ICE IM Compliance Overview

January 2017

TABLE OF CONTENTS

1 Introduction

Offering real-time communication and collaboration capabilities, ICE IM features full retention and audit trails of trader and counterparty communications while meeting corporate and government regulatory requirements such as Sarbanes-Oxley. Additionally, ICE IM provides tools to export ICE IM user logs to an internal or 3rd party SEC 17a-4 compliant data archiving system.

This document describes the feature set of ICE IM compliance offerings. It also illustrates how the offerings can be integrated into an institution's existing framework.

2 Enterprise Control

ICE IM provides an added level of security over the native AIM and Yahoo applications by providing institutional controls over employee access to instant messaging communications, with privacy settings for AIM® and Yahoo! Under most configurations, ICE IM will only allow two IM's per unknown contact, all subsequent IM's will be blocked.

Additionally, ICE IM can be configured to ensure that users login from a specific IP address or block of addresses -- within the safety zone of the institution's firewall.

3 Secure Communication

Traffic distributed to and from the ICE IM client is secured using 128-bit SSL encryption. The SSL protocol precludes tampering and modification of data in transit. Additionally, the server performs authorization on all requests.

4 Compliance Auditing and Administrative Tools

ICE IM includes full retention and audit trails of all communications. Communications are logged on our server prior to transmitting data to the client. This prevents users from altering logs, and ensures that all communication is logged even if the client is using ICE IM outside of an institution's network.

Please note that message logs are not stored in manner fully compliant with SEC rule 17a-4 , and thus only recommended for CFTC regulated entities. They are not recommended for fulfilling SEC and FINRA audits. For clients regulated by the SEC or FINRA, we recommend setting up a message log export to an SEC approved archiving system. This is detailed in the Content Archiving Integration section of this document.

All logs are captured and stored at the ICE Data Center, which is audited annually by a 3rd party for SAS70 compliance. In regards to logging, the SAS70 audit covers the following areas to ensure operating effectiveness:

- Logical Access Controls
- Physical and Environmental Controls
- Backup Procedures and Data Retention
- Change Management

All logs will be stored for a minimum of seven years. Copies of the logs are backed up and stored offsite in accordance with industry best practices.

Logs can be accessed through a number of different channels:

- The ICE IM application
- The ICE IM website's secure client area or Enterprise Admin Console

- Via existing content archiving systems (daily batch process connection)
  - Via daily email
  - Via SFTP file export
- Via specific log request to ICE Support

Message Log Retrieval from the Client Area

The ICE IM application features a link to our online Client Area. On this site, the **Message Log feature** can be used to obtain all available conversations for review and examination. A search feature allows logs to be searched using various filters, including counterparty, time period and conversation content. This feature is available to all ICE IM users as part of their subscription.

Compliance Auditing and Administrative Tools from the Enterprise Admin

For users with additional compliance and administrative needs, the Enterprise Admin Console can be made available. The Enterprise Admin console, or EAC, is web based tool where Compliance and Administrative users can access and audit logs in real time across a configurable subset of employees (i.e., a particular trading desk or department). Administrators can also be permissioned for additional features such as disabling users, monitoring contact lists, setting IM disclaimers, and blocking access to specific contacts. Administrators can also setup custom saved searches to search on specific keywords or phrases. Logs are made available via the EAC for a minimum of seven years.

Additionally, Administrative users can export a result set of message logs directly from the EAC to a CSV file format viewable within MS Excel.

5 Content Archiving Integration

ICE IM easily integrates with other enterprise content archiving and IM auditing systems including, but not limited to: Smarsh, Global Relay, Actiance Vantage (formerly FaceTime), and Symantec IMlogic.

For most configurations, ICE IM is integrated via a file import. ICE IM will host an SFTP site and export your user's logs to a single file on the site, which can be downloaded and imported into your current compliance system. Typically this is setup as an EOD file process, although it can be run more often. Most users will setup a script to automatically download and process the file.

Files are encrypted during transfer to ensure they are not tampered with during transmission.

Additionally, we can convert IM messages to emails and send them directly to an existing content archiving system. This allows for a quick integration, as your IM messages are made available within your existing email archiving system. We typically send one email per sender/receiver pair per day to a specified email address. Multiple email formats are available. For example, messages can be configured to replace the email header's To and From field with the user's corporate email address and the contact's AIM or Yahoo IM address to allow for seamless integration with email archiving systems. Please see your ICE IM representative for questions on available formats.

6 Message Log Purging

By default, ICE IM will log all messages for a minimum of seven years. Alternatively, Administrators can elect to purge their user's logs from the ICE IM archive. Message logs can be set to never record to our archive, or they can be temporarily logged for up to two weeks and then purged from the ICE IM Archive.

7 Information or Questions

For additional information or questions regarding ICE IM's compliance offerings, please contact us at +770.738.2101 option 5.