Autonomy

Audio governance and COBS 11.8 – what does it actually mean and how do firms comply?

Financial services firms have no shortage of regulatory obligations with which they must comply. Each year brings greater scrutiny by regulators and the public, while the breadth and volume of information subject to obligations also increases. In this article George Tziahanas, vice president compliance, Autonomy, provides an overview of the UK Financial Services Authority Conduct of Business 11.8 and how it is put into practice

Overview of COBS 11.8

The UK Financial Services Authority (FSA) Conduct of Business (COBS) 11.8 is one of the latest regulations imposed on information environments for many financial services organisations.

Taking effect March 2009, this regulation requires covered entities to record certain telephonic communications and retain these recordings for a period of at least six months. It also covers a broad set of additional electronic communication, which at first glace may not appear as onerous, but presents firms with a need to manage across information channels.

Prior to this specific regulation, many firms had recorded phone calls or retained other electronic communication for use in potential disputes over orders and trades (along with quality or investigatory purposes). Realising the potential value in recorded information for enforcement and other activities, the FSA mandated that calls be taped and electronic communications retained.

Intent and purpose

As with any law or regulation, the underlying rationale for its development serves as a guide for how it might be used. With respect to COBS 11.8, the FSA in its policy statement[1] made repeated references to the efficacy of taped information as evidence. It specifically noted: "recorded communication may increase the probability of successful enforcement."[2]

The policy statement went on to note, "crucially, the evidence that might be obtained from taped recordings may not be available by other means… The advantage of telephone evidence over documentary evidence/oral testimony is that telephone evidence more often helps to show 'knowledge' and 'intent'." While the FSA's policy statement does make additional reference to the value of COBS 11.8 in the context of greater market confidence and price efficiency, it is clear that the FSA intends to use this information as evidence in enforcement actions.

Covered electronic communication channels

The FSA was careful in promulgating the final rule to avoid narrowly defining the types of electronic communication that were covered. In addition to telephone recordings of covered activities, the rule also covers "communications made by way of facsimile, e-mail and instant message devices."[3] Calls made from mobile devices are specifically excluded from the taping requirement,[4] although e-mail sent from such devices are still subject to the rule.[5]

As drafted, the rule covers the most common channels for communicating between firms and with their clients. However, the FSA was also careful to note that the rule should be read broadly, realising technological innovation often outpaces regulation. In its policy statement, the FSA stated electronic communication "is not limited to these, (the channels noted above), as it captures any electronic communications involving receiving client orders and the agreeing and arranging transactions."[6]

Entities and transactions that are covered

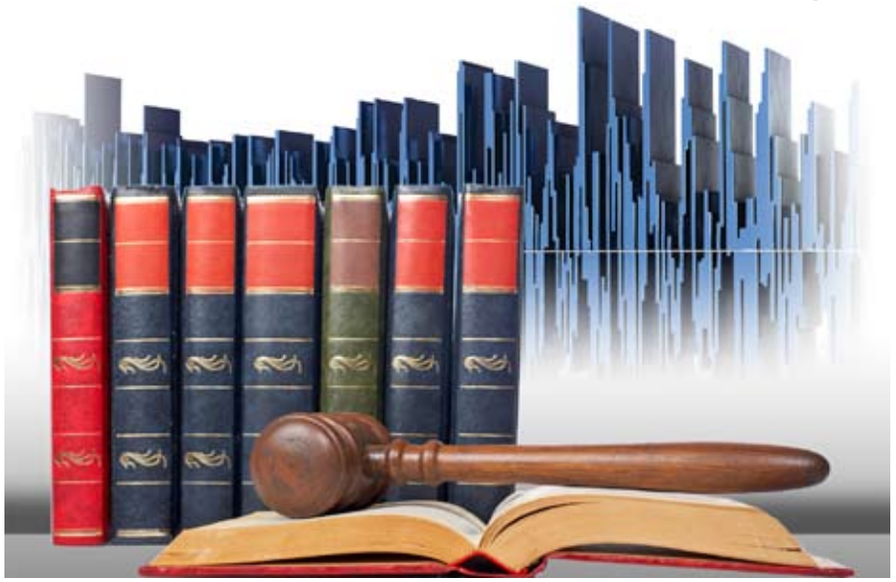
The application of COBS 11.8 "applies only with respect to a firm's activities carried on from an establishment maintained by the firm in the UK." As discussed in more detail below, cross-border and cross-jurisdiction issues arise where one party to a conversation or communication is outside the UK. Entities in the US working with UK affiliates or third parties should be particularly aware that calls will be recorded.

The scope of COBS 11.8 is focused primarily on the types of activities in which a firm or its personnel engage, as opposed to specific definitions of covered entities. The rule applies to a firm[7]:

- receiving, executing or arranging the execution of client orders;
- carrying out transactions on behalf of the firm (proprietary trading); and
- executing or placing orders on behalf of a client (discretionary trading).

It is important to note that a final transaction or trade is not required for application of the rule and associated taping or retention. Rather, conversations or communication "intended to lead to the conclusion of an agreement"[8] are sufficient

[1] *FSA policy statement 08/1, Telephone recording: Recording of voice conversations and electronic communications. www.fsa.gov.uk/pubs/policy/ps08_01.pdf*
[2] *Ibid. at 2.1*
[3] *COBS 11.8.7 G. www.fsa.gov.uk/pubs/hb-releases/rel87/rel87cobs.pdf*
[4] *COBS 11.8.6 R (1)*
[5] *Ibid.*
[6] *See supra note 1. at 2.34*
[7] *COBS 11.8.9 G (1)*



and covered by COBS 11.8. General conversations about market conditions, corporate finance and treasury functions and activities by service providers are exempted from COBS 11.8.[9]

Access and management of recorded and retained communication

The draft version of COBS 11.8 originally proposed a three-year retention period for taped conversations and electronic communication.[10] However, the inclusion of audio recording in this requirement imposes a higher burden for multiyear retention than other communication channels, leading the FSA to impose a six-month retention period.[11]

Retention alone is not sufficient to satisfy requirements under 11.8. The FSA allows storage of conversations and communication in any form, as long as it can be: (1) readily accessed by the FSA; (2) changes or alterations are easily ascertained; and (3) it must not be possible for records to otherwise be altered or manipulated.[12] The FSA went on to note it would "expect that firms' search facilities support a reasonable interpretation of 'readily accessible'."

Deploying a solution

Meaning Based Computing and compliance

In drafting COBS 11.8, the FSA realised that financial services organisations often employ several different communication channels to operate their business. The same types of transactions may be executed across different channels, depending on the client, employee, instrument or other factors. Audio content in particular poses unique technical and operational challenges, and will often need to be aligned with additional channels during an investigation or enforcement action.

While firms may find point technologies that can record or store information, they should focus heavily on the FSA's expectation that all content, including audio, be readily accessible. As such, firms should deploy single-platform solutions that can not only store data, but can record, analyse, archive and access information across a multitude of formats and channels. Audio should be managed and searched alongside and in the same manner as other mission-critical files, documents and e-mail. Only solutions leveraging Meaning Based Computing technology that can manage and search all types of enterprise information and interactions based on an understanding of their content can sufficiently support COBS 11.8 requirements.

Legal and supervision implications

Although COBS 11.8 only imposes an affirmative duty to record for firms operating in the UK, companies operating abroad, especially in the US, should consider the implications of this regulation. All types of electronically stored information are subject to discovery under the US Federal Rules of Civil Procedure.

US courts have broadly interpreted their powers to require discovery of relevant information, even if information is held by affiliates (or potentially third parties) in a foreign jurisdiction. This means that firms operating in the US and UK should have the ability to quickly apply a legal hold on all types of content, including audio. Additionally, a firm's access and search technologies should allow it to aggregate and analyse audio and other information together to determine whether any potential compliance issues are present.

Finally, COBS 11.8 does not impose an affirmative duty to supervise or proactively review audio recording or other communication subject to the rule. Knowing that the FSA fully intends to use audio recordings and other communication in enforcement action, it seems reasonable to suggest that firms implement a corresponding supervision programme for these channels.

Conclusion

The FSA's COBS 11.8 requires that firms record telephone conversations and retain other types of electronic communication. In its guidance, the FSA makes clear that audio content brings unique context and value as evidence in enforcement actions. Firms subject to COBS 11.8 must have the ability not only to retain audio and other electronic communication but, more importantly, provide ready access. Meaning Based Computing provides the means to manage and access information across communication channels, which is necessary where such complex legal and cross-jurisdiction obligations exist.

[8] *COBS 11.8.9 G (1)*
[9] *COBS 11.8.2 and 11.8.3 R*
[10] *See supra note 1. at 1.3*
[11] *COBS 11.8.10 R (1)*
[12] *COBS 11.8.10 R (2)(a-e)*

Responsible information management – ensuring data privacy in the enterprise

Frontline employees are interacting freely with customers through a diverse set of channels, each of which is often overlooked in corporate governance and compliance policies. In this article, Autonomy presents the most common causes of data breaches and why safeguarding this sensitive data is a corporate responsibility

The problem – customer data is a liability

Widespread availability of customer and client data is becoming a great liability to corporations, their customers and their clients, creating easier access to sensitive materials and inviting crimes of opportunity. Organisations have invested tremendously against external threats to information privacy, while internal backdoor threats grow and remain unchecked. Recent news reports have suggested a rise in the underground market for sensitive data exchange, where 'data brokers' can sell customers' addresses, credit card information and social security numbers, and call centre operators are compromising credit card and account information for personal profit. This threat of losing personal data has put both businesses and consumers on high alert and begging for better practices and more effective technology for curbing this growing problem.

The corporate responsibility

Safeguarding sensitive data from leakage is a legal and ethical responsibility for any corporation that collects, transmits and processes sensitive data about the company or its customers. Data privacy laws such as the *Data Protection Act* in the UK, the European Union's *Internet Privacy Law of 2002*, as well as the *US Patriot Act*, the *Payment Card Industry Data Security Standards* and the *Health Insurance Portability and Accountability Act*, among many others, mandate provisions for customer data privacy and require compliance from all corporations that handle particular types of information. However, despite these regulations, 285 million data records were breached in 2008 alone.[1]

Between 2007 and 2008, insider theft more than doubled,[2] affecting more than 15% of the US population. In addition, many recent, well-publicised cases in the US and the UK have involved corporate data leaks, identity theft and information scams. Failure to prevent data leakages demonstrates negligence, and executives can face significant fines from regulators (such as the Federal Trade Commission), jail time and public scrutiny. The corporate risk from data leakage is truly immeasurable. Aside from legal liability and settlement fees, the tarnish to a brand and its perceived trust after a data breach can be damaging beyond repair.

A number of media agencies and privacy watchdog groups have reported incidents of stolen or compromised data across various industries. Recent examples include the following:

- **Data breach in the call centre**[3]
Symantec, a globally recognised provider of security software, experienced their own backdoor data compromise in March 2009 as a BBC investigator was able to purchase valid credit cards from an employee at a call centre in India. Symantec sent warning letters to 200 customers notifying them that their information may have been stolen.
- **Financial services company experiencing data leakage**[4]
The FBI arrested a former Countrywide employee in an alleged scheme to steal and sell sensitive personal information, including social security numbers. The breach occurred over a two-year period. The insider was a senior financial analyst at Countrywide's subprime lending division. The alleged data thief was said to have downloaded about 20,000 customer profiles each week and sold

[1] *Verizon Business Data Breach Investigations Report*
[2] *www.idtheftcenter.org*
[3] *www.bbc.com*
[4] *www.privacyrights.org*

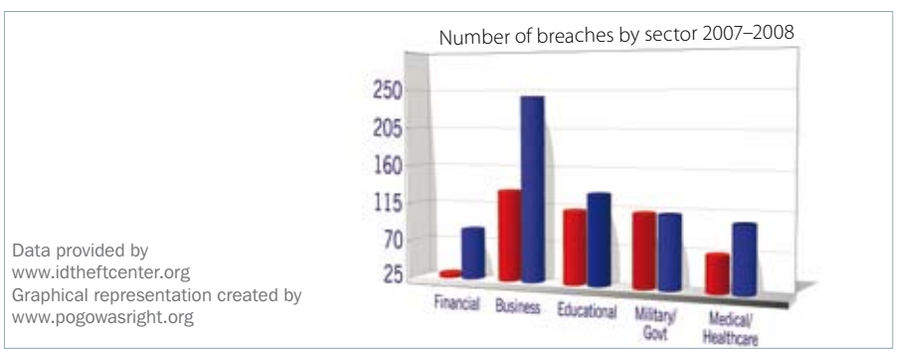


Figure 1: Data theft on the rise

files. In a 2009 settlement with the State of Connecticut, Bank of America agreed to pay at least $375,000 in fines.

The real threat of internal data theft

The doubling of data crime indicates current measures are ineffective at deterring data thieves inside the organisation. Preventing such data leaks requires the ability for organisations to comprehensively and continuously monitor employee activity, including desktop applications, website activity, e-mails, instant messages and phone calls, as well as the ability to identify and act on potential data privacy violations. Suspicious activities may include:

- frequent copying of files onto mobile media (CDs or flash drives);
- excessive time on screens containing personal data;
- transmission of files or information to e-mail addresses beyond the firewall;
- discussion of a customer's personal information over the phone without the customer present;
- accessing restricted or unauthorised applications; and
- transferring of information from one application to another (copy/paste).

Knowing what to look for is only half of the solution. With huge numbers of employees and even larger amounts of electronic information being stored and transmitted every day, businesses require advanced technologies that proactively monitor employee interactions and provide business and compliance managers with intelligence that enables them to take decisive action on violations and their proprietors. The combination of 24/7 activity monitoring and severe consequences for employees conducting data theft or leaking information to third parties is a critical step in curbing these crimes of opportunity.

The bottom line

With the increased availability of digital information and records, a corresponding increase in data leakage and theft attempts is inevitable. Organisations unwilling to implement the necessary technologies to prevent the needless leakage of sensitive information are a risk to their customers and business partners – clients who may soon rethink the practice of exchanging data with unsecured organisations.

Figure 2: Autonomy Interaction Control Element (ICE)

"Insider theft, now at 15.7%, has more than doubled between 2007 and 2008. On the other hand, data on the move and accidental exposure – both human error categories – showed a noteworthy improvement, but still account for 35.2% of those breaches that indicate cause. Electronic breaches (82.3%) continue to outnumber paper breaches (17.7%)."

Identity Theft Resource Center, January 5, 2009

Autonomy Corporation plc (LSE: AU. or AU.L), A global leader in infrastructure software for the enterprise, spearheads the meaning-based computing movement. It was recently ranked by IDC as the clear leader in enterprise search revenues, with a market share nearly double that of its nearest competitor. Autonomy's technology allows computers to harness the full richness of human information, forming a conceptual and contextual understanding of any piece of electronic data, including unstructured information such as text, e-mail, web pages, voice or video. Autonomy's software powers the full spectrum of mission-critical enterprise applications including, pan-enterprise search, customer interaction solutions, information governance, end-to-end eDiscovery, records management, archiving, business process management, web content management, web optimisation, rich media management and video and audio analysis.

AUTONOMY INTERACTION CONTROL ELEMENT (ICE)

To protect companies from unnecessary data leaks and security breaches, Autonomy offers a groundbreaking technology that automates security, governance and regulatory processes across the enterprise, allowing corporations to maintain focus on enterprise data privacy. By automatically identifying possible violations that occur in employee communication and desktop activity, Autonomy enables organisations to effectively monitor and take action on potentially criminal behaviour.

Autonomy ICE is language and application-agnostic, allowing it to operate on any system and connect to any application, including web-based applications, recording systems, customer relationship management and helpdesk suites, e-mail systems and chat applications. By combining defined parameters with a real-time understanding of the content within an interaction made via phone, e-mail, chat, web or desktop application, Autonomy ICE identifies and takes action on any suspicious or potentially threatening interaction occurring within the organisation. When a suspicious interaction is identified, Autonomy ICE can be configured to record and archive the end-user's audio and desktop interaction, mask or mute sensitive data from a voice or screen recording, send an alert to a compliance officer, lock a workstation or perform any other number of activities to minimise and ultimately prevent sensitive data from leaving the confines of your organisation.

To learn more about Autonomy ICE, download the white paper: www.etalk.com/dataprivacy