AD ACCESSDATA®

Compliance Officers at UK Financial Institutions Leverage Technology for Faster Response to Regulatory Investigations

The business practices of companies in the UK financial industry are under increasing scrutiny. European and American regulators have handed down large fines to more than 10 banks and brokerages for their roles in rigging the prices of financial benchmarks such as LIBOR and Euribor. Banks in the UK have also been hit with significant financial penalties for misleading customers into using their systems to trade currencies and for trying to manipulate the spot foreign exchange (forex) trading market.

One key new set of rules for professionals in UK financial institutions is the Market Abuse Regulation (MAR), which creates an updated regulatory regime for market abuse, establishing new offences and making it easier for government agencies to enforce compliance. MAR defines activities that now constitute market manipulation and insider dealing, providing a variety of specific examples, and presenting a list of indicators relating to false and misleading signals and price securing.

"

It's more common now for an organisation to be served with a regulator's demand to produce internal evidence in response to an enquiry ... and to do so on very short notice, sometimes as little as 48 hours.

Meanwhile, a new regime of data security regulations has gone into effect in recent years and forced UK compliance managers to take note. The updated Markets in Financial Instruments Directive (MiFID II) provides a list of areas where new compliance steps have to be taken by companies, ranging from voice recording to collection of trade data. The new Senior Managers Regime places compliance officers under greater pressure when they need to access sensitive data inside their own organisations. And of course, the General Data Protection Regulation (GDPR) contains all sorts of rules to govern the way personal data is protected within the EU and is exported beyond the EU's boundaries.

This rising regulatory pressure on UK financial institutions has resulted in a new compliance landscape. It's more common now for an organisation to be served with a regulator's demand to produce internal evidence in response to an enquiry … and to do so on very short notice, sometimes as little as 48 hours.

Given the realities of the information age in which we now live, this evidence—typically, correspondence between company executives and other corporate documents—consists of electronic data that resides on email servers and other data repositories. So how can corporate executives meet these pressure-packed compliance obligations to review vast troves of electronic data and produce responsive evidence under seemingly impossible turnaround deadlines?

components of that model show up in the UK as well. But for now, there are a few key steps in the e-discovery workflow that are important for UK corporate teams to understand in order to better meet their compliance obligations in response to regulatory enquiries.

Collection

Collection is a crucial part of the e-discovery process and corporate teams should leverage the power of software tools to quickly gather the universe of potentially relevant data from their various information systems. For example, the right e-discovery software products can ensure data is not being altered, dropped or missed during collection.

> **UK organisations are finding a secret weapon at their disposal: the use of electronic discovery (or e-discovery) software in order to deal with huge amounts of data and to extract relevant information.**

Electronic Discovery

UK organisations are finding a secret weapon at their disposal to comply with these sorts of data-intensive regulatory investigations: the use of electronic discovery (or e-discovery) software in order to deal with huge amounts of data and to extract relevant information.

Electronic discovery software collects, extracts and organises the data from all kind of servers and devices. Importantly, these tools allow in-house teams to discreetly conduct an e-discovery project—collect sensitive data, search for the responsive evidence needed and produce it to the regulators—without involving too many internal or external professionals who might not need to know about the enquiry that is underway.

Some organisations actually use three or four different products throughout the e-discovery workflow, which requires the data to move from one tool to the next. But many UK corporate executives have discovered the benefits of cost-efficiency and risk management that can be realised by using a single software platform to manage the entire spectrum of evidence collection, processing, review and production.

There is a comprehensive model that is commonly used to support e-discovery requirements in the complex commercial litigation that is prevalent in the U.S. and we're increasingly seeing more

While certainly not a requirement, forensic data collection capabilities are especially valuable in an e-discovery software solution. Forensic collection has important advantages, as well as heightened defensibility, including the ability to audit the collection and the ability to collect deleted files. In other words, an organisation that uses an e-discovery software tool with forensic collection capability not only chooses the strongest level of collection stability, but also shows regulators that it's at the front of a developing trend in compliance.

Processing

The processing phase is the real workhorse of any good e-discovery software tool. Within this phase, all data that was collected previously gets extracted and turned into information that can be culled down for greater relevance. As such, speed and accuracy are at a premium and the ideal software solution should be one that can easily and affordably scale using existing hardware to achieve fast processing speeds.

As always, the best advice is to run a thorough proof of concept test with your own sample data set and have a full understanding of the service level objectives when responding to a regulatory enquiry. The single criterion that varies the most across e-discovery vendors is accuracy, so make sure you're using a tool that has a proven track record for not only speed and culling rates, but also thoroughness and accuracy of its processing engine.

Analysis

The analysis phase of the e-discovery process entails taking the large and unorganised set of data from the processing phase to determine what electronic evidence you have that will be responsive to the regulatory demand you received. The best e-discovery software tools help you get this done quickly by categorizing, refining and bucketing data.

The most well-known functions are keyword searches and culling. All software applications and support processes should have an efficient and effective method for using keywords to analyse and reduce the subject corpus of data down to a manageable subset. In addition, your software should be able to quantify and present which documents did and did not meet your search criteria. These reports and metrics are critical input to note as they can influence whether or not you'll need to perform additional collections as the investigation develops. Reporting can also help to quickly determine if chronological or conceptual gaps exist in the current data set.

Production

Production completes the arc of the e-discovery process. The way data gets out of a system is a key part of the production process and you should be able to export it from the system in various formats without incurring an additional expense or using a third-party application.

Production includes much more than just printing documents out or emailing a batch file to the government investigative team. For example, today's productions come in many formats and some may never see paper, so your e-discovery software has to be capable of handling not only the traditional production duties of redacting, printing and numbering, but also be able to produce data in its many formats and iterations. Having said that, the UK and EU regulatory worlds are far from giving up on paper, so your software tool should also make it easy to click and print.

Conclusion

The use of e-discovery software has been common among American lawyers for more than a decade now as it's the only realistic way to comply with U.S. litigation rules when trying to deal with huge amounts of data and to extract relevant information. However, this same technology is increasingly becoming commonplace in the UK as a way for making it easier to organise and access data involved in time-sensitive compliance matters.

There is no industry in the UK under more intense regulatory scrutiny at the moment than the financial markets. By leveraging the power of e-discovery software tools, corporate executives in the financial industry can empower themselves to discreetly collect, process, analyse and produce responsive electronic evidence to regulators under short deadlines.

AD ACCESSDATA®

AccessData Group has pioneered digital forensics and e-discovery software development for more than 25 years. Over that time, the company has grown to provide both stand-alone and enterprise-class solutions that can synergistically work together to enable both criminal and civil e-discovery of any kind, including digital investigations, computer forensics, legal review, compliance, auditing and information assurance. More than 130,000 customers in law enforcement, government agencies, corporations and law firms around the world rely on AccessData® software solutions, and its premier digital investigations products and services. AccessData Group is also a leading provider of digital forensics training and certification, with its AccessData Certified Examiner® (ACE®) and Mobile Phone Examiner Certification AME programs. For more information, please go to www.accessdata.com.

Global Headquarters

+1 801 377 5410
588 West 300 South
Lindon, Utah

North American Sales

+1 800 574 5199
Fax: +1 801 765 4370
sales@accessdata.com

International Sales

+44 20 7010 7800
internationalsales@accessdata.com

LEARN MORE →

www.AccessData.com