Crowe Horwath

May 2017

Data Analytics and Compliance: Why Big Data Is a Big Deal

An article by Clayton Mitchell, CAMS, CFIRS, and Paul Osborne, CPA, AMLP, CAMS

Data seemingly is everywhere. It is the engine behind areas as diverse as consumer product development and entertainment programming to healthcare and human resource management.

A force this pervasive was bound to catch the eye of regulators – especially financial institution regulators.

Data provides a treasure trove of information on customers, products, and services that financial institutions can collect and analyze. The amount of data available has grown with the spread of automation and introduction of artificial intelligence. But while most banks have used this information in their business decision-making, many have been slow to put it to work for compliance.

Those that have lagged behind could soon suffer repercussions in their examinations. Regulators' expectations for compliance efforts are increasingly data-driven, particularly in regard to consumer protection matters, including unfair, deceptive, or abusive acts or practices (UDAAP) and fair lending.

Regulators realize that financial institutions have significant amounts of data available that would facilitate identifying compliance risks, completing analyses, and executing remediation. If banks do not know what to look for within this data, it can be overwhelming without providing additional value. That's where data analytics come in – data analytics hold the key to identifying and monitoring compliance risk effectively.

The Case for Data Analytics in Compliance

Despite the integration of data analytics into business decision-making, some banks remain skeptical or naive about unleashing these capabilities for compliance purposes. They might not grasp the range of benefits data analytics can bring to this essential activity.

For starters, data analytics empower proactive and ongoing compliance efforts. Rather than waiting for compliance issues to emerge through periodic testing or through risk-based internal audit activities, a bank can uncover potential problems before they fully hatch and then take the steps necessary to correct the problems before they come to regulators' attention. Data analytics also:

- Expand the breadth and depth of the rules and regulations banks can examine
- Enable the evaluation of larger populations rather than only small samples of consumers or transactions
- Help banks make better decisions about their use of risk models
- Enhance processes to meet regulators' data reporting requirements (especially those calling for standardization of data, including impending *Home Mortgage Disclosure Act* (HDMA) enhanced reporting)
- Help identify systemic compliance risk factors and align remediation efforts

Nonetheless, the data analytics picture is not all rosy. For example, a bank can find it expensive to collect or normalize the applicable data in the requisite format. Establishing programs to do so will require upfront investment. Banks will need staff with cross-functional expertise in compliance or data analytics, and these professionals must be able to communicate effectively. Such expertise can be scarce and, therefore, costly. In addition, the need for ongoing governance and changes to adapt to evolving regulatory challenges can drain resources. A bank might well engage in internal debate over the costs and benefits of using data analytics experts for risk management versus deploying that money to build the business.

Ultimately, though, if regulators are using advanced data analytics methods and a financial institution is not, that institution is creating significant risk for itself. And there is no doubt that regulators are using analytics to drive risk assessments across banks, identify industry trends and patterns, perform deeper-dive examinations, identify outlying institutions, and conduct more robust supervision.

Data Risk Management Activities

To confirm that data is reliable for purposes of compliance analytics, financial institutions need several types of risk management activities that support strong data governance:

Data sourcing. First and foremost, banks must know which data to monitor for compliance and where and how to obtain it. Collection can prove challenging in today's banking environment because many institutions have undergone extensive merger activity and might now have disparate information systems in place, some of which may still exist in

paper form. As a result, banks can have similar yet different data stored in different places or have issues modernizing the information that they have.

Data management. Data management – which works simultaneously with data sourcing – refers to the governance and use of data. Proper data management is necessary to make certain that the data is handled appropriately and that it can be used for different purposes. The data management process should identify the data owners and stewards who are responsible for ensuring that changes to any source application are communicated to all users of that information and for developing and understanding any potential effects of the changes. Doing so prevents the changes from affecting the end-user community. This process also ensures the same data is used across the organization for a common purpose and prevents inconsistent information from being shared with regulators.

Data quality. The saying "garbage in, garbage out" is trite because it's true. Data is of no use unless it's consistent, accurate, and complete.

Data validation. Banks must have independent validation of their design and development, input processing, implementation, output and use, and performance to verify that the controls related to their compliance risk management activities are working correctly.

Data lineage. Data lineage considers the life cycle of data, including its origins and where it moves over time. It's essential to understand what happens to data as it travels through diverse processes. Clear lineage makes it easier to trace errors back to the breakdown point and gives banks confidence that the key risk indicators (KRIs) they have selected to identify potential areas of vulnerability are providing accurate guidance for further investigation. Regulators now require data lineages from the organizations they are responsible for regulating.

Prerequisites to Successful Compliance Data Analytics

With their increasing reliance on systems and the integrity of data, financial institutions can run into systemic risk factors. Not surprisingly, those factors have drawn intensified regulator attention recently. To successfully counter these risks in its compliance reporting, a bank requires compliance knowledge, which drives the design and use of compliance analytics, which, in turn, drives the need for the acquisition of certain compliance data.

Compliance knowledge. A bank cannot properly define KRIs without sufficient knowledge of the various compliance requirements and a defined risk appetite and risk tolerance for overall compliance and for compliance with specific consumer compliance regulations. Many banks, though, take a reactive approach: waiting until issues arise to think about data collection. The better approach is to develop a formal policy that spells out the KRIs that should be monitored on a continuing basis – and when the red flag should be raised and to whom.

Compliance knowledge can reduce the odds that warning signs are overlooked. For example, significant overdraft fees generally are not regarded through the prism of compliance, but they can point to the regulatory risk of noncompliance with *Electronic Fund Transfer Act* Regulation E overdraft protection rules. Similarly, an uptick in the number of disputes about electronic fund transfers (EFTs) could indicate an external risk (for example, that a hacker has stolen card information) or an internal risk (for example, the failure to provide clear and conspicuous disclosures to customers). Without appropriate compliance knowledge and without viewing available data through the appropriate lens, these red flags could go unheeded.

Compliance analytics. Armed with the necessary compliance knowledge, a bank can apply analytics to its data. It can use multiple sets of data – by themselves or as part of regression or other statistical methods – to identify patterns or anomalies in their data that do not adhere to defined KRIs requiring further investigation and possibly remediation.

Banks must also take care to avoid model bias when creating their analytic models. For example, complexity does not necessarily reduce risk; a simple model might be more effective for many purposes. The mere existence of fee charges does not mean a bank is somehow failing in its consumer protection practices. And not every regression is valuable, particularly if the items being compared are not actually alike.

Compliance data. Of course, effective risk compliance analytics will require substantial data.

The sources of this critical data can include:

- Bank-specific complaints and disputes
- Transaction data for compliance and timing requirements
- Customer data
- Socioeconomic factors and other available information, such as proxy methods

- Census data to impute demographic information and potential prohibited basis factors
- Market or publicly available information (for example, HMDA data and information from the Consumer Financial Protection Bureau's consumer complaint database).
- Social Security Administration name, gender, and ethnicity data

It's important to recognize that the necessary data does not reside in a single location – pulling it together will require a good amount of time, effort, and possibly capital, at least initially.

Areas to Monitor

The following areas are ripe for compliance monitoring through the use of data analytics:

Consumer protection/UDAAP. Data analytics can help banks monitor customer outcomes – specifically, how actual outcomes compare with those expected. For example, if a bank budgeted for $1 million in overdraft fee income but actually booked $5 million, or experiences greater than expected first payment defaults and delinquencies, analytics can tip the bank off to the need for a root cause analysis and determination of the underlying issues.

Analytics also can play a role in detecting disparities in marketing to certain groups. If, for example, a bank's distribution model is online only, it could unintentionally have an impact on the elderly and others who lack internet access, such as low-income populations.

Regulators have stressed consumer complaint investigation and response as core components in the administration of UDAAP and consumer compliance programs, making responsiveness to consumer grievances that are separate from the formal complaint process (for example, verbal complaints made to branch employees) another area for monitoring. Banks must respond to these grievances both on a tactical level, addressing the granular grievances themselves, and more holistically, looking at their meaning as a whole to identify, understand, and create an action plan regarding the identified risks.

Third-party risk factors should be monitored, too. When a financial institution partners with a third party, such as a financial technology company that develops and implements underwriting models, regulators will hold the bank responsible for any breaches of the data being passed back and forth.

Managing inherent risk factors adequately also requires monitoring. Some questions that may be asked include: Do the underwriting or pricing models raise any issues about how they were constructed? Do factors exist that would violate fair lending or UDAAP rules?

Data analytics also can help banks develop UDAAP dashboards. Dashboards give the board of directors and senior management the appropriate amount of high-level detail (versus complaint-by-complaint data) to identify UDAAP risks and make strategic business decisions.

Information asymmetry and clarity of disclosures. Issues related to the adequacy of information disclosures to consumers are coming under increased regulatory scrutiny. Banks should be monitoring the level of clarity and consumer understanding of fees, penalties, annual percentage rates, and loan costs to confirm that average consumers have the necessary knowledge about their financial products.

Risk of consumer fraud or abuse. Historically, consumer fraud and abuse have not been considered compliance issues, but they are rapidly becoming enmeshed in that realm. For example, a distributed denial of service attack on a bank could block a customer's access to his or her paycheck or close down automatic online bill payments, leading to late fees or worse for customers. Denial of service would have clear compliance implications and thus requires monitoring.

It's Not Just for the Big Banks

Data analytics does not affect only big banks; it is trickling down to midsized and community banks as well as to other types of nonbank financial institutions faster than some might realize. Every financial institution needs to know the answers even before regulators ask the questions, and data analytics can help make it easier for banks of all sizes to have the confidence to do so.

Learn More

Clayton Mitchell
Principal
+1 317 208 2438
clayton.mitchell@crowehorwath.com

Paul Osborne
Partner
+1 317 706 2601
paul.osborne@crowehorwath.com

crowehorwath.com

This article was originally published in the May/June 2017 issue of ABA Bank Compliance.