Jefferies, a global investment banking firm. The report focused on issues related to IBM Watson and highlighted an example of a health sciences project that required a significant amount of services and effort to integrate data sources from different systems and did not produce the desired results.

According to the Jefferies report, for example, MD Anderson has already spent over \$60 million dollars on a Watson project and stated that “IBM is very ‘picky’ about the data it feeds Watson.” The project has since been halted because of the extensive integration that would have been required to make it work with MD Anderson's systems.

As part of their normal course of business, financial institutions already have to archive and analyze large amounts of data. By implication, ML platforms that rely on restrictive data inputs only make this problem worse. Financial institutions would need to store separate data in different formats in order to support advanced analytics models.

In communications compliance, this becomes a much bigger problem due to the large variety of structured and unstructured data sources. Financial firms need to weigh the pros and cons—should I invest in a one-off ML project which requires custom integration, or layer ML on top of my existing surveillance solution? A lot of work already goes into making data useable for the surveillance process—why not leverage the data that your organization has already organized and curated for ML as well?

The expectation needs to be that ML is not intended to be self-sufficient. It needs to work hand-in-hand

with a human compliance analyst, at least for today.

Fit for use is another challenge these projects face. This issue of the usability of the data was also highlighted in the MD Anderson/Watson audit, which concluded that the Watson system was “not ready for human investigational or clinical use.”

Just having an ML system spit out results is not enough. You have to be able to integrate these results into the day-to-day supervision and investigative workflow of your compliance analysts, in a way that's intuitive and contextual. This ensures that your ML is not just creating “more noise” but instead providing useful information for decision making.

**The expanding role of machine learning in compliance.** Today, numbers alone are not useful to compliance analysts. Consider, for example, under regulations such as MAR and MiFID II (which will soon go into effect), it is no longer sufficient to just monitor for actual fraudulent trading practices; firms also need to monitor communications for “intent to commit market abuse” throughout a trade or transaction lifecycle. This necessitates obtaining additional context surrounding monitored users and their respective activities. This might include behavior anomalies, relationship discrepancies, or other fluctuations in communications or trade data.

The expectation for such analysis is also being driven by regulators such as the Securities and Exchange Commission, which has already started to incorporate these techniques into their daily compliance processes. SEC Acting Director Scott W. Bauguess (also acting chief economist DERA) said during an OpRisk North America presentation in June 2017 that the SEC uses “unsupervised algorithms to detect patterns and anomalies in the data, using nothing but the data.”

When it comes to financial communications compliance, machine learning technologies can truly improve the compliance process, but only if they fit into your firm's current workflow. There's no such thing as true AI in financial compliance (at least not yet), but ML can enhance your compliance team's view of monitored users, help to detect financial communications compliance issues, and—if implemented and applied correctly—facilitate analyst decision making. ■





# Make Third-Party Risk Management Less Painful

Dun & Bradstreet's Data Cloud of over 300 million business records provides the corporate linkage, ownership structures and 360 degree view of third party entities to help you remain compliant with regulatory pressures.

To learn more, call 1-855-556-9872  
or visit [dnb.com/compliance](http://dnb.com/compliance)