Treliant

New Coordinates

SUMMER 2019

IN THIS ISSUE

Summer Salutations!. 1

Financial Crimes Compliance Officers and the Age of Change. 4

Managing Compliance Risk in an Era of Innovation 7

Insurtech: Managing Risks to Consumer Privacy, Information Security, and Fairness 11

New Coordinates is published quarterly by Treliant, provider of trusted advisory services and specialized business solutions. In each issue, we analyze opportunities, challenges, and best practices in the global market for financial products and services.

Managing Editor
Melissa S. Pazornik

Washington, DC
202.249.7950

New York, NY
646.315.9430

Summer Salutations!

By B. Scott Fisher

Welcome to our Summer 2019 edition of *New Coordinates*. I hope you are having a terrific summer and managing the record heatwave. Travelers to France and Italy have seen some of the most elevated temperatures in history. Can you imagine what the Tour de France cyclists experienced? I made it to Newfoundland and Nova Scotia, and the break from the heat was most welcome. Average daily temperatures ranged from the low 50s to low 70s. Great hiking weather and stunning scenery. I recommend it.

As summer winds down, we all transition to planning for 2020. So Treliant has lined up some forward-looking perspectives in this edition. My colleagues touch on a number of challenges that financial services companies face today in managing regulatory change, building the case for risk and compliance programs, de-risking innovation, and protecting consumer privacy. I hope you find it all thought provoking.

Autumn Headwinds Surrounding NIM

Before the summer, I spent some time talking with financial services leaders across the country. A common concern I heard was how the changing interest rate environment would impact Net Interest Margin (NIM). This is putting financial executives in a tough situation. Most of them are wearing a lot of hats, weighing strategic choices for investment, and now battling NIM headwinds.

(continued on next page)

B. Scott Fisher
Chief Executive Officer
Treliant

Just as a reminder, NIM is the all-important delta between what banks pay on customers' deposits and, in turn, charge for extending credit. As the Federal Reserve eases rates in the back half of 2019, earnings forecasts for 2020 are already projecting risks associated with tighter margins.

The war for gathering and retaining low-cost deposits while finding attractive credit opportunities will wage on. Surgical pricing will be essential, from a profitability perspective. But from a compliance perspective, bankers must remember to maintain consistency to avoid UDAAP or Fair and Responsible banking issues. Their pricing activities are closely watched by a myriad of regulatory agencies.

The Diversification of Outsourcing

A second theme I heard was around the topic of outsourcing services versus hiring permanent staff. Outsourcing or leveraging contractual labor offers both appeal and risk. The appeal is that the expense is viewed as variable, with the ability to suspend on short notice. The risk is that the third-party relationship must be monitored to ensure alignment with all stakeholders.

We are seeing a rise in managed services activity including:

- **Secondments.** This is typically in higher-level roles where an external search is occurring. A six- to nine-month bridge can allow proper time to onboard a new hire, while continuing "business as usual." Risk functions are particularly scrutinized by regulatory examiners to ensure that there is continuity. We also see companies hire a secondment to serve as an onboarding coach to a newly hired senior officer. It is not a given that a chief executive officer has the background to appropriately coach that individual on the requirements of the role. Coaching is an effective way to ensure a successful transition and ramp up.
- **Interim resource surges.** People are often requested two to 10 at a time. These spurts tend to be project-related and can carry a wide range of durations. In some cases, companies lack subject matter expertise and supplement staff this way. In other case, companies simply lack internal bandwidth and need this incremental support to move through a project or business need.
- **Large-scale projects.** These require 50 to 100 resources to handle repetitive tasks such as lookbacks, quality control, or transaction monitoring. There may be a sponsor at the company who provides guidance and oversight, or the project can be viewed as independent monitoring.
- **Outsourcing a function altogether.** This is often called for when geography might limit a company's ability to source permanent talent.
- **Joint marketing agreements.** These can be viewed as a means to offer clients products in a "white label strategy."

(continued on next page)

(CONTINUED)

Summer Salutations!

As you can see, leveraging external resources to assist with business objectives can happen in a variety of ways. The key is to ensure you align yourself with a reputable firm that has "skin in the game" with your company. This is something we do frequently at Treliant for our clients. We are happy to have a conversation if you are considering such a strategy.

Meanwhile, enjoy our newsletter.

B. Scott Fisher

B. Scott Fisher, Chief Executive Officer, is a senior financial services executive with a 32-year career in banking, including responsibility for mortgage, retail banking, consumer credit, product management, brokerage, private banking, commercial banking, network planning, e-commerce, call centers, and operations. sfisher@treliant.com

Financial Crimes Compliance Officers and the Age of Change

By Ross Marrazzo

Ross Marrazzo
Managing Partner
Treliant

A recent conversation drove home for me (yet again) the precarious nature of work in Financial Crimes Compliance (FCC) in this age of constant change. The problem is only getting worse, and we all need a better understanding of the bank risks that can go unchecked when the FCC role is undervalued and underfunded.

The takeaway from my discussion with a former FCC officer was compelling. "Why would I stay in a field with so much personal risk?" he asked. His point of view is certainly understandable—yet more concerning than ever as financial crime escalates, technology accelerates, and regulatory uncertainty persists.

Compliance officers have long faced objections to spending money on their (and therefore, their company's) needs to build and maintain an effective, sustainable compliance program. Even in companies that have gone through the nightmare of an enforcement action, executive management and boards soon forget what got them into the mess in the first place. Short-term memory kicks in, and they revert to old ways as if nothing happened. That's often the point at which expense management under the auspices of gaining efficiencies is replaced by blind cost cutting. It's the moment when new managers are brought in to decimate the very enhancements required by the enforcement action or to maintain an effective compliance program—or current managers are saddled with eliminating the staff and tools required for long-term sustainability.

(continued on next page)

Now Is Not the Time to Cut Corners

Not since the adoption of the U.S. Bank Secrecy Act (BSA) and USA PATRIOT Act have so many changes to the financial crimes risk management environment been in play, such as:

- Interagency statements late last year in which U.S. regulators encouraged banks to develop more effective and efficient FCC tools—and allowed banks to share resources where appropriate;[1]
- U.S. Congress's consideration of changes to the BSA;[2] and
- Introduction of new regulatory technology (RegTech)—in particular, artificial intelligence (AI) as a method to gain efficiencies and be more effective.

These recent moves are targeting methods for the industry to leverage itself for greater efficiencies, thereby reducing regulatory burden. But they should not be misread by executive management and boards to mean that compliance departments will require less funding for staff or tools to manage and mitigate risk.

For example, it may make sense for smaller institutions to work together on processes such as FCC training to reduce their costs, as suggested by regulators. However, more challenging to cross-leverage may be Financial Intelligence Unit activities.

Meanwhile, in Congress, you might think the changes under consideration are going to cut FCC compliance program requirements. But this probably won't be the case, since lawmakers are astute enough to know that any changes cannot be allowed to reduce the effectiveness of U.S. law but should rather modernize it to make it more efficient and effective for today's risks. And those risk considerations are clearly much more focused on terrorist financing and human trafficking.

And then there's RegTech. Machine learning and AI are being held out as lifesavers and the ultimate cost reducers. However, AI has not yet been perfected. And while the experts seem to believe it will deliver greater efficiencies and effectiveness, this does not automatically translate into a reduction in staff.

All this may be from a U.S. perspective but this is not to say that FCC officer challenges are unique to U.S. financial institutions or foreign bank offices in the U.S. The regulatory environment across the globe carries similar expectations for effective compliance programs with FCC compliance officers in the cross-hairs. Personal liability is a constant risk no matter where you are located.

Making the Case for Compliance

Compliance officers often face tough arguments against hiring. Their rebuttal should be just as strong. They need to make sure their executive management and board are

(continued on next page)

Personal liability is a constant risk no matter where you are located.

There are no silver bullets in this broad and changing regulatory, legislative, and RegTech environment.

well-informed of the financial crimes risk management expectations and the tools that are available for gaining efficiencies while maintaining effectiveness. But there are no silver bullets in this broad and changing regulatory, legislative, and RegTech environment—something company leaders need to know. Driving home this point will allow compliance officers to direct the discussion about the environment, while keeping a finger on the pulse of executive management and the board to forestall any considerations of material reductions to funding an effective compliance program.

Compliance officers should routinely report their department activities through metrics, no differently than sales executives report sales. This will provide inarguable support for "Big C" and "Little c" compliance needs, with Big C being the Compliance function and Little c being those areas that own compliance risk, like first line of defense functions. A + B = C metrics are extremely compelling and difficult to challenge.

At the same time, compliance officers should constantly reassess their department from a staffing and structure perspective, and be prepared to offer up reasonable reductions when needed—but only if they can live with them. To live with reductions means that there are stopgap processes available to ensure that no critical processes or controls are compromised.

Ross Marrazzo

Ross Marrazzo, Managing Partner and Service Area Executive, has over 33 years of domestic and international experience in the design, oversight, and assessment of corporate and regulatory compliance, Anti-Money Laundering (AML)/ Bank Secrecy Act (BSA), sanctions and fraud programs, and internal controls. Ross possesses a thorough knowledge of executive and operating functions and responsibilities within public companies and the financial services industry, including consumer and commercial banking, investment banking, insurance, and wealth management. rmarrazzo@treliant.com

[1] https://www.fincen.gov/sites/default/files/2018-12/Joint%20Statement%20on%20Innovation%20Statement%20%28Final%2011-30-18%29.pdf and https://www.fincen.gov/news/news-releases/interagency-statement-sharing-bank-secrecy-act-resources

[2] https://financialservices.house.gov/uploadedfiles/hhrg-116-ba10-20190313-sd002_-_memo.pdf

Managing Compliance Risk in an Era of Innovation

By Mark Westmoreland

Mark Westmoreland
Managing Director
Treliant

The modern economy is built on innovation and technology. The internet and smartphones have enabled an era of innovation that scales faster than anything in human history. But this ever-accelerating pace of change is creating its own risk, and we're watching that risk play out in real time. Tech companies, especially social media companies, are now facing an unprecedented backlash from the U.S. Congress, Justice Department, Federal Trade Commission, and even more from overseas governments. Comprehensive privacy legislation is already in place in Europe, with similar legislation being contemplated in Washington. And the backlash could intensify for tech companies—calls for breaking up certain companies or requiring divestitures are now being voiced by both Republicans and Democrats.

All this turmoil illustrates the real and potential costs of mismanaging risk in an innovation environment. Compliance or legal professionals working in FinTech should be especially vigilant as federal and state regulators are finally starting to scrutinize the risks of Silicon Valley's long-uttered mantra, "Move fast and break things." When it comes to banking, federal regulators have more experience and sophistication in assessing these risks than Congress. And they have long institutional memories.

What should FinTechs and banks do now? My career in the FinTech ecosystem and bank product testing environments has surfaced three key challenges, outlined below along with practical solutions. As head of Treliant's FinTech practice, I've had the opportunity to work with dozens of FinTech companies over the past nine years. But my truly immersive

(continued on next page)

experience in this space was formed by working for two FinTechs earlier in my career—plus a large bank "innovation lab," or rapid-cycle testing unit, back before there was social media or smartphones. All these environments were focused on the same activity: rapidly developing and deploying new products or services, testing the results, and then adjusting and evolving.

Outsiders have invigorated banking with a host of new products and innovations.

As we watch the headlines play out for tech and social media companies, it's easy to see that FinTechs face many of the same challenges, but with a banking twist. Consider these three:

Challenge #1: The Business is Unfamiliar with Banking Laws

It's common to find a subset of businesspeople at FinTech companies who are not familiar with all the laws and regulations that apply to their products. This isn't intended as a criticism. Quite the opposite. Banking was due for a transformation, and outsiders have invigorated banking with a host of new products and innovations that benefit consumers, many of whom have been shut out of traditional banking. Even so, the situation does present a challenge. While senior executives at most FinTechs have extensive banking experience and subject matter expertise, that experience is not as common to find on some project teams or those tasked with day-to-day execution.

Solution: The solution is common sense and it's widely known: training. The conventional approach to training is to put your employees through the alphabet soup of online training modules for everything from Regulation B to Regulation Z, followed by a quiz at the end. This can be effective at building general awareness and is definitely required by regulators, so checking off this box is important. However, in an innovation environment where products or processes are being developed at the bleeding edge of banking, it can be a challenge for employees to connect the dots from a statement about Federal Credit Reporting Act prohibitions in a training module, for example, to their day-to-day job. The solution to this challenge is two-fold:

- **Real-time Training:** This informal approach looks for teachable moments as they happen in the workday. It is sometimes difficult to come up with examples and scenarios to use in annual regulatory training modules, but you're likely to encounter new situations every day or week that merit pausing with businesspeople and reinforcing key themes from the annual training. Real-time training like this tends to resonate and stick.

(continued on next page)

- **Targeted, Recurring Training:** This is a more formal approach that develops short, targeted training sessions of perhaps 30 minutes or less using recent, real-world examples to discuss with the team. These can be scheduled monthly or even weekly if there is a new product or service launching.

Challenge #2: The Pace of Innovation

The proliferation of technology tools and data sets means more innovation at a much faster pace than ever before, and compliance and legal professionals are challenged to keep up.

Solution: Documentation is key to keeping pace. It may seem counterintuitive and out of fashion, in a world that is currently enamored with "agile" project management—where suggesting that you write things down will get you a torrent of frowny face emojis from your business partners. But remember that agile was created for software development. Agile is actually the anti-project management approach to rapid-cycle testing. It may work well in many environments, but there are laws and regulations in banking that require certain information to be documented and retained. As a result, federal and state regulators will expect to see these documents, too.

Yes, taking time to document product development can slow things down a bit, but there's a synergistic value to the business that's often ignored. A key point of launching new products is to test and learn what works. A record of how a product was developed, deployed, and received in the market captures the foundational elements to analyze whether the product is successful and works as intended. Important insights like this are gleaned from documentation and really represent the whole point of launching a test in the first place: to learn. Learning is how a business improves over time, which creates shareholder value, and everyone can agree on that.

Challenge #3: Accuracy and Usability of Data

Social media and smartphones have created a supernova explosion of new data types and sources that marketers and model builders in the FinTech space have rushed to use. But not all of it is legally usable for its most valuable purpose—or at all. Unlike mining data to sell sneakers or luggage or any other consumer product, there are long-standing laws and regulations that limit what data can be used to market or make decisions on financial products.

Solution: We'll revisit this topic in a future article, but solutions start with answering and documenting the following questions:

- What is the source of this data?
- What are all the uses of the data (marketing vs. decision-making vs. model building, etc.)?
- What variable or variables will be used?
- Where will the data be housed/protected?
- Who will have access to the data and for what purposes?

(continued on next page)

The Fair Credit Reporting Act, Regulation B, and other rules require documentation of this kind of information regarding data usage. Having a program in place to document and track such questions and answers is crucial to a safe and sound program.

The Final Analysis

The new era of innovation is running at full steam through almost every industry, including banking. Compliance professionals want to enable this transformation while still satisfying federal and state regulators because they know, as recent headlines show, that regulators, politicians, and the public all care deeply about core issues of privacy and fairness. Finding a sustainable path through this cycle of innovation is something everyone wants.

Mark Westmoreland

Mark Westmoreland is a Managing Director and head of Treliant's Corporate & Regulatory Compliance service area. He is an attorney and experienced regulatory compliance executive who has led large consulting projects for several Top 10 banks and numerous FinTechs. He previously served as in-house counsel at Capital One Bank and JPMorgan Chase Bank, where he developed expertise in credit cards, student loans, and closed-end installment loans, including deep subject matter expertise in the Fair Credit Reporting Act and fair lending data usage and governance. mwestmoreland@treliant.com

Insurtech: Managing Risks to Consumer Privacy, Information Security, and Fairness

By Lynn Woosley, Max B. Sherman, and Princeton W.G. Graham

As the insurance industry continues to undergo a profound digital transformation, three main drivers are telematics in auto insurance, "connected health" apps in health insurance, and alternative data in all insurance sectors. Each of these innovations in insurance technology, or insurtech, presents potential benefits and risks to both consumers and providers.

Among the benefits, new technologies and data sources can increase consumer access to insurance, expand choice and convenience, improve pricing, and better inform decision-making. For insurance companies, new technologies and data may also result in more accurate underwriting and pricing, enhanced product offerings and customer experiences, and improved fraud detection.

However, insurtech risks include privacy violations, data breaches, and the fallibility of alternative data, as new risks emerge regarding information security, data accuracy, consumer fairness, and other essentials. This article elaborates the risks and recommends steps to manage them.

Insurtech Overview

Auto insurers have access to an increasing volume of information collected by telematics, which merges telecommunications with information processing to remotely monitor location, condition, and other data related to individual automobiles. In practice, a policyholder either inserts a telematic device into a car's onboard diagnostic port, accessing the vehicle's computer, or installs a telematics app on a smart phone.

(continued on next page)

Lynn W. Woosley
Senior Director
Treliant

Max B. Sherman
Senior Analyst
Treliant

Princeton W.G. Graham
Senior Analyst
Treliant

Connected health apps have been found in recent studies to present numerous privacy issues.

Data available via the diagnostic port could include location, date and time of vehicle use, driving time and distance, air bag deployment, instances of hard braking or cornering, acceleration rates, lane stability, activation of the vehicle collision warning or automatic emergency braking systems, and road conditions. App-based telematics could gather driving speed, distance, location, acceleration, and braking, as well as instances of distracted driving, such as calls, texts, or other apps used while in motion.

By linking data gathered from the telematics device with GPS and time data from the car or phone, the insurer can determine whether the consumer is:

- Speeding, by comparing vehicle speed to the posted speed limit;
- Rolling through stop signs, by using vehicle location and speed combined with stop sign locations on route maps;
- Traveling to, or parking in, areas with greater incidence of accidents or vehicle theft, by matching location data with geographic statistics; and
- Driving in a fashion consistent with the vehicle use stated in an individual's insurance application, by tracking whether the car is in use during the day or night, miles driven, and destinations.

For health insurers, there are applications, often called "connected health apps," that track almost every aspect of a user's health and lifestyle, including exercise, diet, weight loss, blood glucose, pregnancy, stress, sleep, smoking, and menopause, just to name a few. Some apps let users research symptoms and find doctors or medical specialists.

And across all insurance sectors, insurers are now mining new alternative data sources when issuing and pricing policies. Digital payment platforms, mobile wallets, social media networks, travel, daily activity levels, neighborhood health and safety patterns, "real world" credentials such as college degrees and professional accreditations—these and other sources are increasingly explored for their usefulness in establishing insurability beyond driving records, medical histories, credit bureau scores, and other more traditional inputs.

Privacy

A review of privacy policies for a number of commercial health, auto, and property insurance apps found in the Apple App Store or the Android Store on Google Play indicates that most are using tracking technologies. These may include cookies, beacons, tags, scripts, and location data, as well as collecting and transmitting log files including IP addresses, device type, browser type, internet service provider, clickstream data, date and time stamps, pixel tracking, and HTML5 Local Storage Objects. Many also capture information about web browsing history, even when transactions are within the app.

Auto insurance apps usually collect driver's license information and vehicle identification numbers and contain driving histories. Insurance apps often ask for access to a user's

(continued on next page)

device camera to take pictures of insured items for coverage or claim purposes. For apps with in-app payment capabilities, bank account or payment card information may also be stored. Even without in-app payments, some insurance apps collaborate with third parties to gather banking data about app users.

Connected health apps have been found in recent studies to present numerous privacy issues, including excessive mobile device permissions and undisclosed data collection, such as email addresses, phone numbers, photos, and locations.[1] It is unclear whether health apps offered by insurance companies or employers have the same issues as those offered by technology and wellness companies, but it is clear that such apps collect a variety of sensitive personal data points. These include ID, policy information, social security number, coverage limits and rates; email, phone number, address, marital status, age, claims, and medical history, including doctors, prescriptions, and diagnoses.

In addition to data collection, data sharing is a key consumer privacy concern. After collecting sensitive data, does the insurer share it? If so, with whom? The studies of health and wellness apps mentioned above found that the apps were sharing the information collected with social media platforms, advertisers, and, in some cases, pharmaceutical companies and employers. Although there is no evidence that insurance companies are currently sharing this broadly, some health and wellness apps used in employer-sponsored wellness plans do share data with employers. Even though such data is supposed to be anonymized under the Affordable Care Act (ACA), in practice employee segments may be small enough to reduce anonymity.

Some auto insurers have reserved the right to share telematics data in the future. A review of a sample of iOS and Android insurance app privacy policies indicates that insurance company apps frequently share data with marketing partners, affiliates, and analytics or service providers, as well as state insurance departments. Some apps noted they also shared information with unaffiliated insurance companies, reinsurance companies, insurance agents, third-party claims administrators, consumer reporting agencies, and financial institutions. Our review of insurance app privacy policies revealed that insurtech-related companies are also using social media and large tech firms for analytics.

Information Security

In the studies referenced above, testers found unencrypted transmission of data to third parties, including sensitive health information, passwords, and consumer contact information. Several health and wellness apps made unencrypted requests for HTML content or unencrypted or plaintext requests to servers in a fashion that would permit "man in the middle" code injection, data leakage, and cyberattacks. Others sent unencrypted user authentication cookies, offering opportunities for account takeover.

A review of the consumer disclosures of several insurance apps showed that many insurance app providers disclose very limited information regarding their data security

(continued on next page)

After collecting sensitive data, does the insurer share it? If so, with whom?

practices, making it difficult for consumers to understand potential information security risks. None provided details regarding how their apps store and transmit consumer information. As data hacks proliferate, the need increases for robust encryption and other methods of obscuring personally identifiable information (PII)—on the device, during transmission, and in the cloud or physical storage of the app owner—to ensure that opportunities for malicious actors are minimized.

Data Accuracy and Reliability

Two risks associated with some insurtech and alternative data are accuracy and reliability. Insurers should incorporate robust data cleaning routines and consider the impact of noisy or inaccurate data.

Consider phone-based telematics, for example. Sensor data from a smartphone's gyroscope, compass, and GPS systems is notoriously noisy. The app cannot tell if the consumer is the driver, a passenger, or out jogging. The app may not know, especially in some speed ranges, whether the consumer is in a car, a train, or a plane. Health and wellness apps do not know whether the symptoms searched by a user are their own, a family member's, or a topic being researched for some other purpose. In addition, purchased data that is combined with device-collected data may have unknown accuracy, completeness, and reliability, particularly since data providers may not be subject to regulatory oversight.

Consumer Fairness

As insurance firms use more alternative data and telematics, there are increasing consumer fairness risks. Consumers may not understand the impact of alternative data on insurance underwriting and pricing decisions. Whenever there is a lack of transparency or consumer understanding, the risk of unfair trade practices increases.

Inappropriate use of alternative and location data can increase the risk of illegal discrimination in insurance. Just as the use of location data in credit decisions raises redlining risk, the use of telematics in auto insurance quotes could result in insurance redlining based on driving or garaging location.

Several court cases have found that illegal discrimination in availability, coverage, pricing, or claims processing of insurance covering residential real estate violates the Fair Housing Act (FHA). The Department of Housing and Urban Development (HUD) has held that refusing to insure multi-family properties that include "subsidized housing" and "low-income housing" has a discriminatory effect based on race and national origin in violation of the FHA.[2] Although the FHA does not cover auto and health insurance, there are similar prohibitions on illegal discrimination in other laws governing insurance.

Earlier this year, the New York Department of Financial Services (NYDFS) joined the Federal Trade Commission (FTC),[3] General Accounting Office (GAO),[4] and the Open Technology Institute[5] in expressing concerns regarding the use of alternative data in financial services,

(continued on next page)

including underwriting insurance policies. In Insurance Circular Letter #1 (2019),[6] the NYDFS reminded insurers operating in the state of their obligations and risks in using external data in underwriting life insurance. Under New York state law,[7] it is illegal to discriminate in providing insurance because of prohibited criteria, including race, color, creed, national origin, status as a victim of domestic violence, past lawful travel, sexual orientation, or any other protected class. Many data points potentially useful in underwriting life insurance, such as community-level home value, home ownership, mortality, crime, accident, and addiction or smoking data, may be proxies for prohibited criteria.

In addition, some data points collected via health and wellness apps may be proxies for information protected under the Americans with Disabilities Act (ADA) or the Genetic Information Nondiscrimination Act (GINA). For example, histories of searches of certain symptoms or medical conditions could reveal genetic or disability information.

Recommendations for Risk Management

As insurers adopt new data and technologies, they should take these six steps to help manage their consumer protection risks:

1. Insurers should be transparent with consumers regarding the information they collect, how they use that information, and whether and how they share that information.
2. Insurers should adopt strong cybersecurity measures, including elimination of unencrypted or plaintext collection, transmission, and sharing of potentially sensitive data.
3. Permit consumers to opt out of third-party and affiliate sharing, with ease.
4. Insurers should consider fairness broadly in their use of emerging data sources and technologies. Evaluate whether the adoption of new technology would result in unfair trade practices or unfair claim settlement practices. Where appropriate for a particular insurance product, consider the effect on compliance with the FHA, ADA, GINA, and state laws prohibiting discrimination.
5. Before using alternative data, insurers should evaluate the relationship of the data to risk. In insurance underwriting or rating, insurers should evaluate whether the data and its usage is supported by generally accepted actuarial principles and consistent with claims experience.
6. Finally, insurers should assess whether there is a valid rationale for differential treatment of otherwise similarly situated consumers based on the alternative data.

Insurtech offers the promise of increased access to insurance, expanded consumer choice, and more accurate underwriting and pricing. To achieve these promises without consumer harm, insurers must manage the consumer protection risks of new technologies and data.

Rebecca (Lynn) Woosley, CRCM

Lynn Woosley, Senior Director, has extensive senior executive experience in regulatory compliance, consumer and commercial credit risk, credit and compliance risk modeling, model governance,

regulatory change management, acquisition due diligence, and operational risk. Over the last two decades, Lynn has held leadership positions within the enterprise risk management division of a Top 10 bank. She has also served as Senior Examiner and Economist at the Federal Reserve Bank of Atlanta. lwoosley@treliant.com

Max B. Sherman

Max Sherman, Senior Analyst, is experienced in fair lending, Anti-Money Laundering (AML), internal audit, and regulatory exam preparation. He has managed compliance and risk management projects for institutions of all sizes, from start-ups to systemically important financial institutions. msherman@treliant.com

Princeton W.G. Graham

Princeton Graham, Senior Analyst, has experience in FinTech compliance, operational and third-party risk, and fair and responsible banking. At Treliant, he has built compliance monitoring and testing infrastructures, conducted small business fair lending and competitive pricing analyses, and performed large-scale mortgage origination and servicing reviews. pgraham@treliant.com

---

[1] See, for example, https://www.wsj.com/articles/popular-apps-cease-sharing-data-with-facebook-11551044791, https://hbr.org/2017/01/workplace-wellness-programs-could-be-putting-your-health-data-at-risk, https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8272037, and https://www.eff.org/wp/pregnancy-panopticon.

[2] See, for example, https://www.hud.gov/sites/documents/17CONCILFIREINSURANCE.PDF, https://www.hud.gov/sites/documents/17MACKCONCIL.PDF and https://www.hud.gov/sites/documents/17MCGOWANCONCIL.PDF.

[3] https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf

[4] https://www.gao.gov/assets/700/690803.pdf

[5] https://www.ftc.gov/system/files/documents/public_comments/2014/10/00078-92938.pdf

[6] https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2019_01

[7] Including, but not limited to Insurance Law Articles 26 and 42, Insurance Law §§4224. Executive Law, and General Business Law.

Announcing

Treliant's New Corporate & Regulatory Investigations Service Area

Treliant's Corporate & Regulatory Investigations practice provides forensic accounting, data analytics, and expert witness services in investigations before the Securities and Exchange Commission (SEC), Department of Justice (DOJ), Financial Industry Regulatory Authority (FINRA), and other government agencies. Our service offerings include:

Corporate Investigations

Treliant has deep experience working closely with law firms and general counsel to assist clients in management-led internal investigations and independent audit-committee investigations in regulatory matters. The services we provide include:

- Forensic accounting, including risk-based judgmental sampling and analysis of underlying records and supporting documentation related to specific accounting transactions
- Forensic technology, including data analytics and discovery management
- Supporting counsel in interviews of accounting, finance, and audit personnel
- Reporting on investigation findings and recommended remedial measures, where appropriate
- Assisting counsel with presentations to the SEC, DOJ, and other government agencies on investigative procedures and factual findings

Regulatory Investigations

Our securities experts provide support to counsel in private securities litigation and in DOJ, SEC, and FINRA investigations involving broker-dealers, investment advisors, hedge funds, and private equity firms. Our services include:

- Internal and Audit Committee Investigations
- Market Manipulation Investigations
- Improper Commingling of Invested Funds
- Sales Practices and Supervisory Investigations
- Regulatory Exam Preparation, Internal Audits, and Mock Examination Services
- Remediation of Compliance Program and Internal Control Deficiencies

Pam Parizek, a Treliant Managing Director in the Washington, DC office, specializes in corporate and regulatory investigations. A former Senior Counsel with the U.S. Securities and Exchange Commission's (SEC's) Enforcement Division, she is an advisory leader with over 29 years of experience investigating securities fraud, accounting irregularities, and bribery allegations, as well as advising U.S. and global clients on regulatory compliance.

Executive Leadership

Martin Nesbitt
Chairman

B. Scott Fisher
Chief Executive Officer

Ross Marrazzo
Managing Partner

John P. Carey
Senior Managing Director

Kathryn Reimann
Senior Managing Director

Service Area Leadership

Michael J. Corcione
Managing Director

Ralph Fatigate
Managing Director

Constandino Papagiannis
Managing Director

Pamela J. Parizek
Managing Director

Carl G. Pry
Managing Director

Mark Westmoreland
Managing Director

Lynn Woosley
Senior Director

Senior Advisory Board

Susanna Tisa
Executive Partner

Waldo M. Abbot
Senior Advisory Board Member

Steve Bartlett
Senior Advisory Board Member

Edward B. Kramer
Senior Advisory Board Member

Senior Regulatory Advisors

	Prior Experience
April A. Breslaw	Consumer Financial Protection Bureau, Office of Thrift Supervision
Agnes Bundy Scanlan	Consumer Financial Protection Bureau
Angela Desmond	Federal Reserve, Securities and Exchange Commission
Fred Finke	Office of the Comptroller of the Currency
Chris Sablich	Office of the Comptroller of the Currency

Independent Members of the Board of Directors

John Brennan
Former Director of the Central Intelligence Agency

Colin Dyer
Former CEO, Jones Lang LaSalle

Dmitri Stockton
Former Executive, General Electric and Former Chairman, President, and CEO, General Electric Asset Management

Neal Wolin
Former Secretary of the U.S. Department of Treasury

FOLLOW US!

Treliant

treliant.com