Aptean Respond

A Case & Complaints Management System

Financial Regulatory **Innovation in the US**

How to successfully navigate new compliance challenges in a new era

aptean Ready for What's Next, Now™

Introduction

A decade of global reforms has created a radically new regulatory landscape for the US financial services sector. Technological and socio-economic changes have given rise to a new generation of concerns for regulators, with the issues of data privacy, customer vulnerability and organizational accountability taking center stage. And, with more than $327bn paid in fines by the 20 largest global banks for mis-selling financial products since 2012[1], financial services organizations simply can't afford to put a step wrong.

For the US financial services industry, this shifting landscape has seen the creation of a new set of legal and regulatory challenges. Against a backdrop of increased competition, ever-changing risk, and heightened customer expectations and needs, evidenced by the 44% increase in customer complaints filed by the Consumer Financial Protection Bureau (CFPB) in 2020[2], rising to meet these new challenges can be easier said than done.

With the right systems, processes and procedures in place, regulatory compliance doesn't need to be difficult. What may seem like a void of time-consuming and resource-draining tasks and check-boxes, can actually add value to your business. It can underpin operational best practice and nurture those vital long-term customer relationships, delivering a customer experience that's not only fully compliant but consistently excellent.

---

1 CCP Conduct Costs Project Report 2017

2 Report: Massive Uptick in Consumer Finance Complaints During Coronavirus Pandemic, LendEDU

The Digital Age

The continued growth of digital banking has always been expected, but 2020 expedited that growth, with global events giving rise to the need for socially-distanced money management. In 2019, more than three quarters of Americans[1] used mobile devices to check bank balances and the number of mobile payment transaction users across the globe is predicted to increase from 950 million in 2019 to a staggering 1.31 billion by 2023[2].

The increased digitization of how customers interact with their banks has led to a change in the nature of complaints, as well as an increase in the amount of complaints coming in. This is partly due to the ease with which digital channels enable complaint-making, but also due to the technology itself. For mobile banking apps in particular, almost a third of digital banking customers complain about app problems, with 30% reporting problems just accessing the apps, never mind achieving what they want to when using them[3].

What we're seeing is disconnect between what banks are providing and what some customers are able to use. Banks are rightly trying to adapt their processes and apps to suit the increasingly digital nature of not only banking but society in general, yet customer ability to embrace these new ways of working varies greatly across demographics. Apps that are meant to streamline and simplify processes and procedures are, in some instances, causing far more problems than they're solving and failing to meet ever-increasing customer expectations.

1 Mobile Banking Statistics, DataProt

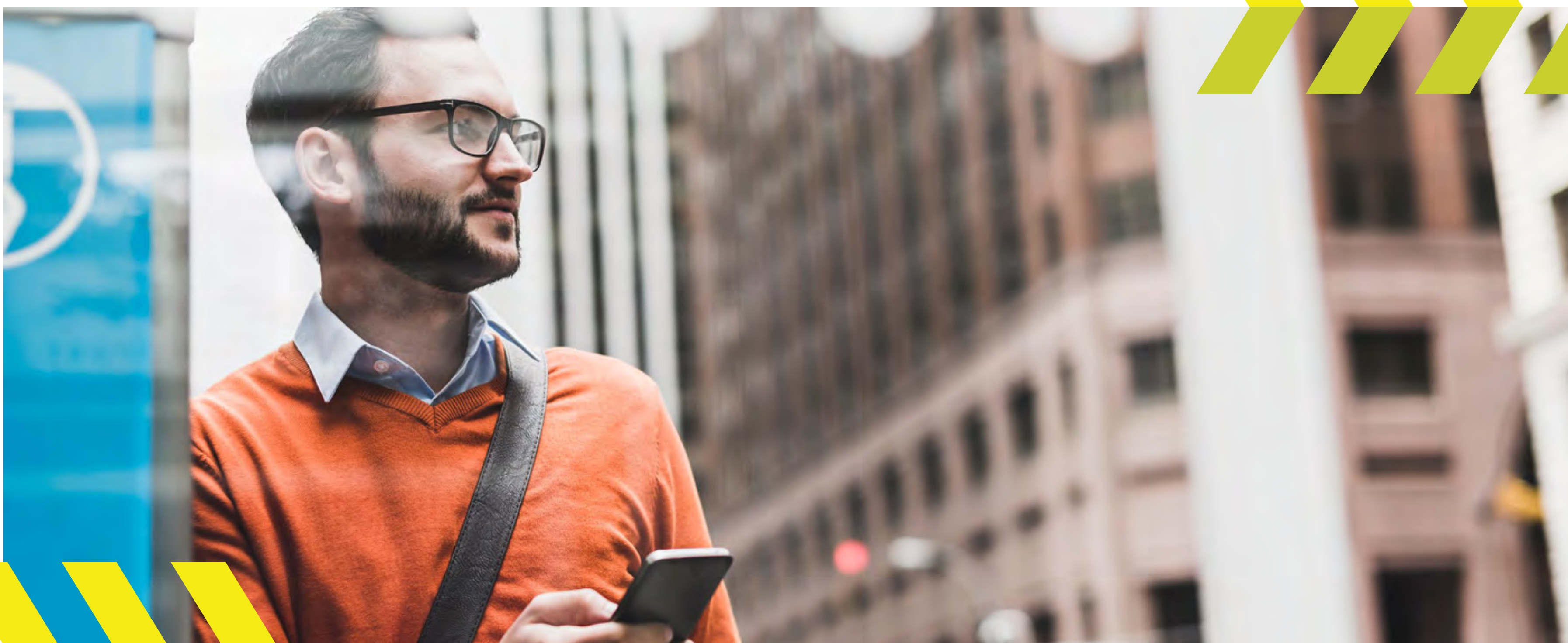
2 Mobile Payments Worldwide, Statista.com

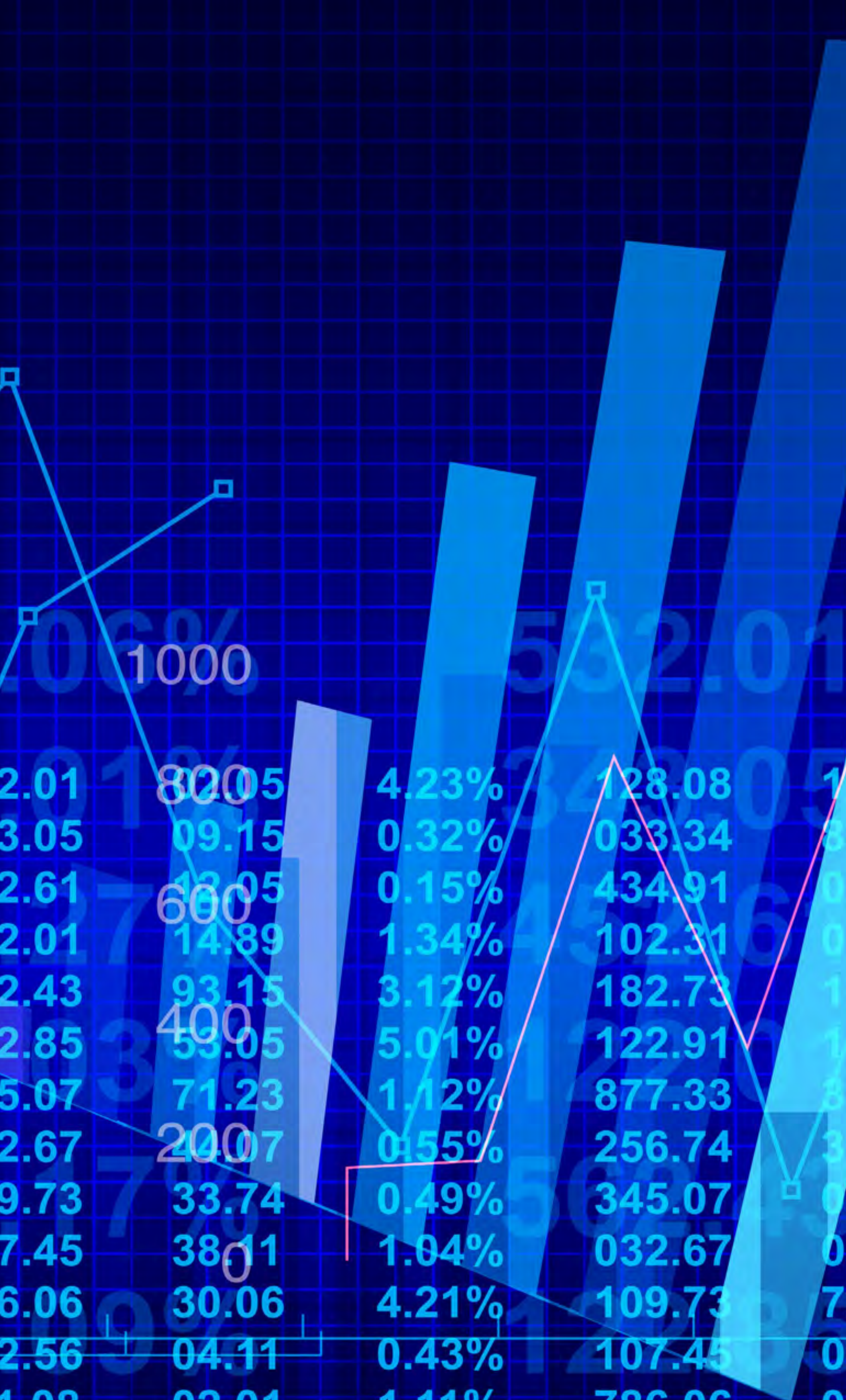
3 Friction Report, Mobiquity

Technology is Key

We're well and truly in the digital age, not only in terms of how businesses need to operate but also how customers expect to interact with their financial services suppliers. Where some older institutions are saddled with slower, less agile legacy systems, many newcomers to the industry have more streamlined, digitally-native processes already in place, giving them an immediate advantage over other more established organizations when it comes to operating in our new digital world.

Recognizing this shift, many financial services firms are investing in technology, accelerating the modernization of financial services systems and taking full advantage of the benefits they can bring, striking the perfect balance between innovation, compliance and managing risk. To build and maintain a competitive advantage, it's crucial that financial services businesses achieve this balance, embracing new business models and ways of working to demonstrate a commitment to ensuring an excellent customer experience while maintaining the highest levels of regulatory compliance.





New Risks to Manage

Whilst focused on driving continuous improvements and taking the necessary steps to mitigate against traditional financial risk, financial services executives are coming under more pressure to manage non-financial risk (NFR) too. Covering such diverse areas as cybersecurity, employee misconduct and customer protection, issues of NFR are quick to hit the headlines and can be extremely damaging to a business's reputation. This warrants a thorough reassessment of risk management priorities, again ensuring the right balance between compliance, customer experience and risk management. The pressure is on to readily identify NFR compliance challenges, putting in place the right skills and enabling technologies to ensure the effective and efficient management of NFR, without adversely affecting the rest of the business.

Compliance doesn't discriminate, and the legal and regulatory requirements placed on financial services organizations are applicable to both financial and non-financial risk, with the voting in of the California Privacy Rights Act (CPRA) evidence of this. Robust compliance management can underpin excellence in both financial and non-financial risk management, ensuring a consistent and effective approach to risk, regardless of the source.

The Current Regulatory Environment

The CCPA

Enforced by California's Attorney General, The California Consumer Privacy Act (CCPA) is a state-wide privacy law that regulates how businesses handle the personal information of California residents. It applies to any company, including financial services organizations, that collects or plays any part in processing this data if:

- They sell the personal information of more than 50,000 Californian residents per annum
- Their gross annual revenue is more than $25 million
- They derive more than 50% of their annual revenue from selling the personal information of California residents

With possible fines of $7,500 per violation and $750 per affected user, it's in a business's interest to ensure CCPA compliance by putting in place the right systems and processes to guarantee best practice and adherence to these far-reaching regulations.

At the heart of the CCPA lies the ability for consumers to exercise three specific rights:

- The Right to Know
- The Right to Delete
- The Right to Opt Out

For financial services organizations in particular, it's crucial to establish the optimum systems and processes to facilitate the effective and auditable management of these rights requests, fulfilling CCPA requirements while meeting obligations to customers too.

The CFPB

Born out of the Dodd Frank Act as part of new efforts to re-regulate financial services markets in the US, The Consumer Financial Protection Bureau (CFPB) is a regulatory agency charged with overseeing financial products and services that are offered to US consumers. One area of its jurisdiction involves examining the complaint resolution processes of financial services businesses, as well as acting as complaints ombudsman, ensuring consistency, fairness and best practice when it comes to complaint management.

Financial institutions have no choice but to comply with the CFPB regulations. And, to avoid incurring fines that can total millions of dollars, they need to put in place the right tools and processes to record every complaint that's received, as well as categorizing and actively addressing each complaint.

The FDIC

Of particular relevance for insurance firms, The Federal Deposit Insurance Corporation (FDIC) is an independent agency created by Congress to maintain stability and public confidence in the USA's financial system. Its primary roles include insuring deposits, examining and supervising financial institutions for safety, soundness, and consumer protection; making large and complex financial institutions resolvable, and managing receiverships.

As part of the FDIC examinations, organizations need to have business plans in place for training, policies and procedures, monitoring and consumer complaint response. Financial institutions must show how they're handling complaints promptly, with defined procedures in place which specify how employees should respond to consumer complaints to expedite quality resolutions. In light of this, more firms are turning to dedicated complaints management systems to better manage complaints and provide the levels of transparency and auditability required to satisfy stringent FDIC regulations.

What's Next?

The California Privacy Rights Act (CPRA)

The California Privacy Rights Act (CPRA), or Prop 24 as it's also known, was passed in California's ballot on November 3, 2020. Designed to clarify certain areas of the California Consumer Privacy Act (CCPA), it creates additional privacy rights for Californian consumers along with placing obligations on certain businesses, extending the reach of the CCPA, expanding the breadth and depth of access and deletion rights that are currently in place.

Due to come into effect on January 1 2023, it's set to be enforced by a first-of-its-kind enforcement agency, the California Privacy Protection Agency (CPPA) as of July 1 that same year. The Agency will also be responsible for building public awareness of privacy risks, while providing businesses and consumers with guidance on privacy.

The biggest change is the newly-defined 'sensitive personal information' (SPI) data category and regulatory guidance on how to limit its use and disclosure. SPI includes such details as Social Security numbers, account login credentials, financial account information, and data regarding sexual orientation, and puts further restrictions on how businesses deal with this information. The CPRA also brings in higher fines for violations involving children's data, as well as codifying Fair Information Practice Principles (FIPPs) regarding data quality, data minimization, security safeguards and use limitation.

Crucially, the act puts in placer a higher threshold for applicability. To qualify as a business that's subject to the CPRA, you must collect or deal with information from over 100,000 households or consumers, up from the 50,000 stipulated by the CCPA.

As California continues to lead the US conversation on data privacy, businesses across the nation would be wise to develop the right strategies and systems to keep pace with the ever-evolving data privacy landscape, ready to achieve robust regulatory compliance when necessary. At the same time, this demonstrates a real commitment to safeguarding customer data, helping to nurture and sustain increasingly important long-term customer relationships.

Lessons To Learn From The Global Complaints Landscape

In light of the CCPA and the CPRA, it's almost inevitable that the US will soon see more states getting on board the data privacy train, with some even discussing the potential introduction of federal regulations. With a view to getting prepared, US financial services businesses can learn a great deal from the GDPR experiences of their European counterparts.

Since coming into force in 2018, the General Data Protection Regulation, to give GDPR its full name, has proved to be a significant challenge for businesses. In particular, organizations must ensure the compliant management of eight rights requests, putting in place the right processes and procedures to coordinate how these requests are managed, fulfilling data obligations to customers without unnecessary delay.

Increasing numbers of businesses have turned to technology to solve their GDPR issues, establishing the optimum systems and processes to facilitate the effective management of multiple rights requests. They're making full use of their GDPR data to capture unique insights into customer interactions, turning this data into valuable insight to inform and evolve data and privacy processes, providing organizations with the potential to better manage future requests.

At the same time, this demonstrates a real commitment to safeguarding customer data, helping to nurture and sustain important long-term customer relationships through a consistently excellent customer experience.

With this in mind, what can businesses in the US learn from the experiences of their peers when it comes to data protection compliance?

- **Regulators aren't afraid to use their powers.** Don't be fooled into thinking regulators will only target larger businesses. The rules apply to all.
- **It's not just about the fine.** The consequences of non-compliance aren't just financial. More customers are aware of their rights when it comes to data protection and security and, regardless of fines, reputational damage can be much harder to overcome.
- **Compliance isn't a one-time thing.** Compliance is a moveable feast, one that continues to evolve. Tools and processes need to be robust enough to ensure compliance, but flexible and scalable enough to adapt in-line with changing needs.
- **It's not just an IT problem**. Key stakeholders and everyone who's going to come into contact with customer data need to be educated and sufficiently trained to uphold the required compliance standards. Joined-up, collaborative working between teams, departments and business functions is a must.
- **Technology is your friend.** It's almost impossible to achieve robust compliance without technology to help. The right systems can manage all customer data within the relevant compliance framework, with checks and balances in place to ensure breeches don't occur.
- **Proof of compliance.** Your systems should facilitate comprehensive reporting and auditability, providing in-depth visibility into your compliance processes and supplying the evidence needed to demonstrate robust compliance.
- **Use it as a business differentiator.** As consumer awareness and knowledge of data privacy increases, so will the expectation that firms will do all they can to help. Compliance can soon become a driver of best practice and a key business differentiator in an increasingly competitive marketplace.

How can Aptean Respond help?

Aptean Respond, a complaint management system, furnishes your business with the depth and breadth of functionality required to ensure the highest standards of legal and regulatory compliance. With regulatory-specific capabilities built-in, including report formats, task management, workflow management and vulnerability detection, it gives you the ability to adapt quickly in response to changing regulations.

By putting in place the right combination of processes, workflows and controls, tailored to suit the particular needs of the financial services sector, Respond provides the ways and means to achieve full compliance. It allows you to strike the perfect balance between compliance, customer service and risk management, adding real value to your business and using robust, compliant best practice as the foundation for an enhanced customer experience.

- Industry-specific templates and tools
- Full auditability to demonstrate robust compliance
- In-depth reporting functionality
- Comprehensive visibility across entire customer journey
- Stay up-to-date with the latest regulatory and legal requirements

Are you Ready to **Learn More?**

Interested to learn how Aptean Respond can help you better manage your complaints?

Contact us at **info@aptean.com** or visit **www.aptean.com**.

aptean Ready for What's Next, Now™

Aptean provides very specific industries with very specific ERP, supply chain management, and customer experience solutions. In today's fast-paced, highly competitive economy, organizations don't have time to waste forcing homegrown software, spreadsheets, and one-size-fits-all solutions to do things they were never designed to do. Aptean is on a mission to end those workarounds – with industry-specific solutions instead of generic software, expert support instead of making you go it alone, and a steady influx of new ideas instead of the status quo.

For more information, visit **www.aptean.com.**