Insights

Winter 2022

Wolters Kluwer

About Wolters Kluwer Governance, Risk & Compliance
Governance, Risk & Compliance is a division of Wolters Kluwer, which provides legal and banking professionals with solutions to help ensure compliance with ever-changing regulatory and legal obligations, manage risk, increase efficiency and produce better business outcomes. GRC offers a portfolio of technology-enabled expert services and solutions focused on legal entity compliance, legal operations management, banking product compliance and banking regulatory compliance.

Wolters Kluwer (AEX: WKL) is a global leader in information services and solutions for professionals in the health, tax and accounting, risk and compliance, finance, and legal sectors. Wolters Kluwer reported 2021 annual revenues of €4.8 billion. The company, headquartered in Alphen aan den Rijn, the Netherlands, serves customers in over 180 countries, maintains operations in over 40 countries and employs 19,800 people worldwide.

In this issue

Adapt. Transform. Thrive.

Our industry is emerging from an intense period of disruption. Despite obstacles such as those presented by the pandemic, economic turmoil, and intense regulatory change, like you, we delivered on our steadfast commitments to serve our customers through ingenuity, grit, agility, and dedication. In short, we lived the mantra, "Adapt. Transform. Thrive." Now is the time to collectively acknowledge these efforts and successes. On behalf of Wolters Kluwer, I want to take this moment to say thank you.

As we turn the page to a new chapter, we want to help your institution capitalize on the momentum generated over the past few years. We are keenly aware of the transformations some of our customers made because we were invited to be part of those journeys by providing products and expertise that enable financial services professionals to solve problems and make things happen for their customers. And for banks on the digital transformation journey, our team of experts, some of whom participated in the first digital loan created on our platform over 20 years ago, can guide your institution through the fundamentals of storing, securing, and confirming the certainty of your digital lending assets.

Right now, your future is our focus. We will measure our success by how prepared the professionals we serve are to comply with new regulations, adapt to new and grander ways to serve clients, and achieve operational efficiencies through the use of purpose-built technologies. Preparing for the future means taking time to plan, reinvent processes, and optimize the allocation of scarce resources.

This booklet contains a selection of recent articles and whitepapers written by Wolters Kluwer regulatory compliance experts. We hope you can find a few minutes to read and reflect on these pieces, which cover a variety of topics of significant interest to compliance and risk management professionals, ranging from the digital lending transformation underway, to the significant proposed changes to the Community Reinvestment Act regulations, to the rising role of RegTech in managing federal and state regulatory demands. You can be confident that Wolters Kluwer will be there to support you as you prepare for whatever might be next. We value our relationship as a trusted business partner, and we remain committed to helping you make an impact for consumers and businesses in your local communities.

Thanks,
Steve Meirink

Steve Meirink
Executive Vice President
and General Manager
Wolters Kluwer *Compliance Solutions*

[Connect with Steve on LinkedIn]

Reg Change and Bob Dylan:
You Don't Need a Weatherman to Know Which Way the Wind Blows

As published in ABA Bank Compliance Magazine | By **Elaine Duffus**

As a compliance professional of a certain age, this familiar line from Bob Dylan's hit song, *Subterranean Homesick Blues*, really speaks to me about where we are inexorably headed when it comes to Compliance Program Management ("CPM") in general, and Regulatory Change Management ("RCM") in particular, within the financial services industry. First, an interesting personal tidbit about that song. I can recite every verse—but I have trouble recalling what I had for breakfast this morning. Be that as it may, here is the connection. You have seen and heard in publications, speeches, and actions by banking industry regulators that financial institutions are expected to mature their CPM processes using artificial intelligence and automation, especially as they grow in size and scope.

That is where the wind is blowing. And emerging risks related to Environmental, Social and Governance (ESG) issues, the digitalization of everything, cryptocurrencies, third-party oversight, and others beg the question of whether your compliance staff will be able to keep your institution up-to-date with all that may apply to your products, services, locations, and customers.

For example, a financial institution is no longer going to be easily forgiven for spending lavishly on improvements to customer-facing apps while their compliance department relies on using spreadsheets, free apps, and emails to ensure the institution is properly protecting those same customers and the institution itself.

But where to focus first? In my experience, RCM. Identifying and maintaining a library of laws, rules, regulations, standards, guidance, and internal obligations that apply to your business model is of primary importance. Why? Because all the other elements of your Compliance Program should be mapped to and driven by them. If you have made those critical connections, when a reg change event occurs, you will know immediately where and how it might affect your institution.

The goal then, especially if your institution is growing in size and scope, is to persuasively inform the people controlling the purse strings at your institution of the risk, inefficiency, and cost of your current manual processes to manage regulatory change versus automation.

This is especially true if your institution is subject to various state obligations, as it is getting more challenging to keep up with the fast-moving, complex regulatory activity at the state level, including from state mini-CFPBs.

What are the risks? The primary risk would be failing to address an applicable regulatory compliance obligation—particularly one that negatively impacts your customers.

And what are some of the inefficiencies and potential costs related to manual regulatory change processing that your Board or Compliance Committee should know about to help you get the funding or other resources you need for automation? As it turns out, there are several, and quantifying the problem is fairly simple.

Manual processing of regulatory change makes ineffective use of your most skilled personnel. That is a real risk today, as experienced compliance personnel are in high demand, and there are greater strains on limited resources.

- The manual gathering of potentially applicable regulatory change events, guidance and other important releases for your institution using web-scraping, RSS feeds and email pushes from law firms, regulatory bodies, industry associations and others cannot continue to keep up with the quantity of releases that your institution is subjected to and needs to be aware of today. This is true especially as it grows in size and scope, and if it is subject to state obligations.

- If you want to better quantify your exposure to regulatory change risk, simply visit the websites of the regulators, agencies, and others you rely on for regulatory change events and horizon scanning, and count the number of releases over the previous quarter. That means counting not just the regulatory change events, but the guidance, litigation releases, speeches, enforcement actions, exam manual changes, interpretive letters, press releases and many other developments that your institution needs to be aware of and that your compliance staff review today. That will be an eye-opening metric when compared to your resources.

- Think about the human resources you have processing regulatory changes at your institution today. What will happen to the process when those resources retire or otherwise move on, and are replaced by compliance professionals who are more accustomed to leveraging and integrating technology solutions? Is the process efficient and easily transferred to new employees?

Automation of RCM will never replace the mind of trusted, experienced, issue-spotting compliance personnel. However, it can significantly reduce workload and allow compliance professionals to concentrate on the more essential elements of their position by:

- Gathering applicable regulatory intelligence releases from federal and state sources into one central location
- Separating those releases into actionable or informative categories
- Connecting those releases to policies, procedures, products, services, risks, controls, testing and other elements of your Compliance Program—if you have taken the time to map the applicable citations in your Regulatory Library when you implemented your automated solution

Use of spreadsheets can cause myriad, potentially costly problems that automation solves, especially as your institution grows in size and scope. Consider these challenges:

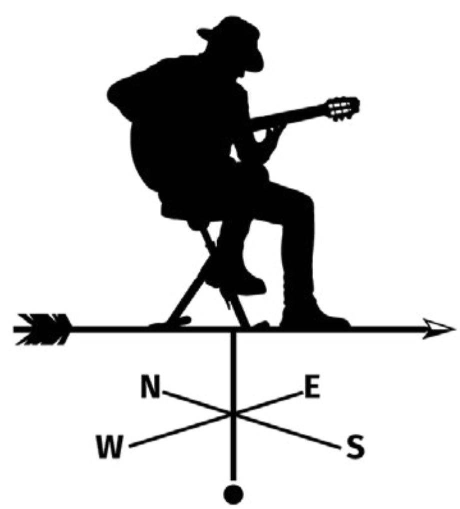
- Version control for tracking when changes occurred
- Access control to identify who made changes
- Formula or human errors that may go undetected
- No ability to associate related regulatory releases
- No connection to your Regulatory Library
- Limited reporting capabilities; and
- Complicated workflows—which means:
  - Need for a central repository of assignments related to a regulatory change event
  - Need for documentation for the future about who was informed of and/or worked on a regulatory change event
  - Need for robust data to generate reporting for regulatory change-related activities and milestones

So where does one start when choosing an automated RCM solution? In my experience, the best path forward is first to research. Speak to peers and review industry ratings of the established RCM content providers. Engage procurement. Be realistic about what you want or need automation to do.

For example, if you want to receive releases in a timely manner, they may not be curated, or may just be summarized by the issuing body. So, determine what features are most important to your institution.

When creating your criteria for RCM automation, strongly consider:

- Requiring flexible technology for the regulatory content data feed—as your institution may change GRC (governance, risk management and compliance) platforms
- The depth and breadth of the coverage you need—particularly if you are now or may become a global institution
- Requiring that solution providers exhibit their commitment to growing their content—so as your institution's regulatory scheme changes through new products, services, or acquisitions, new regulatory bodies can be added
- Ensuring that as part of the implementation process, all who need to be trained are trained, including leaders and business team members who may be accessing the solution



Remember that automation will only take you so far—for example, most solution providers will not write your obligations related to a regulatory change or be able to map elements of your Compliance Program to your Regulatory Library.

While all that work can be done on most technology platforms, it typically requires the institution itself, or additional consultants, to provide the connections that will be made during the implementation of an automation process. That is where the spreadsheet records you use today will come into play—they will not go to waste, and they will likely form the basis of your automated solution.

Include your vendor procurement group early in the process to perform due diligence so that there are no surprises later regarding your institution's third-party service provider requirements. Also, consider a Request for Information and/or Request for Proposal process where you can clearly state what you want in your RCM automated solution and weed out any providers that do not measure up.

A word of caution though: even where an institution's RCM process is automated, you may have the firehose problem—if the content coming into the automated process is not properly configured, to wade through the irrelevant content can consume your expert compliance resources as much as the manual processes. Keep that issue in mind as you venture down the road to automation. Ensure that automated solutions you may be considering provide you with the means to help control the firehose.

And finally, ensure you understand how any automated solution you are considering works, including its use of artificial intelligence and whether it is augmented by human experts in any way. You may need to explain how it works, at least generally, to your Board, Compliance Committee, regulators, or others.

Knowing which way the winds of regulatory change are blowing is only part of the solution in addressing the onslaught. Take action now to include emerging technology augmented by human expertise to bolster your regulatory change management program and avoid finding yourself—as Bob Dylan says, "...on your own, with no direction home."

Best wishes on your continuing regulatory change management journey!

__Elaine F. Duffus,__ CSCP, CFCS, FLMI, JD, is a Senior Specialized Consultant with the Financial Services Compliance Program Management solutions team at Wolters Kluwer. She brings more than 20 years of professional expertise to her role, including several as Chief Compliance Officer in the insurance, securities, and banking industries.

Elaine can be reached at
Connect with Elaine on LinkedIn

Overdrafts: Litigation, Regulatory Trends, and Action Steps

As published in BankingExchange.com | By **Therese Kieffer** and **Karl Leslie**

Compliance officers everywhere are likely aware that overdrafts have been a hot topic for decades

Compliance officers everywhere are likely aware that overdrafts have been a hot topic for decades. On the litigation front, for financial institutions battling overdraft lawsuits, it's been like playing a game of whack-a-mole. Solve for one claim and another legal theory pops up somewhere else. On the regulatory front, the banking agencies have been continuously addressing the topic, too. This article will discuss decades-long trends in overdraft litigation, regulatory activity, and suggest some possible actions for financial institutions that are looking to respond to the most recent trends.

Early Overdraft Lawsuits

In the late 1990s and early 2000s, there was an avalanche of overdraft fee lawsuits, typically brought as class actions,[1] and focused on the practice of processing items from "high to low." Financial institutions argued this practice ensured important, big-ticket items, such as a mortgage, would be paid. Consumers countered that financial institutions were just trying to maximize profits. As a result of these lawsuits, it has become common practice for financial institutions to disclose their payment order of items.

Interagency Guidance on Overdraft Protection Programs (2005)

It was partly in response to these early overdraft-related lawsuits, and the publicity they generated, that four agencies joined together to release the "Joint Guidance on Overdraft Protection Programs" in 2005.[2] In this guidance, they covered many best practices that are still relevant today. For example, the guidance notes that institutions must consider concerns relating to unfair or deceptive acts or practices when advertising overdraft protection services, and also reminds financial institutions of the need to comply with the requirements of the Truth in Savings Act and the Electronic Funds Transfer Act.

The Regulation E Overdraft Rule

On November 17, 2009, the Federal Reserve Board published a final rule amending Regulation E. Today, the rule is generally known as the Reg E overdraft opt-in rule.[3] The rule became effective July 1, 2010. Since then, the Dodd-Frank Act transferred rulemaking authority of Reg E to the Consumer Financial Protection Bureau (CFPB), and while Reg E has undergone some changes under the CFPB's jurisdiction, the overdraft opt-in rule has not.

[1] See, e.g., *Gutierrez v. Wells Fargo*, 704 F.3d 712 (9th Cir. 2012), or more recently, *Parrish v. Arvest Bank*, 2016 US Dist. LEXIS 91302 (OK. W. Dist. Ct., July 14, 2016)
[2] https://www.federalreserve.gov/boarddocs/srletters/2005/sr0503a1.pdf
[3] See 12 CFR 1005.17

At a high level, Reg E requires financial institutions to obtain an opt-in from a consumer before being able to charge the consumer a fee on a one-time debit card or ATM transaction. The opt-in rule includes the requirement to provide the consumer with a notice which adequately describes the overdraft services so that the consumer is able to make an informed decision about whether to opt-in to the overdraft service.

To facilitate the opt-in process, the Fed developed a consumer-tested model Opt-in Notice (Model A-9) (though a financial institution could use their own).[4] The rule and commentary required the notice to be given as a standalone form, provided a "safe harbor" for using the model, and implemented strict restrictions against making modifications to the model form. Recently, several court cases are causing financial institutions to rethink how the model form gets used. More on that in a bit.

Current Agency Focus – CFPB and OCC
For anyone who has stayed current on the subject of overdrafts, they already know that, under the current administration, financial institution overdraft practices have been under the microscope. Several agencies have expressed "concern" that financial institutions are "deeply dependent" on overdraft fees. They have also been investigating the impact that overdraft practices have on consumers. That does not mean the various banking agencies are planning any new overdraft rulemaking. In fact, that doesn't appear to be the case at all, as overdrafts have not made the CFPB's Regulatory Agenda since a pre-rule item was moved to an inactive status in 2018.[5]

Instead, the CFPB has indicated throughout this past year that they are looking closely at overdraft and NSF practices as part of their supervisory and enforcement efforts. In December 2021, the CFPB released research on Overdraft and NSF fees demonstrating financial institutions' dependence on such fees.[6] As part of their report, the CFPB warned that any financial institutions (or individuals) engaged in illegal overdraft practices would be subject to enforcement action.

In June 2022, the CFPB reported that, since the beginning of the year, it had been piloting a supervision effort to collect information from 20 supervised institutions on their overdraft and NSF practices.[7] The CFPB indicated they intended to use this information to identify institutions for further examination and would share the information with other regulators.

The CFPB is not the only agency scrutinizing overdrafts. The OCC's Michael Hsu has given several addresses during his tenure indicating his agency is looking at overdraft fees and encouraging financial institutions to adopt more consumer-friendly practices.[8] In addition, the topic of overdrafts has repeatedly appeared front and center in agency bulletins. Some of which will be discussed below.

It is also worth noting that not only are the agencies revisiting overdraft practices, but Congressional interest in the topic appears to have picked up. While it appears unlikely that any bills will be passed by both houses of Congress, there have been several high-profile hearings in the past year.[9]

And while agency scrutiny and Congressional hearings suggest future changes might be coming to overdraft practices, the biggest current impact on practices and documentation continues to come from lawsuits.

Recent Trends in Overdraft Litigation – APSN
One of the primary trends in overdraft litigation is typically called the "Authorized Positive, Settle Negative" theory, or APSN. An example of an APSN transaction is where a debit card transaction is initially authorized against an amount available in the account. But then, prior to settlement, an intervening transaction creates a situation where there is not enough money to cover the initial transaction. Consequently, the financial institution charges an overdraft fee.

The legal cases typically argue that the account agreements promised the financial institution would set aside funds in accounts at the time of authorization to cover payments for the authorized transactions and position the claim as either a breach of contract or a violation of unfair, deceptive, or abusive act or practice.[10]

Various agencies have weighed in on this practice and most assert the practice should be avoided. Of interest, the agency analysis seems to have evolved from calling APSN "deceptive" or "unfair" to simply labelling it as "unfair."

For example, in 2015, the CFPB's Winter Supervisory Highlights noted that consumers could not have anticipated this practice since it was not properly disclosed.[11] This suggests the CFPB viewed the practice as "deceptive." However, Interagency Guidance from 2016 includes a slide describing APSN as an "unfair practice".[12] This summer, the New York Department of Financial Services also labeled APSN an "unfair."[13]

The significant difference between unfair and deceptive is that an institution cannot disclose its way out of an unfair practice. Instead, the practice should just be avoided.

4 Appendix A to 12 CFR Part 1005
5 "CFPB Moves Regulation E Changes & Overdraft Regulations Down on Their Priorities List," NACHA (May 18, 2018) (includes links to CFPB's press release and Spring 2018 regulatory agenda)
6 "CFPB Research Shows Banks' Deep Dependence on Overdraft Fees," CFPB Press Release (Dec 1, 2021)
7 "Measuring the impact of financial institution overdraft programs on consumers," Patrick Gibson & Lisa Rosenthal, CFPB Blog (June 16, 2022)
8 Michael J. Hsu: "Reforming Overdraft Programs to Empower and Promote Financial Health" (Dec. 8, 2021) and "Don't be the last banker to update your overdraft program," American Banker (March 28, 2022)
9 For example, see 2022 US HR 4277
10 E.g., *Hash v. First Fin. Bancorp*, 2021 U.S. Dist. Lexis 42711 (Ind. S. Dist. Ct, March 8, 2021), *Gardner v. Flagstar Bank*, FSB, 2021, U.S. Dist. LEXIS 158548 (Mich. E. Dist. Ct., Aug. 23, 2021)
11 CFPB Supervisory Highlights, Winter 2015
12 Interagency Guidance, 2016
13 Industry Letter: Avoiding Improper Practices Related to Overdraft and Non-Sufficient Funds Fees, New York State Department of Financial Services (July 12, 2022)

Recent Trends in Overdraft Litigation – Ledger Balance v. Available Balance
Another trend in litigation is the argument that the financial institution has not adequately disclosed that it is using the "available" balance instead of the "ledger" (or "actual") balance. The argument typically goes that, because the financial institution did not adequately define "available" balance, the consumer could not determine if they had enough money in their account to cover a transaction and therefore would not know when a fee would be assessed. In Tims v. LGE Community Credit Union,[14] for example, the court, addressing a breach of contract claim, determined that, in viewing the Model A-9 form alongside the other account documentation, the definition of "available balance" had not been adequately disclosed.

It should be noted that the terms "available balance" or "ledger balance" are not defined in any regulations either. In cases, courts have defined the "ledger balance" as the "actual amount of money in an accountholder's account at any particular time." The "available balance", in contrast, is "the actual amount of money in the account minus any 'holds' on deposits and pending debits that have not yet been posted."[15] But without a regulatory definition, institutions are really left to define this on their own.

Recent Trends in Overdraft Litigation – Reg E Model Opt-In Form Ambiguous
The litigation over "available" vs "ledger" balance is often paired with the theory that the language in the Model A-9 form is not sufficient.

In such cases as *Adams*[16] and *Grenier*,[17] the courts, addressing the Reg E violation claim, focused solely on the Model A-9 form, and did not consider the language in the context of the account agreement or other documentation, since Reg E requires the disclosure to be "segregated" from all other information. The model form simply says "An overdraft occurs when you do not have enough money in your account to cover a transaction" but does not describe what "enough money" means. Therefore, the plaintiffs argue they cannot determine when their account will be charged an overdraft.

Financial institutions usually counter that a specific definition of "available" is not necessary because Reg E offers a safe harbor for using the model. They also point out the regulatory restrictions on making any changes to the Model A-9 form. But courts have routinely rejected this defense and found the financial institutions' disclosure to be inadequate, suggesting that if the language of the model form does not accurately and completely describe an institution's practice, then it is inadequate.

The CFPB, for its part, has yet to provide any guidance on this particular issue.

Recent Trends in Overdraft Litigation – Re-presented Items (or ACH Retry)
The last litigation trend this article will address is the "re-presentment" situation,[18] which is really a nonsufficient funds dispute—not an overdraft dispute. In this scenario, the merchant submits a request for payment, which is denied due to insufficient funds. A fee is assessed. Sometime later, the merchant submits another request for payment – that is, they re-present the item for payment. If there are still insufficient funds, the payment is again denied, and another NSF fee is assessed. Of course, this can recur multiple times. Thus, a customer might be assessed multiple NSF fees for what, in their view, is the same transaction.

And that really is the center of the dispute. The consumer argues that this was a single transaction, and should be assessed one fee at most. From the institution's perspective, each time the request for payment is submitted, that is a unique transaction. And so a fee can be assessed for each transaction.

The lawsuits center around whether the practice has been disclosed, suggesting that the practice is deceptive. Of great interest, however, are statements from the FDIC in March[19] and in August[20] of this year and from the New York Department of Financial Services in June of this year.[21] While both call the practice deceptive and note the need for adequate disclosure, both agencies have also indicated that in some circumstances the practice might be considered unfair. As a result, there may be a need to avoid the practice altogether or, alternatively, to modify the practice to avoid the portion that is unfair. According to the FDIC, to avoid the practice being considered unfair, institutions need to provide meaningful notice at the time an NSF fee is assessed as well as adequate time for the consumer to bring the account balance current before assessing any further fees.

The FDIC August 2022 Supervisory Guidance on this topic also provides financial institutions with some important information. Specifically, the FDIC provides guidance for financial institutions that self-identify and fully correct violations, including the potential of limiting the lookback period to two years from the date of the letter.[22]

[14] 935 F.3d 1228 (11th Cir. 2019)
[15] *Grenier v. Granite*, 570 F.Supp.3d 18 (New Hampshire Dist. Ct, Nov. 8, 2021)
[16] 2021 WL 3726007
[17] No. 21-cv-00534-LM, 2021 WL 5177709 (D.N.H. Nov. 8, 2021)
[18] E.g., *Lambert v. Navy Fed. Credit Union*, 2019 U.S. Dist. LEXIS 138592 (Va. Eastern Dist. Ct, Aug. 14, 2019), *Mawyer v. Atl. Union Bank*, 2022 U.S. Dist. LEXIS 65397 (Va. Eastern Dist. Ct., April 7, 2022)
[19] FDIC Consumer Compliance Supervisory Highlights, March 2022
[20] FDIC Supervisory Guidance on Multiple Re-Presentment NSF Fees, August 2022
[21] Industry Letter: Avoiding Improper Practices Related to Overdraft and Non-Sufficient Funds Fees, New York State Department of Financial Services (July 12, 2022)
[22] FDIC Supervisory Guidance on Multiple Re-Presentment NSF Fees, August 2022

Emerging New Topic – So-Called Double Fees
In July 2022, the New York State Department of Financial Services identified "double fees" on a "futile" overdraft transfer as another practice financial institutions should avoid.[23] According to the NYDFS, an unfair act or practice occurs when a consumer is charged both an overdraft fee and a transfer fee on a transfer from a linked account where the linked account does not have enough money available to cover the overdraft.

Action Steps
There are a number of steps financial institutions can take to mitigate risk. At a minimum, financial institutions should make sure their account documentation matches their practices. For example, a financial institution can state whether they use the available balance or the ledger balance method and then describe what that means for that institution in an overdraft context.

Financial institutions should also pay special attention to whether a claim is considered deceptive, unfair, or both. Institutions may be able to work with counsel to disclose their way around acts or practices that are considered deceptive. However, if an act or practice is considered unfair, institutions may need to work with counsel and processors to determine how to avoid the act or practice altogether – or at least avoid (or appropriately respond to) the portion of the act or practice that is considered unfair.

Maybe the most interesting dilemma is addressing the cases around the use of the Model Reg E Opt-In notice and how to balance the Reg E restrictions on making modifications to the model form against the court cases saying institutions need to amend the form to accurately describe their practices. To do this, institutions should work with legal counsel to determine the best approach for their institution. Factors to consider include:

- What method does the institution use: available, ledger, or some kind of hybrid? Institutions that use the available balance method, or some other complex method, may be at higher risk.
- Where is the institution located? Review the decisions for the courts that the institution is likely to be sued in and determine whether there are cases in that jurisdiction requiring Model A-9 to be modified in some circumstances. For example, Tims was an 11th circuit case (which covers Alabama, Florida, and Georgia).
- Finally, for institutions that use a content provider, make sure the provider offers the ability to modify the opt-in form so that any changes deemed necessary can be made.

Conclusion
In conclusion, all the activity in this area indicates that overdraft litigation and scrutiny are not going away any time soon. And that makes it important for financial institutions to stay current and responsive to what is happening with litigation as well as agency and Congressional activity.

Therese Kieffer *is a Specialized Consulting Manager with the Regulatory Analysis Team of Wolters Kluwer's Compliance Center of Excellence. She develops content strategies to simplify the most complex regulatory challenges today—including UDAAP, cryptocurrency, Truth-in-Savings, among others.*

Therese can be reached at
Connect with Therese on LinkedIn

Karl Leslie *is a Principal Consultant with the Regulatory Analysis team of Wolters Kluwer's Compliance Center of Excellence, where he acts as the lead attorny in areas of deposit law, tax-advantaged accounts, and anti-money laundering. With over 30 years of experience, he uses his knowledge to help businesses develop strategies to confidently face emerging compliance challenges.*

Karl can be reached at
Connect with Karl on LinkedIn

[23] Industry Letter: Avoiding Improper Practices Related to Overdraft and Non-Sufficient Funds Fees, New York State Department of Financial Services (July 12, 2022)

OneSumX® ProViso

To learn more, visit wolterskluwer.com →

Complete state law compliance and data safety, utilizing clustering, AI-based tagging, and expert-augmented intelligence.

Financial Services Expanding Through Partnerships—Fair and Square

By **Tom Grundy**

"Diligence is the mother of good luck."
 -Benjamin Franklin

There was a time when the topic of third-party risk management largely focused on third-party service providers contracted to support back-office core functions necessary to carry out a financial institution's delivery of products and services. While this remains true today, third-party risk management has expanded significantly to cover a much wider range of relationships that, in many cases, effectively serve as outsourced lines of business, expanding the types of products and services banks can offer to their customers without the direct investment in technology and other resources.

As someone who is fortunate to have been involved in an early financial technology venture dating back to the 1990s—and as an observer of the growth in the number and types of FinTech over the past two decades—there's no question that financial technology firms are here to stay. Once perceived as rivals by traditional finance participants, fintech entities have proliferated over the past two decades. Today, many are maturing as going concerns that bring considerable technological prowess combined with an insatiable appetite for innovation, and the ability to go to market quickly. This dynamic creates an ever-expanding range of ready-made solutions that can help traditional financial institutions, which are seeking to expand into new products and services, and to compete in an increasingly technology-focused world.

Digital delivery of financial services, driven largely by shifting demographics, and boosted in recent years by the COVID-19 pandemic; the emergence of artificial intelligence and increasing use of alternative data in financial decision-making; and the March 2022 announcement by the Consumer Financial Protection Bureau (CFPB) that the agency will target discrimination in its oversight and enforcement of unfair, deceptive and abusive acts and practices (UDAAP), all point to an increasingly complex and competitive financial marketplace.[1]

For any financial institution on the partnership path to strategically expanding financial products and services, these developments make a compelling case for establishing an experienced, highly skilled, and well-rounded due diligence team that includes fair and responsible banking compliance expertise in all relevant aspects of building and managing a relationship with third parties.

[1] CFPB Targets Unfair Discrimination in Consumer Finance, March 16, 2022, go to: [CFPB Targets Unfair Discrimination in Consumer Finance | Consumer Financial Protection Bureau]

Key Considerations for Managing Third-Party Service Provider Relationships

When was the last time you took a hard look at your bank's third-party risk management program? Is it largely the same program established years ago when regulatory guidance in this area was released, or under an earlier business model and strategic plan for the bank? Given the pace of change in financial services driven by technology-centric consumer demographics, your bank's third-party risk management program may be due for an update.

For federally supervised financial institutions, the FFIEC's Outsourcing Technology Services guidelines as well as the outsourcing and third-party guidance issued by each of the regulatory agencies provide a good amount of information for identifying risk and structuring programs for onboarding and overseeing external relationships. As such, regulated financial institutions should have the basic bone structure of a third-party risk management program in place. For fintech startups, it is understandable that third-party risk management policies, procedures, and processes may be relatively new. What follows are some core framework considerations that banks and nonbank financial services providers alike should build into third-party risk management processes.

Risk management practices should be commensurate with the level of risk and complexity of third-party relationships. An institution's board of directors and management should identify those third-party relationships that involve critical activities and ensure that appropriate risk management practices are in place to assess, monitor, and manage the risks. Effective third-party risk management entails the following elements:

Strategy and Planning

With more and more strategic partnerships forming between regulated financial institutions and fintech entities, understanding the strategic priorities and plans of the parties to a partnership can greatly inform the prospects for developing a successful venture.
For a traditional financial institution seeking a partnership, knowing the plans a fintech partner has regarding new products and expansion strategies, joint ventures, or joint marketing initiatives could benefit its strategic planning activities and support the decision of whether or not to partner.[2]
For any due diligence exercise, always keep in mind that institutional reputation is at stake and can be negatively impacted by the actions of a prospective partnership. From a fairness and UDAP/UDAAP perspective, financial technology startups generally are inexperienced when it comes to regulatory oversight. Well-intentioned partners can make adverse headlines.[3] As you plan and strategize, maintaining an intentionally darker view of what could potentially go wrong could serve you well in the long run.

In July 2021, proposed interagency guidance on third-party relationship risk management provided a long list of planning considerations, chief among them was understanding the strategic purpose of the business arrangement and whether it aligns with a bank's overall strategic goals, objectives, risk appetite, and broader corporate policies. Also on the list was a point for considering the complexity of the relationship, the volume of transactions generated, use of subcontractors, and the technology required to support the business.

The addition of a single partnership can introduce numerous, complicated variables that can exponentially elevate compliance, fair lending, and UDAP/UDAAP risks. Therefore, closely examine the prospective third party's corporate philosophies and practices regarding legal and compliance management; operational excellence, quality assurance, and customer service; and employment policies and practices. It is important to select a partner that aligns with your corporate policies and practices, shares your organizational views, and is compatible relative to diversity policies and practices.[4]

Due Diligence and Third-Party Selection

As more and more regulated entities consider entering a relationship, putting brand names and charters on the line to facilitate the origination of products or services by relatively new fintech entities is paramount to accounting for and analyzing the many potential risks.[5] Conducting due diligence on a prospective third-party partnership should be commensurate with the level of perceived risk and complexity that will be involved in managing the proposed relationship. Agility and preparedness to adjust the scope of due diligence and testing as you conduct analysis should be agreed upon going in, and as risk issues surface, additional or different testing and analysis may be necessary. Throughout this process, never lose sight that you are guarding the reputation of your institution while attempting to build successful and fully compliant business relationships with an external organization.

Conducting due diligence on a prospective third-party business partner can be a large and complex exercise. The team that you assemble and deploy to conduct this exercise should be subject matter specialists representing all affected business and functional areas of the enterprise. The many areas of consideration will typically address the following topics and themes:

Strategies and Goals. Does the third party's overall philosophies, business strategy, goals, and employment practices align with those of your organization?

2 Conducting Due Diligence on Financial Technology Companies A Guide for Community Banks, August 2021, go to: Conducting Due Diligence on Financial Technology Companies A Guide for Community Banks (fdic.gov)
3 Solving the problem of racially discriminatory advertising on Facebook, Jinyan Zang, October 19, 2021, go to: https://www.brookings.edu/research/solving-the-problem-of-racially-discriminatory-advertising-on-facebook/
4 Proposed Interagency Guidance on Third party Relationships: Risk Management, go to: pr21061a.pdf (fdic.gov)
5 FDIC Consumer Compliance examination Manual, VII-4.3

Legal and Regulatory Compliance. Consider:

- How effective is the third party's legal and regulatory compliance program? Does it have the necessary licenses to operate and the expertise, processes, and controls to operate in a compliant manner under both domestic and international laws and regulations?
- Sufficiency of internal and external Legal and Compliance resources
- Level of expertise in leveraging artificial intelligence and alternative sources of data in financial decision-making
- Adequacy of resources dedicated to fairness, as well as to the responsibility for identifying and documenting UDAAP risks and assessing the effectiveness of controls?

Financial Condition. Evaluate the third party's financial condition and overall stability by scaling the analytics and underwriting relative to the significance of the activity that the third party will perform.

Business Experience and Reputation. Assess the third party's reputation, including history of customer complaints or litigation. Determine how long the third party has been in business, its market share for the activities, and whether there have been significant changes in the activities offered or in its business model.

Fee Structure and Incentives. Determine if the fee structure and incentives would create burdensome upfront fees, result in inappropriate risk-taking, or result in disparate treatment.

Qualifications, Backgrounds, and Reputations of Company Principals. Are thorough background checks conducted on the third party's senior management, employees, and subcontractors who may have access to critical systems or confidential information?

Risk Management. Evaluate the scope of risk management activities and the effectiveness of policies, processes, and internal controls, as appropriate.

Information Security. Does the third party have sufficient experience in identifying, assessing, and mitigating known and emerging threats and vulnerabilities?

Physical Security. Evaluate whether the third party has sufficient physical and environmental controls to ensure the safety and security of its facilities, technology systems, and employees.

Management of Information Systems. Gain a clear understanding of the third party's business processes and technology that will be used to support the activity.

Operational Resilience. Determine whether the third party maintains disaster recovery and business continuity plans that specify the time frame to resume activities and recover data.

Incident-Reporting and Management Programs. Are clearly documented processes and accountability for identifying, reporting, investigating, and escalating incidents in place? Risk management practices should be commensurate with the level of risk and complexity of third-party relationships.

Human Resource Management. Review and assess:

- Training programs to ensure that the third party's staff is knowledgeable of laws, regulations, technology, risk, and other factors that may affect the quality of the activities provided; and
- Hiring policies and practices with respect to diversity.

Reliance on Subcontractors. Evaluate the third party's ability to assess, monitor, and mitigate risks from its use of subcontractors, helping to ensure that the same level of quality and controls exists regardless where the subcontractors' operations reside.

Insurance Coverage. Verify that the third party has fidelity bond coverage to insure against losses attributable to dishonest acts, liability coverage for losses attributable to negligent acts, and hazard insurance covering fire, loss of data, and protection of documents.

Conflicting Contractual Arrangements with Other Parties. Evaluate the potential legal and financial implications of contracts between the third party and its subcontractors or other parties.

Organizing and assimilating the results of due diligence activities as the process unfolds will reveal whether the prospective third party is a fit. Results presented to senior management and the Board should support a clear decision as to whether the third party aligns strategically—and whether to proceed with the partnership.

Contract Considerations

Developing a contract that clearly outlines the rights and responsibilities of all parties sets the foundation of the relationship. This section provides a non-exhaustive list of some key considerations as you proceed to contracting with a third party.

Confidentiality. Entering a relationship with a third party poses many risks and threats, particularly to the bank's information. Prohibiting the use and disclosure of the bank's information by a third party and its subcontractors should be addressed, except only as necessary to fulfill contracted activities and to maintain compliance with legal requirements. Moreover, the contract should be clear that the third party implements and maintain controls to ensure compliance with privacy regulations and regulatory guidelines relative to customers' personally identifiable information. Responsibility for timely disclosure and notification, among other requirements, of information security breaches resulting in unauthorized intrusions or access that may materially affect the banking organization, or its customers should be detailed.

Use of Subcontractors. Contracts with third-party relationships can provide direction and control regarding the use of subcontractors and, if permitted should outline expectations for the third party's oversight responsibilities in selecting and managing these relationships. Requiring your third-party relationship to provide advance notice of the use of subcontractors and to seek prior approval by the bank is advisable. Agreements can define or prohibit services that may be subcontracted; set expectations for the third party's due diligence process for engaging and monitoring subcontractors, and set the notification and approval requirements regarding changes to the third party's subcontractors. Detail the third party's obligations for reporting on subcontractor conformance with articulated performance measures; required periodic audits and reporting of results; and compliance with laws and regulations including UDAAP and expectations relative to fair and responsible execution of responsibilities. The third party's liability for activities or actions by its subcontractors should be addressed, along with the responsibility for any costs and resource commitments required for additional monitoring and management of the subcontractors. Reserve the right to terminate the contract with the third party without penalty if the third party's subcontracting arrangements do not comply with the terms of the contract.

Compensation. The contract should establish an effective process for review and approval of compensation, fees for services by a third-party partner of service provider. Fee structures and incentives may result in inappropriate risk-taking by the third party to the extent of potential unfair and deceptive acts or practices or could result in unfair and discriminatory provision of products and services. Remain vigilant at all times to ensure that contractual compensation arrangements are appropriately balanced and present no potential for heightened risk.

Complaint Management. The contract should define processes ensuring that the third party appropriately addresses customer complaints directly or through a process that meets your corporate standard. It is important to protect your right of access to monitor complaint activity, analysis, response, and course of action to resolve underlying issues.

Operational Resilience and Business Continuity. Contracts should address planning and responsibility with respect to the continuation of the business function in the event of problems affecting a third party's operations, including degradations or interruptions resulting from natural disasters, human error, or intentional attacks. Stipulate the third party's responsibility for backing up and otherwise protecting programs, data, and equipment, and for maintaining current and sound business resumption and contingency plans.

It is prudent going into the relationship to be realistic and ensure provisions are drafted into the contract that in the event of the third party's bankruptcy, business failure, or business interruption, would allow for transferring the bank's activities to another third party without penalty.

Right to Audit and to Require Remediation. Ensure that the contract establishes your organization's right to audit, monitor performance as an ongoing matter, and to require remediation when issues are identified. Be clear in stating the types and frequency of the audit reports expected of the third party, including fair lending analytics, assessment of consumer risks, and independent validation of models. The contract can also inform the third party that audit reports and independent reviews and work papers should be available and provided to regulators upon request.

Compliance with Laws and Regulations. Third-party relationships with regulated entities are subject to regulatory examination. The contract should cover specific laws, regulations, guidance, and self-regulatory standards applicable to the third party's activities.

Insurance Coverage. Legally require the third party to maintain adequate insurance, naming the bank as insured or additional insured, where appropriate. Require notification to the bank of material changes to coverage, and to provide evidence of coverage either directly, or upon request. The types of insurance coverage include fidelity bond; cybersecurity; liability; property hazard and casualty; and intellectual property.

Limits on Liability. Because a contract may limit the third party's liability, this necessitates an assessment of whether the proposed limit is in proportion to the potential liability or loss that could result because of the third party's failure to perform or to comply with applicable laws. Scenario analyses pondering the potential worst-case outcomes and failures may have to be performed to establish the range of potential damage to the business and financial loss. Consider provisions directed to the third party regarding liability for delayed or erroneous transactions, and other potential risks, particularly associated with UDAAP and fair lending. Each partnership has unique characteristics. Consult counsel on holding third parties accountable.

Default and Termination. Looking ahead and establishing provisions for a range of relationship-ending possibilities is an effort worth making. The many situations that you should consider include change in control; merger or acquisition; substantial increase in cost; repeated failure to meet service standards; failure to provide critical services and required notices; failure to prevent violations of law or unfair and deceptive practices; bankruptcy; company closure; and insolvency.

Consult your legal counsel to ensure that adequate legal protections are addressed in the contracts you establish with each third-party relationship.

Ongoing Monitoring

Actively monitoring the performance of third-party relationship relative to established expectations will serve you well. Whether the third party is originating consumer loans in partnership with the bank or contracted to perform critical activities, the level of monitoring should be tailored to the business activity and commensurate with the level of risk inherent to the relationship. To ensure that adequate monitoring is established, identifying bank staffing resources with the necessary expertise, authority, and accountability to monitor the third party is the first step. Monitoring can take the form of regular onsite visits and automated exception reporting, to the provision of regularly scheduled management dashboard reporting.

Monitoring of risk and assessment of the effectiveness of risk-mitigating controls, performance in relation to service level agreements, and compliance with legal and regulatory requirements should be part of the overall monitoring plan. As a general matter, the criteria assessed during initial due diligence should continue to be periodically reviewed as part of the ongoing monitoring. Particular attention, however, should be directed to monitoring the volume, nature, and trends of consumer complaints, in particular those that indicate potential UDAP/ UDAAP compliance or fair lending risk and the third party's ability to appropriately respond to, and remediate the root cause of customer complaints.

It is important to keep in mind that the level and types of risks may shift during the life cycle of a third-party relationship and, consequently, monitoring activities must adjust, resulting in changes to the frequency and types of required reporting, including service-level agreement performance reports, audit reports, and control testing results. Relationship managers should escalate significant issues or material weaknesses noted through ongoing monitoring or as indicated by audit findings, deterioration in financial condition, security breaches, data loss, service or system interruptions, or findings of non-compliance with laws and regulations.

Termination, Contingency Planning, or Exit Strategy

Third-party relationships eventually terminate due to the expiration or satisfaction of the contract; desire to seek the services of a different service provider; decision(s) on the part of the board and management to bring the activity in-house; discontinuance of the activity; or due to a breach of contract. Having a well-thought-out exit strategy to ensure that relationships terminate in an efficient manner, whether the activities are transitioned to another third party, brought in-house, or discontinued, is a prudent risk containment measure that will serve to protect the interests of the bank and your customers.

__Tom Grundy,__ CRCM, is the Senior Director, U.S. Advisory Services, for Wolters Kluwer and leads a team of subject matter professionals advising financial services industry clients. He is a former federal regulator with the Office of the Comptroller of the Currency and Federal Reserve Board, has served as a compliance professional for national-level banking and mortgage providers, and was a pioneer in FinTech.

Tom can be reached at
[Connect with Tom on Linkedin]

Regulatory change management elevated

Discover how Wolters Kluwer's data feed powers cutting-edge GRC operations

To learn more visit **wolterskluwer.com** →

10 Cs for the rest of 2022 and into 2023: Top challenges for banks

By **Tim Burniston**

The pressure for banks and other financial service providers to demonstrate effective and sustainable compliance risk management remains high as regulators demand greater levels of accountability and impose stricter enforcement measures. At the same time economic conditions and other significant global events add to unpredictability amidst the adoption of new or modified business practices and a rapid pace of change. There are already a range of initiatives underway and several more anticipated that present major risk challenges for financial institutions. With so many moving parts, where should one focus their efforts? This regulatory outlook is brought to you by the letter "C" and the number 10.

1. Climate

Climate risk management is receiving significant attention in the regulatory community. While we are still in the early stages of fully understanding how climate change imposes risks to banks and other financial service companies, it will remain a front and center topic for the Biden Administration, Congress, and regulators now and moving forward.

In March, the SEC issued a proposed rulemaking that would enhance and standardize climate-related disclosures. The SEC continues to work through the large volume of comment letters it received on its proposal and did miss a self-imposed October 2022 date for issuing a final rule. But there is a high degree of certainty that a final rule will be issued. Most " inside the Beltway" pundits coalesce around a Q1/Q2 2023 time frame for a final rule.

There is also engagement on climate change issues across the U.S. government and regulatory community. The federal prudential bank regulators are considering how, for example, the financial effects of climate change should be factored into banking supervision. We are seeing more and more guidance on how climate change exposures should be addressed in risk management practices.

We also expect more climate change activity at the Financial Stability Oversight Council, at the global level from the Basel Committee's Task Force on Climate-Related Financial Risks, and at the state level. Additionally, the impacts of climate change on low- and moderate-income communities have been raised in the context of the national discussion to modernize the regulations that implement the Community Reinvestment Act.

2. Community Reinvestment Act (CRA)

On May 5, 2022, the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency issued a uniform interagency proposal to modernize the regulations that implement the CRA. One of the key issues is how to adapt the CRA regulations to a digital world where banks increasingly serve their customers online rather than at physical branch locations. Modernizing the CRA regulations offers new opportunities to address community needs and embrace change, but it also presents challenges, including different evaluation methodologies, revised performance expectations, and changes in data collection. Over 650 comment letters were received on that proposal. Regulators continue to consider those comments as they work towards a final. Again, the time frame for release of a final rule is uncertain but many banks have already begun to evaluate how the proposal will affect their CRA programs going forward and are looking at 2023 as an intense implementation period.

3. Compliance and Consumer Protection

Regulators are increasingly devoting significant examination time and resources to fair lending issues including redlining, pricing, use of artificial intelligence in credit determinations, and appraisal bias. Last year, the DOJ recently announced its "Combatting Redlining Initiative," calling it one of the most aggressive and coordinated efforts to combat discrimination in lending. We have seen several redlining settlements with financial institutions since then and it is believed there are other cases pending. While the use of artificial intelligence to make credit decisions offers opportunities to promote inclusion, it carries real and potential fair lending risks. Those risks have also captured the attention of regulators.

The CFPB's rule implementing Section 1071 of the Dodd-Frank Act is expected to have a tremendous impact once finalized. This rule would impose new data collection and reporting requirements on lenders for credit applications made by women or minority-owned small businesses. Covered institutions will be required to compile, maintain, and submit extensive data to the CFPB and analyze that data to determine ECOA compliance. Respondents to the Wolters Kluwer 2021 and 2022 Regulatory & Risk Management Indicator surveys listed this rule as one of their most pressing regulatory challenges, making it one to watch. A final rule is expected by March 2023, which means that mobilizing internally to implement that rule will be essential. And doing that at the same time as a bank is operationalizing a new CRA rule will be daunting to say the least.

We have also seen changes in the Bank Secrecy Act (BSA) and anti-money laundering (AML) compliance area. Several initiatives emanated from the 2021 National Defense Authorization Act, including rules requiring certain companies to provide FinCEN with information about their beneficial owners, a new whistleblower program, and increased penalties for BSA/AML violations. On September 29, 2022, the U.S. Department of Treasury's Financial Crimes Enforcement Network ("FinCEN") issued a final rule implementing the Beneficial Ownership Information Reporting Requirements. Those requirements reflect the government's commitment to combatting corruption, money laundering, terrorist financing, tax fraud, and other illicit activities.

The OCC is also weighing in on BSA/AML compliance. In their supervisory priorities for 2023, as the agency did in 2022, the OCC notes it will continue to focus on evaluating the effectiveness of BSA/AML/OFAC risk management systems. Examiners will also focus on the nature and scope of the bank's products and services offered, customer base, and geographic footprints served. Other areas of focus will be the growing number and complexity of OFAC sanctions programs related to recent geopolitical events; evaluating technology and modeling solutions to perform or enhance BSA/AML and OFAC oversight functions; and determining the adequacy of suspicious activity monitoring and reporting systems and processes in providing meaningful information to law enforcement. Examiners will assess bank change management plans for implementing changes to existing BSA/AML compliance programs that will be necessary to implement the requirements of the Anti-Money Laundering Act of 2020.

The CFPB is sharpening its supervisory scrutiny on other consumer protection initiatives, including overdraft fee policies and what it characterizes as "junk" fees in the banking industry. The CFPB director has raised concerns about the effect certain fees have on consumers' ability to shop for credit.

4. Cybersecurity

In Wolters Kluwer's latest Indicator survey, cybersecurity ranked as the risk garnering the most concern and attention looking forward. And the threat of ransomware attacks led the list of factors in organizations' enterprise risk planning with 72 percent of the respondents rating it as their highest risk

Computer incident notification rules from regulators became effective on April 1, 2022, with a compliance date of May 1, 2022. The rule requires a bank to notify its regulator (FDIC, OCC, FRB) as soon as possible and no later than 36 hours after the bank determines that a computer-security incident that rises to the level of a notification incident has occurred.

In response to an increase in cyberattacks and data breaches, the Federal Trade Commission (FTC) recently amended the federal Standards for Safeguarding Customer Information (Safeguards Rule) under the Gramm-Leach-Bliley Act (GLBA). The updates put pressure on financial institutions to develop, implement, and maintain a comprehensive security system to keep their customers' information safe. Financial institutions have until January 10, 2023, to review their operations and ensure compliance with the amended Safeguards Rule.

We can also expect to see other announcements from bank regulators and an examination emphasis on operational risk, resilience, incident response, data recovery, and business resumption.

5. Cryptocurrency

There is palpable concern across the federal and state regulatory communities about the risks associated with the adoption of cryptocurrency to both financial entities, investors, and individual consumers. It is hard to imagine we won't see regulatory and other developments here that provide more protections. Further, the Federal Reserve is studying and evaluating the concept of a Central Bank Digital Currency (CBDC), which is basically a cryptocurrency version of the dollar. When and to what extent remains to be seen, but we can safely predict there will be activity in the cryptocurrency field in 2023.

The Federal Reserve Board, OCC, and FDIC announced a series of interagency "policy sprints" focused on crypto assets. As supervised institutions seek to engage in crypto-asset-related activities, the agencies recognize the importance of providing coordinated and timely clarity, where appropriate, to promote safety and soundness, consumer protection, and compliance with applicable laws and regulations.

6. Change management

The velocity, frequency, and some might say ferocity of regulatory change will necessitate banks implement a robust regulatory change management program. Advancements, such as digital lending transformation and AI, are bringing about changes in how products and services are delivered, opening new markets, and advancing inclusion. Conversely, risks need to be identified and managed. Regulators, including the CFPB, are looking at those risks and determining how best to manage internal and customer-facing operational changes due to disruptive events like the pandemic.

7. Competitive changes

Innovation is a necessary component of an organization's ability to effectively compete, grow, and survive. We've seen the banking industry embrace this need to innovate. However, innovation needs to happen in a compliance environment integrated within a risk management framework.

Financial technology will continue to invigorate the banking world. There has been an increasing presence and influence of fintechs and regtech on product design and delivery. We expect to see bank partnerships with fintechs continue to proliferate as traditional banks become more comfortable with digital lending and AI. We are likely also to see more transactions involving fintechs acquiring and merging with banks.

These changes highlight the importance of effective compliance management systems and third-party risk management. In fact, third-party risk management is a distinct focal point for regulators. The industry still awaits interagency guidance on third party risk management any time now. However, communications from regulators provide insights into their concerns. For example, the OCC 2023 bank supervision operating plan notes the following about third party risk:

“Examiners should determine whether banks are providing proper risk management governance of their third-party relationships, commensurate with the risks posed, which may include relationships with financial technology (fintech) companies. Examiners should identify the risk attributes of these relationships, for example, if they involve customer-facing products and services, are critical to bank operations, represent significant concentrations, affect the bank’s operational resilience, or affect compliance with requirements such as the Bank Secrecy Act and consumer protection laws. Additionally, examiners should determine whether the bank and third parties have sufficient, qualified staff to meet contractual obligations. Examiners should be aware of the cyber-related risks arising from third parties and evaluate the bank’s assessments of third parties’ cybersecurity risk management and resilience capabilities.”

8. Consolidation
Bank merger and acquisition activity is expected to receive more robust regulatory scrutiny. Following through on President Biden’s Executive Order on Competitiveness issued in July 2021 regulators are reviewing the Bank Merger Act. In March 2022, we saw the FDIC issue a request for information (RFI) soliciting comments regarding the application of the laws, practices, rules, regulations, guidance, and statements of policy that apply to merger transactions involving one or more insured depository institutions, including the merger between an insured depository institution and a noninsured institution. That review could bring changes that will either bolster existing requirements and standards or identify new ones. Evaluation factors under the Bank Merger Act standards that could receive additional scrutiny include “convenience and needs,” which ties in CRA and fair lending, among others, and management factors that encompass compliance and risk management.

9. Continuing effects of the pandemic
While we are certainly not in the same place in our nation’s response to the pandemic as we were in March 2020, it is not over. Continued vigilance in managing the fallout from the pandemic and periodic surges is still in the regulators’ bullseye. Operational and credit risks continue to be concerning to regulators and the industry. There are also economic pressures, most notably the rise in the inflation rate, interest rate increases by the Federal Reserve Board, and other matters such as energy prices, and a possible recession, not to mention the war in Ukraine and other global unrest.

10. Cannabis banking
According to BankDirector.com, the cannabis industry is growing exponentially, and nationwide sales are estimated to exceed $30 billion in 2022. Will we see federal marijuana legislation pass this year or in 2023? It isn’t clear, but something may happen. There are two proposals currently at play — the Secure and Fair Enforcement Banking Act (SAFE Banking Act) and the Cannabis Administration and Opportunity Act (CAO Act). While the House of Representatives has passed the SAFE Act many times, the bill has not gotten similar traction in the Senate, at least not yet. However, until legislation passes, the cannabis industry must rely on agency policy pronouncements and clarifications as issues arise.

The 10 Cs
Based on what we’ve seen from the regulators in 2022 and what is to come in 2023, we can expect substantive activity in key areas of risk and compliance. While this regulatory outlook highlights some of the most likely developments, the banking industry is rapidly changing. And if we’ve learned anything recently, it is to expect the unexpected.

Overall, to manage the significant amount of regulatory change on the horizon, financial institutions need to be vigilant about having a robust regulatory change management program and fully functioning Compliance Management Systems with updated policies and procedures. As the ripple effects of the pandemic, the economy, and other legislative and regulatory developments continue to burden financial institutions, developing a disciplined, automated approach to regulatory change will provide the consistency and transparency that regulators expect.

Timothy R. Burniston *is the Senior Advisor for Regulatory Strategy at Wolters Kluwer Compliance Solutions. In this role, he advises the executive leadership team and clients on emerging issues, legislative and regulatory developments, and regulatory strategy.*

Tim can be reached at
Connect with Tim on LinkedIn

Bringing digital signature to mortgage close

As published in Mortgage Professional America | By **Simon Moir**

Companies are integrating their technology so consumers can sign digitally at a mortgage close

The electronic signing of upfront disclosures has achieved widespread adoption in the mortgage industry. Closings, with the official signing of the final promissory note, are still commonly done in person and signed on paper.

A new partnership between Wolters Kluwer Compliance Solutions and Floify, a point-of-sale product for the mortgage industry owned by mortgage technology company Porch Group, Inc., should help change that and make digital closings in the consumer space more ubiquitous.

The companies are collaborating in a product integration that incorporates Wolters Kluwer's eOriginal® digital promissory note (eNote) technology into Floify's loan processing system. By doing so, Floify customers gain the ability to do eClosings, so they can use digital signatures rather than pen and paper.

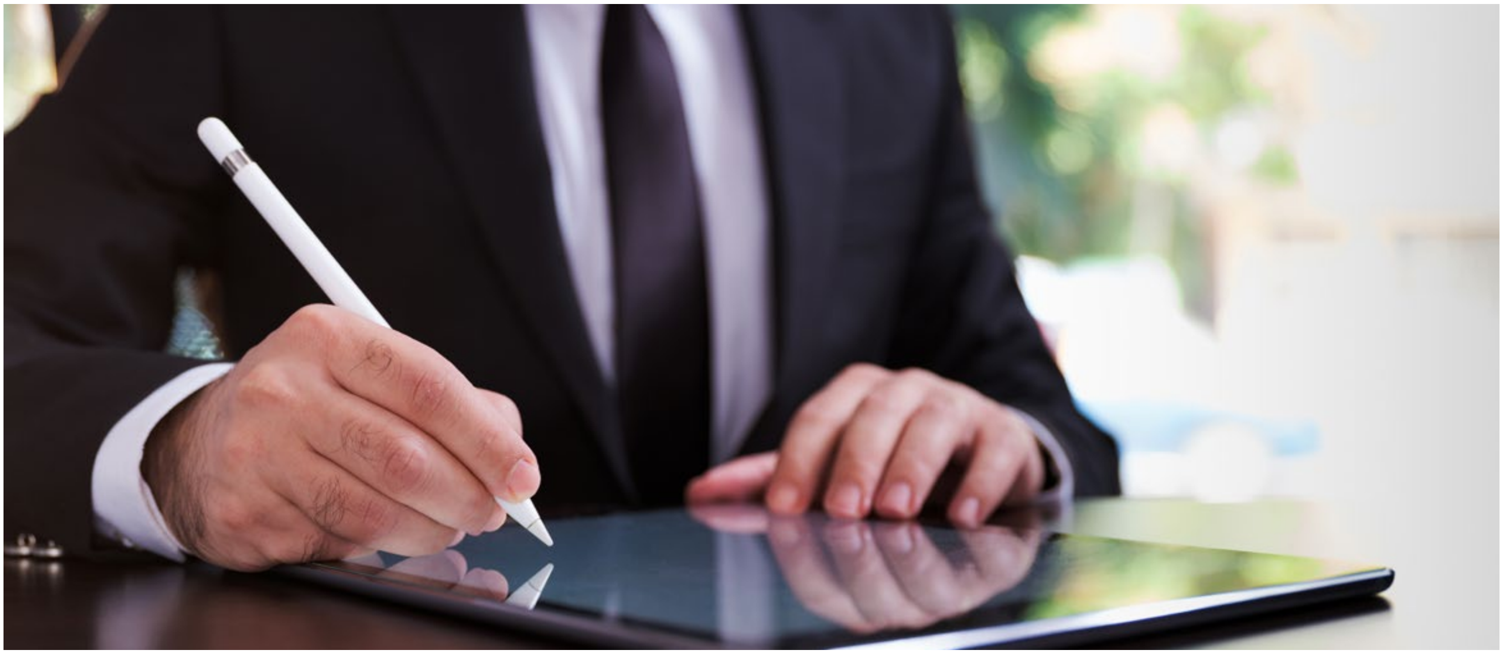
“This partnership is actually very specific about just one document,” said Simon Moir (pictured), Vice President, Banking Compliance Solutions for Wolters Kluwer Compliance Solutions.

“You might [sign] 200-plus pages of documents as part of [the mortgage process], but the most important document in that package is the promissory note … you borrowed this money and you promised to pay back this lender, and that's called the promissory note,” Moir said.

“This partnership with Floify is about being able to take what was once a paper promissory note and making it an electronic promissory note, or what we would call an eNote.”

That ability matters for a number of reasons. Electronic signature technology has been around for while, but, as Moir explained, many of these documents can be signed using digital signing tools on a normal PDF, with no need to know which of multiple copies that might exist is the original. For many documents, that approach works just fine. With the final mortgage document, the electronic promissory note, there's a difference.

“When you come to this electronic promissory note … you know which one is the original,” Moir explained. “If you think about a negotiable instrument, if you hold that piece of paper or you have that (signed) check, then that is the authority you need, right? You have the original [and you can] ask someone to pay for it. How can I do that in an electronic world? If you have a copy … who has the real promissory note? Our technology helps you create, store and assign that original electronic note to the right party.”



Dave Sims, Floify's CEO, said in prepared remarks that the arrangement will let it offer mortgage products "that reduce time and fees throughout the process."

Porch Group, an insurtech and software company focused on the home services industry, paid $76.5 million in cash and $10 million in Porch common stock for Colorado-based Floify in 2021. Floify focuses on helping mortgage companies and loan officers create a better customer experience during the mortgage and refinancing processes.

New uses

Wolters Kluwer obtained additional digital lending technologies, including its eNote technology, when it acquired eOriginal the company in 2020, a Maryland-based provider of cloud-based digital lending software founded in 1996. Moir, the acquired company's former chief product officer, said that uptake of the digital signature process was slow at first because not everyone in the banking system embraced it.

In a closing you have "the lender, the settlement agent, the borrower – this is a multi-party transaction," Moir said. "For it to be digital, you need to have a borrower who is comfortable or has access online to get documents. You have to have a lender who is able to create documents that can be electronically signed. You have to have a settlement agent, or even a person who is going out to do the closing ... [with] the ability to access or operate a [digital] system."

Moir noted the MERS registry, a platform that is a registry of all electronic promissory notes in the mortgage space. It indicated a slow take-up of eNote technology at first, he recalled.

From 2004 into 2017, fewer than 300,000 eNotes were signed and managed out of between 6 million and 7 million mortgage transactions annually. Over the last three years that has grown to about 1.5 million, Moir said.

According to Moir, business clients have used Wolters Kluwer's eNote/eVault technology well before the Floify arrangement, including Quicken, Wells Fargo, Fannie Mae and Ginnie Mae, among others.

The Floify integration is complete at this point, and is now in implementation phase, Moir said, with plans to go live with a customer shortly. Target customers include banks that handle mortgages, as well as independent mortgage bankers.

Simon Moir *is Vice President, Banking Compliance Solutions, Wolter Kluwer Compliance Solutions. he has overseen the growth and development of the segment's banking compliance product portfolio and its open digital lending platform and expert solutions ecosystem. Simon joined Wolters Kluwer following its acquisition of eOriginal, Inc in December 2020. At eOriginal he held a variety of leadership positions. Originally from New Zealand, Simon holds a Bachelor of Science in Chemistry from the University of Canterbury.*

Simon can be reached at
[Connect with Simon on LinkedIn]

Wolters Kluwer Expert Shares eVaulting Technology Insights

Key considerations including assessing business needs and digital readiness

As published in Small Might Mean Survival Digital Edition | Mortgage Banker Magazine | By **Kevin Wilzbach**

As mortgage markets become increasingly digital, most lenders, regardless of their lending strategy, will eventually need an eVaulting capability because eVaults are a requirement for moving electronic promissory notes, or eNotes, through the digital mortgage ecosystem. That's according to Wolters Kluwer Compliance Solutions, sharing its digital lending expertise in an article, “Three Steps Lenders Should Take When Selecting an eVault Provider."

“eVaults are an integral part of any end-to-end digital mortgage transformation. They enable lenders to originate and securely hold eNotes and accelerate capital market transactions," said Kevin Wilzbach, Director, Technology Product Management at Wolters Kluwer Compliance Solutions. “eVaults also support an enhanced customer experience for borrowers and streamline interactions with other participants—warehouse lenders, investors, servicers, etc.—within the mortgage ecosystem."

He pointed to some key considerations in selecting an eVault vendor, which starts with assessing one's business needs and the “digital readiness" of counterparties, understanding the elements of a successful implementation, and conducting due diligence on the experience and connectivity of potential eVault partners. The evaluation includes assessing a provider's ability to seamlessly interact with MERS®, the breadth and depth of its counterparty working relationships, and its participation in all MISMO® (Mortgage Industry Standards Maintenance Organization) groups, such as eMortgage, eDoc/eVault Interoperability, RON and SMARTDoc as a means of staying ahead of future requirements and an ability to work on different eVault platforms.

Wilzbach wrote that a common misperception of eVaults is that they are just for the storage of eNotes and other documents, including paper documents that have been wet-signed and uploaded into the eVault as part of a hybrid transaction. “But they also must be compliant, provide a comprehensive audit trail to track various activities and actions, be seamlessly integrated with the Mortgage Electronic Registry System (MERS) eRegistry, and have the scale and connectivity to enable capital market transactions."

“The true purpose of an eVault ... is to reliably establish the person or entity to whom the single, transferable record of the digital loan is assigned, issued or transferred," Wilzbach wrote. “It provides an immutable, tamper-proof eNote that financial institutions can rely on when they pledge, sell and securitize eNotes."

This capability, he said, is crucial today for capital market transactions. Fannie Mae and Freddie Mac both use eVaults and encourage eNote sales. Having an eVault is a requirement for delivering eNotes to these entitities—and an opportunity to increase capital market efficiencies. “Various types of lenders may experience different advantages to using eVaults. A portfolio lender, for example, might want to add an eVault to offer eClosings and eNotes that enhance their borrower experience and help them compete more effectively against national retail lenders," Wilzbach explains.

“As a critically important component in digital mortgage lending, it's not a matter of if lenders adopt eVault technology, but when and how," concluded Wilzbach. “And more importantly, how successful they are in selecting an eVault provider with a proven track record to deliver."

***Kevin Wilzbach** has over 30 years of marketing and sales experience in both B2B and B2C spaces. Prior to his position of Director of Product Management at Wolters Kluwer Compliance Solutions, he was Vice President of Product Management at eOriginal.*

Kevin can be reached at
Connect with Kevin on LinkedIn

Wolters Kluwer's Expert Insights

What are the building blocks of digital lending?

HousingWire recently sat down with Steve Meirink, Executive Vice President and General Manager, Compliance Solutions, Wolters Kluwer's Governance, Risk and Compliance Division, to discuss the impact of digital technology on mortgage and the future of digital lending in an era of accelerated innovation and digital transformation.

As published in HousingWire.com | By **Steve Meirink**

If you don't move forward on digital lending, more efficient competitors will take business away from you

What are the key factors and trends driving the adoption of digital lending? How has the COVID-19 pandemic contributed to this?

Steve Meirink: Digital lending is now a must-have for organizations that need to differentiate in the marketplace by moving faster with greater agility while at the same time reducing costs.

In addition, consumers expect better digital experiences—like what you get with Amazon or Uber. Companies that provide this kind of seamless user experience will move ahead and those that don't will fall behind. We saw this with the COVID-19 pandemic where the demand for contactless transactions took off—such as the 'tap to pay' feature for your smart credit card. In digital lending, this has led to the growing popularity of eClosings and remote online notarization (RON).

What are some of the core building blocks for digital lending?

Steve Meirink: I joined this industry as a Retail Mortgage Loan Officer growing to a Broker Owner in my local community and try to apply a simple concept we share with customers and prospects which is the idea of digital lending made simple. It starts with a document engine that provides the core inputs for a digital loan transaction—fully automated with warranted loan agreements and contracts. At Wolters Kluwer, our document engine is Expere®, which is fully integrated with loan origination systems (LOS) and other core lending systems.

Also important is an eClosing platform to accelerate and simplify complex loan agreements with workflow management to deliver a simple and intuitive closing experience for lenders, borrowers, and settlement agents. This is our ClosingCenter for digital mortgages.

An eVault or an authoritative copy is also needed to consolidate digital loans in one system and ensure digital asset certainty with full ownership and control of assets. This is our OmniVault.

Organizations also need digital asset certainty based on an immutable history and digital chain of custody for all digital financial assets. The idea is that only one digital original exists and is legally transferable and enforceable. When you see Digital Original® in the financial services space, you can have confidence that Wolters Kluwer is in the background enabling that to happen.

Finally, analytics and reporting tools are needed to analyze risk and ensure compliance through information sharing and accurate reporting. This is our Wiz® technology, which delivers data-driven insights and improves decision-making.

For those considering a digital lending platform today, what are the key benefits they can expect? And for those who wait, what are the risks?

Steve Meirink: A digital lending platform lowers the classic "barriers to entry." Companies can adopt new technology faster while increasing efficiency, reducing cost, and growing margin and profitability. And most importantly: they can deliver better customer experiences.

The risks of not moving forward? If you don't, more efficient competitors will "eat your lunch" and take business away. Keep in mind that decisions made today will impact your business for many years to come. It's important to leverage the expertise and experience of trusted advisors who have been working in this field since the dawn of digital lending almost 20 years ago. Our team of experts enabled, along with other industry partners, the first digital lending transaction in many of the industries that we serve today.

Looking forward, what does digital lending look like in the next few years? What are some significant trends and shifts we will see?

Steve Meirink: We speak to customers and prospects about next-generation digital loan compliance management, which today means a fully digital platform with robust loan compliance. Increasingly, businesses will focus on what can be achieved by shifting from manual to automated processes in terms of greater economies of scale and cost efficiencies.

This brings with it a dynamic, enhanced, end-to-end user experience—and all the benefits of digital technology for quick response and action.

A fully digital lending platform solution offers not only powerful tools aligned with key business processes but also analytics to ensure broader compliance and a warranted asset/portfolio matched with end-to-end, digital-asset certainty. Find more information here.

Steve Meirink *is the Executive Vice President and General Manager of Wolters Kluwer's Governance, Risk & Compliance (GRC) division's Compliance Solutions business unit. He leads the financial services portfolio of businesses with full responsibility for P&L, GTM, Technology, Service, Operations, & Strategy. Wolters Kluwer Compliance Solutions is a recognized leader in helping financial institutions, brokerage firms, and insurers make confident and compliant decisions to grow their business.*

Steve can be reached at
Connect with Steve on LinkedIn

Wolters Kluwer's Expert Insights

Datalytics®: Trusted data for the third generation of digital lending

By **Kristen Girard**

AI and machine learning eliminate these inconsistencies and give you the highest levels of digital data

Over the last few years, financial institutions have experienced three waves of digital transformation—with each wave driving fundamental process and technology changes. The first wave was customer experience-driven, as borrowers wanted their manual lending transactions to mirror their online retail transactions. The second wave hit during the global pandemic, creating an urgency for lenders to fast-track their digital transformation. As the third wave of digitization emerges, technology is now a competitive necessity. Financial services organizations and lenders proactively embracing digitization will ride the wave to improved compliance and risk mitigation, lower origination costs, more efficient and improved workstreams, greater consumer engagement, and an enhanced customer experience.

Successful, efficient, end-to-end digital transactions require a fully automated and expedited lending process. Technical barriers have made this goal impossible for years—from the limited availability of a complete set of eSignable documents to highly variable levels of data accuracy and compliance in documents generated by today's eOrigination platforms. However, intelligent, next-generation technologies have emerged that address the persistent problem of digital data quality.

Kristen Girard is the Associate Director of Technology Product Management at Wolters Kluwer. She brings over 10 years of professional expertise to her role, including a proven track record of driving product vision and strategy to solve market problems in digital lending. Kristen shares her perspectives on the emergence of the third wave of digitization and how leveraging Datalytics, powered by artificial intelligence (AI) and machine learning, can deliver significant efficiencies and pave the way for true end-to-end digital transactions.

The generations of digital lending

First generation:
- Focus on loan origination
- Use of available data online to determine creditworthiness
- Improved access to credit for consumers

Second generation:
- Focus on execution and customer experience
- Technologies for RON and eSignature
- Self-service workflows with tracking for full compliance

Third generation:
- Focus on platforms that support compliant, seamless end-to-end loan processes
- Ability to move out of sequence with centralized data
- Smoother, faster processes—with no need to reinvent the wheel

Q: What key digital lending business processes does Datalytics support?

Kristen: Most financial service organizations and lenders are familiar with, and likely already using, eVault technology to secure the final, transferable, authoritative copies of their legal documents. Datalytics is an extension of your eVault, enabling you to intelligently extract data directly from the live, authoritative, and ancillary documents in the eVault, validate and certify it, and move it downstream as trusted, accurate data.

AI and machine learning are game changers for the financial services industry because they vastly improve the quality and accuracy of digital data captured from loan origination documents. Existing methods of extracting and digitalizing this data are slow, cumbersome, costly, and error-prone. In some cases, the number of inconsistencies between paperwork and the digital data extracted is staggering.

AI and machine learning eliminate these inconsistencies and give you the highest levels of digital data accuracy. The accuracy that Wolters Kluwer provides is a digital disruptor for every other technology on the market today because nothing else even comes close. This gives lenders a tremendous advantage because they now have a single solution for dealing with paper documents that can easily integrate into their digital lending lifecycle management processes. Using their eVault, the authoritative system of record, as a trusted source for accurate digital data, lenders can truly have a seamless, end-to-end digital lending process. Datalytics also gives lenders confidence that the validated data accurately represents the data contained in the legal agreement, allowing them to consume it into automated processes without the need for manual quality control. Financial institutions gain visibility across the portfolio, transparency in lifecycle management and certified data pools, and insights for investors and rating agencies—all of which enable quicker access into the secondary market.

Business processes supported by datalytics

Figure 1: Business processes supported by Datalytics

Q: How does Datalytics eliminate data quality issues?

Kristen: To date, origination platforms have primarily relied on legacy platforms that struggle with data consistency and accuracy, as well as form generators that fail to map forms accurately, compliantly, and with consistent disclosures to PDF templates. As a result, even users of industry-leading systems have had to deal with high levels of data inaccuracy. And employing staff to cross-check original paperwork against digital data can increase costs and add days to loan decisions and the funding process.

Leveraging technology innovations, such as AI and machine learning, essentially eliminates data quality issues. Machine learning trains a machine on a document to recognize key data points and leverage additional business logic (such as "if-then" statements) and data modeling. It then uses contextual learning to verify data exactness and completeness. Lenders no longer need human eyeballs to make the comparison. Machine learning will do it for them and assign a level of confidence.

Q: How does Datalytics support intelligent digital data capture and validation? How does data science augment AI and machine learning to optimize the data within the solution?

Kristen: Today, lenders need a human to pull up all these document images, compare them to information on the contract, and verify that the name, address, and other details on the supporting documents are the exact same as what's on the contract. Datalytics eliminates the need to have people manually key in data, which adds risk and is time-consuming and prone to human error. Instead, Datalytics uses machine learning to intelligently capture and validate data with higher efficiency and greater accuracy. Machine learning ensures that your data is certified and compliant.

Specifically, once a contract is executed and eVaulted, it becomes the only authoritative copy. The contract is then run through an intelligent data extraction service executed by data scientists at Wolters Kluwer, assigned a level of confidence using smart technologies, and passed back to the eVault for safekeeping.

Unlike traditional optical character recognition (OCR) services, Wolters Kluwer's eOriginal uses AI-enabled contextual machine learning to understand the asset type and the data itself to validate that it is what we say it is. Our machine learning models continuously learn and become more intelligent over time. With every loan document they process, the models refine their understanding of the data and become more efficient.

Datalytics can be treated as authoritative data, like an eVaulted document. The data is then tamper-sealed, encrypted, stored, and passed back to the lender in an easily consumed format for their use, whether it's making loan decisions, applying analytics and business rules to automate decisions, running reports, generating audit trails, or feeding data into a workflow or another system.

Q: How does a financial institution take advantage of this solution, and what key considerations should be factored in?

Kristen: The big question every lender should ask is, "How and where can Datalytics be used in our business?" We recommend the following five actions you can take to get started and ensure your success:

- Evaluate current workflows and processes to identify manual workflows and bottlenecks
- Identify where access to data is needed and any additional participants that rely on data, such as investors and rating agencies
- Inventory audit and compliance standards, including potential risk
- Prioritize where to focus your investment to realize your most significant potential return on investment

Wolters Kluwer also offers quick, scalable solutions to transition to digital with a full solution for onboarding paper contracts.

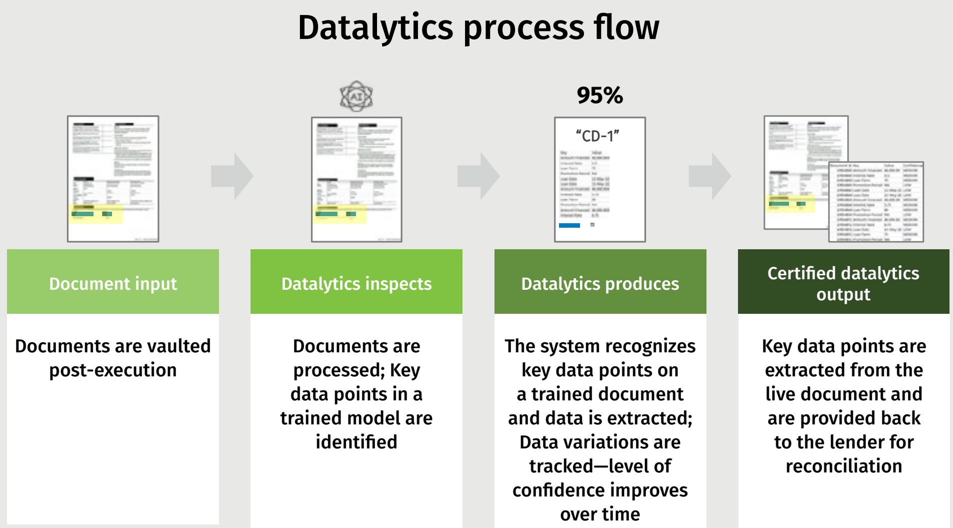


Figure 2: Datalytics business process flow

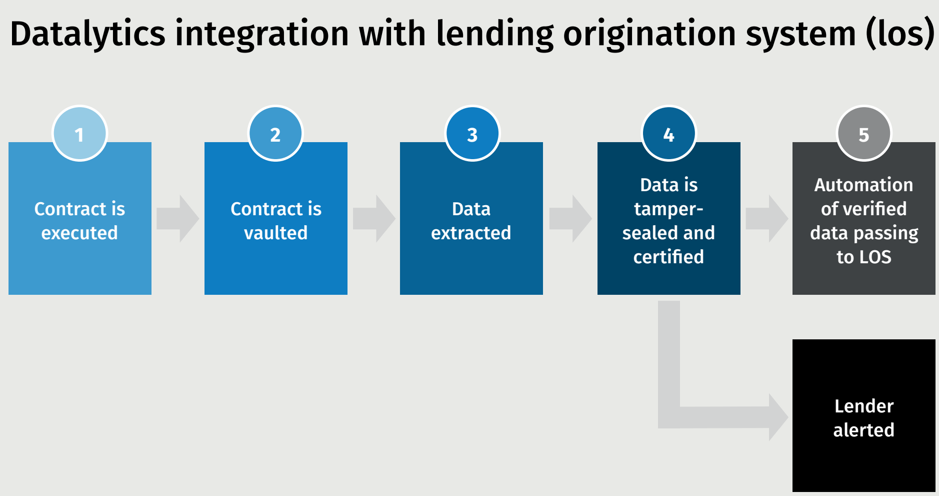


Figure 3: Datalytics integration with lending origination system (LOS)

Q: Where are Datalytics trending for the future?

Kristen: As Datalytics evolve, users can apply AI and machine learning to a trained model to introduce document understanding and business logic. This will enable automated loan decisions and approvals. Looking ahead, we anticipate that funding is the next frontier Datalytics will transform. To fund deals, lenders also need to verify the existence of all required ancillary documents related to a contract and the data on these documents. For example, if a gap policy was sold and financed on the retail installment agreement, the lender must verify that they have the gap policy document. With the broad adoption of this disruptive machine learning technology, we anticipate accelerated innovation in lending and related processes across the financial services industry. This will be a win-win for all.

Learn more about Datalytics and how it can fit into your current and future IT and solutions landscape. Wolters Kluwer is the leading provider of digital loan compliance technology and services, from origination to monetization. We offer the industry's most trusted solutions to navigate the ever-changing regulatory compliance landscape. For more information on world-class compliance expertise, solutions, and services from Wolters Kluwer and our partners, please visit https://www.wolterskluwer.com/en/compliance.

Kristen Girard *is the Associate Director of Technology Product Management Associate Director for Wolters Kluwer. Kristen has over 10 years of experience as a product management leader, excelling at driving product vision and strategy to solve market problems in digital lending.*

Kristen can be reached at
Connect with Kristen on LinkedIn

Fair lending: Know the risk

Fair lending programs should be robust enough to detect and prevent fair lending risk in the lending cycle and within specific transactions. Fortify your compliance program with advisory services and technology solutions from Wolters Kluwer.

Advisory Services

- Compliance Management System (CMS) Review
- Fair Lending Risk Review
- Fair Lending Risk Assessment
- Redlining Review and Integrated Risk Review
- Fair and Responsible Banking Program Development
- Fair Lending Exam Preparation
- Staff and Board Fair Lending Regulatory Training
- UDAAP Risk Assessment
- Complaint Management Program Development and Review

Wiz Suite of Technology Solutions

- Fair Lending Risk Analysis
- Redlining and Marketing Analysis
- Disparity Analysis
- Underwriting & Pricing Decision Analysis
- Underwriting & Pricing Outlier's Analysis
- Comparative File (Matched Pair) Analysis
- Data Quality/Integrity Check
- Model Validation Support

For more information, visit www.wolterskluwerfs.com or call 800-261-311.

Wolters Kluwer's Expert Insights

Proactively addressing key challenges and enabling success for the Chief Compliance Officer

An executive discussion with Elaine F. Duffus, Senior Specialized Consultant for Compliance Solutions at Wolters Kluwer

By **Elaine F. Duffus**

What can CCOs do to bring more to the business? Find out in this exclusive Q&A.

Chief Compliance Officers (CCOs) in the financial services industry face a multitude of challenges in the fast-paced, ever-evolving world of regulatory compliance. The key to success in this environment is understanding and overcoming obstacles and ensuring their institution meets or exceeds applicable regulatory compliance obligations and internal standards.
With so much volatility in the financial services industry, ensuring your institution adheres to regulatory requirements is no small task. Couple this with the reality of limited human and technological resources, and you begin to understand the challenges today's CCOs navigate daily.

Elaine F. Duffus is a Senior Specialized Consultant for Compliance Solutions at Wolters Kluwer. She brings over 20 years of professional expertise to her role, including experience as a Chief Compliance Officer in the insurance, securities, and banking industries. Elaine innately understands the challenges CCOs encounter today, and with this insight, she shares her perspectives and best practices for enabling success.

Q: What are the key characteristics of a good compliance leader?

Elaine: First, a compliance leader must be empowered to act. This means they receive the human resources, technology, and organizational support they need from those with the power and the purse strings. Whether this support comes from the Compliance Committee, the Board of Directors, or elsewhere, this empowerment allows the CCO to act with a clear vision and multi-year compliance strategy to positively impact the institution.

Second, a compliance leader must embrace creativity and innovative thinking around the use of technology, data, and analytics that will enhance and enrich an institution's compliance program.

An example might be when an institution wants to bring a new product or service to market, and the CCO has concerns about its negative impact on the institution or its customers. Instead of voicing their concerns without an alternate path for the business to pursue the new product or service, an informed CCO would use data, analytics, technology, and any other available, relevant information to support the case for proceeding, but in a different way—one that ensures the institution's compliance obligations are adhered to.

Third, a successful compliance leader can see the business' point of view, understand its needs, and then balance that thinking against managing regulatory obligations. This empathy and visibility are critical to developing a sound compliance program that others in your organization will follow. If a CCO can't get that buy-in or support, there is a strong possibility that their perspective may be too one-sided.

Keep asking “why” until you understand the business’ motivation to do or not do something.

Another tip in support of a strong culture of compliance is to communicate frequently with senior leadership. Keep them apprised of the day-to-day compliance issues facing your institution. Also, take note of the evolving views of legislators, regulators, and the public that may impact your business model. And take the time to let them know that their compliance budget dollars are well-spent. For example, if a material enforcement action is issued to a similarly situated institution, prepare a communication to inform senior leadership about how the resources they provide help ensure that the proper policies, procedures, training, or other controls are in place to avoid such an outcome at your institution.

In summary, the key characteristics of a good compliance leader are the ability to empathize with the business, communicate effectively with leadership, and ensure that everyone on the compliance team feels supported and a part of, not apart from, the rest of the organization.

Q: What are the major challenges faced by the CCO in today’s fast-paced, ever-changing financial services environment?

Elaine: In my experience, there are two significant challenges. One is how to create a culture of compliance at your institution, and the other is how to ensure your compliance program captures and addresses the laws, rules, regulations, and guidance that apply to your institution.

Creating and nurturing a culture of compliance means that your communications, training, and other touchpoints with the business are meaningful. That helps participants understand not only their legal or regulatory obligations, but their ethical obligations to always do the right thing. This includes feeling empowered to question when someone else does not act ethically. A culture of compliance will fail if not supported up and down the leadership chain.

Ensuring your compliance program captures and addresses the laws, rules, regulations, and guidance that apply means that the institution has a solid regulatory change management process. What does that look like? Consider your institution’s business model, products, services, locations, and customers. For example, is your institution a community bank with standard product and service offerings or a complex global investment bank with exposure across multiple jurisdictions? Once you understand this, determine the regulatory bodies that govern the activities undertaken. For each regulatory body, maintain documentation of the laws, rules, regulations, or guidance they supervise and note which apply to your institution’s business model. This list becomes your compliance library or inventory.

Concurrent with creating your inventory, there must be a process for receiving and processing regulatory updates issued by the regulatory bodies that supervise your activities. As material regulatory updates are received, map them to the inventory for a holistic view of their potential impact on the institution. Horizon scanning is another key aspect of the regulatory change process, including reviewing new releases and regulatory changes across industry associations, regulatory agencies, law firms, and more to gain insight into what may be coming in the weeks and months ahead.

Q: How do regulatory technology (RegTech) solutions enable compliance leaders to be successful at achieving their goals?

Elaine: RegTech solutions have become a critical component in today's compliance department, providing institutions with the necessary tools to manage regulatory risk. As compliance burdens increase, cutting-edge technologies, such as artificial intelligence and machine learning-enabled solutions, can drive better insights and outcomes.

RegTech solutions also permit CCOs to deploy human resources more strategically. However, there are two critical things to remember about technology. One, it cannot involve a "black box." CCOs must be able to explain how the technology they rely on works to regulators and senior leadership. Second, AI-driven solutions do not always get it right. A human expert review of AI-derived data is preferred when available. For RegTech solutions that manage regulatory change, we call this "expert-augmented intelligence." It is a key growth and focus area.

Another facet of RegTech solutions is the technology needed to make them work. CCOs should strongly consider requiring flexible technology for solutions, such as your regulatory content data feed, to ensure continuity as your institution may change GRC platforms. Successful obligation management solutions enable your institution to reduce regulatory obligations into a more manageable number. Ensure that your RegTech solution providers can accommodate all new regulatory changes and offer support across multiple states and territories. This should include an extensive legal library and a mix of expertise and AI to aggregate and analyze requirements across state laws and jurisdictions.

Regulators use technology in many aspects of their oversight obligations and expect institutions to do the same. When implemented effectively as part of a broader Compliance Program Management (CPM) process, RegTech solutions are invaluable to help control compliance risk, including the firehose of regulatory changes that compliance leaders must manage daily. In sum, leveraging RegTech or other compliance technology to ensure success in an increasingly complex and regulated landscape is no longer an option.

Q: Elaine, you have been a Chief Compliance Officer and offer significant experience. Based upon your tenure, what is the best advice you can offer compliance leaders?

Elaine: My best advice is to ensure that you thoroughly understand your institution's business model. This includes the products, distribution channels, services, compensation, locations, types of consumers—all of it. A fully informed CCO is a much more valuable partner to the business, can see alternative ways to address an issue, and is more often invited to the table to develop new strategies or grow the institution.

For more information on compliance solutions for the Chief Compliance Officer and their team, visit our portfolio of compliance solutions and services that ensure adherence to ever-changing regulatory obligations, manage risk, increase efficiency, and produce better business outcomes.

Elaine F. Duffus, *CSCP, CFCS, FLMI, JD, is a Senior Specialized Consultant with the Financial Services Compliance Program Management solutions team at Wolters Kluwer. She brings more than 20 years of professional expertise to her role, including several as Chief Compliance Officer in the insurance, securities, and banking industries.*

Elaine can be reached at
Connect with Elaine on LinkedIn