

Matthew C. Helland, CA State Bar No. 250451
helland@nka.com
Daniel S. Brome, CA State Bar No. 278915
dbrome@nka.com
NICHOLS KASTER, LLP
235 Montgomery St., Suite 810
San Francisco, CA 94104
Telephone: (415) 277-7235
Facsimile: (415) 277-7238

Electronically FILED by
Superior Court of California,
County of Los Angeles
2/27/2025 8:01 AM
David W. Slayton,
Executive Officer/Clerk of Court,
By G. Carini, Deputy Clerk

Attorneys for Plaintiffs and the Class

SUPERIOR COURT OF THE STATE OF CALIFORNIA

COUNTY OF LOS ANGELES

Daniel Grentz, individually, on behalf of
others similarly situated, and on behalf of
other aggrieved employees,

Plaintiffs,

v.

American Airlines, Inc.,

Defendant.

Case No.: 23STCV03941

Hon. Laura A. Seigle, Department 17
Spring Street Courthouse

**DECLARATION OF SEAN
STONEHOUSE**

1
2
3
4
5
6
7
8
9
0
1
2
3
4
5
6
7
8
9
0
1
2
3
4
5
6
7
8

2. IL YM Group has extensive experience in disseminating class action notices and administering class action settlements, including direct mail services, telephone, and web-based support, database management, opt-out processing, and settlement fund distribution services for class actions ranging in size from 26 to 4.5 million Class Members. Attached hereto, as **Exhibit A**, is a true and correct copy of IL YM Group's current CV, reflecting our primary competencies as they relate to class action administration. IL YM Group maintains the highest level of confidentiality. The class data and all forms of communication received by IL YM Group, Inc. will be held in strict confidentiality and will not be disclosed. IL YM Group, will set up a login for Defense Counsel to transmit the class data through our encrypted secure portal. Attached hereto, as **Exhibit B** is IL YM Group's Security Summary and Protocol. IL YM Group is insured with E&O and Cyber Insurance policies.

4. If appointed by the Court to disseminate the class notice in this case, IL YM Group's duties will include but not limited to: (a) conducting address traces to locate class member addresses as necessary; (b) providing the class notice to the class members by mail & email; (c) handling inquiries from class members concerning the class notice; and (d) performing other such duties as the parties and/or the Court may direct.

5. Upon appointment, IL YM Group will provide a mailing address and toll-free telephone number to receive correspondence and inquiries from class members. After receiving the class data file from Defendant, that should contain the class members' names, last known addresses, and social security numbers, IL YM Group will upload the data into our database and check for duplicates and other possible

1 discrepancies.

2 6. As part of the preparation for mailing the class notice, ILYM Group will process class
3 members' names and addresses against the National Change of Address ("NCOA") database, maintained
4 by the United States Postal Service ("USPS"), for the purpose of updating and confirming the mailing
5 addresses of the class members before mailing of the class notice and opt-out form. To the extent an
6 updated address is found in the NCOA database, ILYM Group will use the updated address for mailing
7 the class notice. If ILYM Group does not locate an updated address in the NCOA database, it will use the
8 original address provided by Defendant for mailing the class notice.

9 7. Should any class notices be returned to ILYM Group's office as undeliverable, ILYM
10 Group will attempt to locate an updated address using the NCOA database and/or other skip trace efforts
11 and will promptly re-mail the class notice.

12 8. Prior to sending out the notice in English & Spanish, ILYM Group will fill in the specific
13 date for the deadline so that all class members will be apprised of exactly when all applicable forms will
14 be due, depending on the deadlines set by the Court, i.e., 60-day Notice period to opt-out, dispute or file
15 an objection. At the expiration of the deadline, ILYM Group will inform all parties as to the number and
16 name of those individuals who filed a timely opt-out, dispute or objection.

17 9. ILYM Group's Disbursement Process will include but not limited to; (a) applying for
18 case EIN; (b) establishing Qualified Settlement Fund ("QSF") Escrow Account), with administering
19 tasks including but limited to overview and reconciliation of account; (c) calculating the individual
20 settlement amounts; (d) preparing, administering and distributing settlement award checks to the
21 Participating Class Members, including necessary tax forms (1099); (e) calculating and withholding all
22 applicable state and federal taxes; and (f) performing other such duties as the Parties and/or the Courts
23 direct. The above services are included in ILYM Group's initial quote. Attached hereto, as **Exhibit C**, is
24 a true and correct copy of ILYM Group's not to exceed quote for this matter.

25 10. ILYM Group's fees are charged: hourly, fixed & per person. No additional charges will
26 be incurred unless the class size increases, or additional services are requested. ILYM Group's fees
27 associated with the administration of this settlement is: \$15,755.

28 ///

1 I declare, under penalty of perjury under the laws of the United States of America and the State
2 of California that the foregoing is true and correct. Executed this 21st day of February 2025, at Tustin,
3 California.

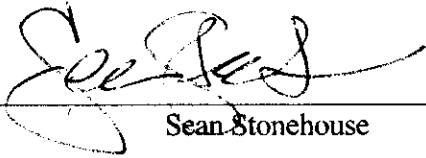
4
5 
6 Sean Stonehouse

EXHIBIT A

Overview of Our Firm:

ILYM Group, Inc is a class action administration, legal notification and direct media outlets firm. With over 14 years of experience, our primary commitments are to client satisfaction, cutting edge technology and data management security, seamless case management and delivery of case expectations. Because, of our adherence to these commitments, ILYM Group, Inc is a one of the fastest growing, Woman Owned Business (NAPW), in the industry and is becoming the go-to firm for class action administration and legal notification. ILYM Group, Inc works with the top defense and plaintiff firms across the United States.

AREAS OF EXPERTISE:

- Wage and Hour
- FLSA
- Insurance and Health Care
- Consumer
- Finance
- Employment and Labor
- Securities
- Antitrust
- TCPA

Malta vs. Wells Fargo Home Mortgage Inc.

- TCPA Case with a class size of 5,200,000.

Gerardo Mojica vs. Compass Group USA, Inc.

- Wage & Hour Case with a class size of 22,573

Jacqueline Jones vs. I.Q. Data International, Inc.

- TCPA Case with a class size of 93,993. Performed a reverse look-up to obtain Class Member information. We were able to obtain contact information for 93.82% of the Class that did not have a name or address.

Grinder, et al. v. Clark County Collection Service, LLC.

- TCPA Case with a class size of 15,659. Performed a reverse look-up to obtain Class Member information. We were able to obtain contact information for 97% of the Class that did not have a name or address.

Kimberly Roberts, et al. v. T.J. Maxx of CA, LLC, et al.

- Wage & Hour Case with a class size of 82,549.

Reza Barani vs. Wells Fargo Bank, N.A.

- TCPA Case with a class size of 82,874. Performed a reverse look-up to obtain Class Member information. We were able to obtain contact information for 87.84% of the Class that did not have a name or address.

Blaise Picchi et al., vs. World Financial Network Bank, et al.

- TCPA Case with a class size of 856,507. Performed a reverse look-up to obtain Class Member information. We were able to obtain contact information for 93.21% that did not have a valid address associated with the contact record.

ILYM | GROUP, Inc.

SETTLEMENT ADMINISTRATION EXPERTS

ILYM Group, Inc. is operational 24/7 delivering true client and class member availability. Our call center is open 24/7/365 days a year, even holidays and is full digital, automated and multilingual. ILYM Group Inc.'s mail and media center is a state-of-the-art facility, fully digital and USPS integrated. We can accommodate cases of any size, from ten class members to multi-millions. ILYM Group, Inc. prides itself on its commitment to service, quality, value pricing and availability. We've committed ourselves to being the best Class Action Administration and Notification Company in our industry. Through our years of experience, ILYM Group, Inc. is dedicated to exceeding our client's expectations.

PRE-SETTLEMENT CONSULTATION

- **Administration Consultation:** Meeting to determine objectives and expectations by both parties. All reporting and responsibilities will be agreed upon as will the seamless process to access data. We will also discuss the opportunities to identify class members with the proposed print and web-based media for optimum reach. Additionally, all expectations and delivery of those results will be planned for and mapped accordingly.

MAILING AND NOTIFICATION

- **Fulfillment and Correspondence:** All provided settlement information will be published via United States Postal Service (USPS first class standards) to the proposed mailing class. Notifications will include a Claim ID and how to respond, or Opt-Out, based on the stipulations.
- **Reverse Lookup:** A confidential reverse phone or reverse cell lookup will provide; owner's name, location, address history, carrier, phone type (landline or cell phone) and more. Our reverse lookup is powered by an extensive database which includes hundreds of millions of cell phone, landline, residential and unlisted number. Our software collects data from multiple data sources and carriers across the US. Our average "hit ratio" ranges from 93% - 98%.
- **Creating Class Database:** All Data is verified and filtered to eliminate duplication against the United States Postal Service (USPS) National Change of Address (NCOA) database. ILYM Group, Inc. will also certify and validate with the Coding Accuracy Support System (CASS) and Track Your Class (TYC) for zone delivery.
- **Claim Forms:** ILYM Group, Inc. will email all claim forms, whenever possible, to have accurate reporting and tracking of all class requests. Emails will contain full text claim forms.
- **Translations:** When needed, ILYM Group, Inc. will translate notices to any language needed to reach Class members.
- **Remails:** Returned mail will be scanned, re-verified and re-mailed. All returned mail is data warehoused and reported to both parties' counsels in a weekly report.

MEDIA & INTERNET BANNER ADS

Notice Publication

- **Legal Notices:** ILYM Group, Inc. can provide a Media Proposal to maximize reach based on quantitative and qualitative methodologies.
- **Electronic Publication (Banner Ads):** ILYM Group, Inc. will utilize Internet Banner Noticing efforts and web technologies for maximum reach via the World Wide Web.

ILYM | GROUP, Inc.

SETTLEMENT ADMINISTRATION EXPERTS

- **Electronic Mail Notices:** ILYM Group, Inc. can email an estimated number of class members a full text notice. We are compliant with all search engines and Internet Service Providers (ISP) so that our emails are always “White List” accepted with minimal returns.
- **Reach:** Every case has its own proposed reach and exposure percentage. We filter, verify and scrub the data to improve reach results.
- **Services Included:** Analysis, Documentation, Research and Methodologies, Execution and Reporting.

PROJECT MANAGEMENT

- **Case Notification, Maintenance and Management:** ILYM Group, Inc.’s Senior Project Managers will provide all Account Management, Pre-Consultation to Case Conclusion, Reporting and Claims Processing. Design, negotiation and implementation, upon approval, of all forms and notices, all distribution reporting and filings with the court.
- **Claims Processing:** All claims can be submitted by USPS, Internet, Fax, and Email or Online submission. Claims will be processed and recorded with matching ILYM database ID's. E-claims will have corresponding records of intake. All deficient claims will be notified via USPS and make provisions for class member to re-submit claims.
- **Call Center:** ILYM Group, Inc. will support class members with a toll-free number to get the most up-to-date case settlement information. Customer service representatives will be available 24/7/365 as will recorded messages.
All class members are given the options to best serve their needs and to receive case information.
- **Internet Support:** Class members can log on to a provided website and view, print or submit information and claim forms regarding the settlement. Frequently Asked Questions (FAQ’s) will be provided as well. Class members may download the claim form with mailing and fax instructions provided on the form.
- **Objection and Request for Exclusion:** All objections and request for exclusion, opt-out, will be data warehoused, dated and reported. Postmarks will serve for exclusion dating and will be forwarded to both counsels’ no more than 5 days post submission. Objection will be reviewed by ILYM Group, Inc. to determine the timeliness and basis of the objection. All information will be forwarded to both parties counsel, along with any representation information from the class member, within 5 days.

DATA ADMINISTRATION AND NETWORK SECURITY

- **Network Security:** All provided data is encrypted, stored and hosted in a Tier 4, SAS70 certified environment.
- **Database Administration:** To be developed with all electronically provided data. Class members will be assigned ILYM Group, Inc. internal tracking ID’s to ensure all collected member data coincides with all received claims.

DISTRIBUTION AND SETTLEMENT FUNDING

- ***Distribution and Management:*** Upon receipt of settlement funds, ILYM Group, Inc. will open a QSF Account for proceeds of the Gross Settlement Payment. The deposited funds will then be managed per the Settlement Agreement. All funds will be settled with class members and counsel along with all federal and state income tax reporting.
- ***Check Printing and Mailing:*** Claims processed, quantified and approved by clients, will be processed for distribution. All checks will be printed and mailed via USPS first class standards. ILYM Group, Inc. will reissue checks in accordance with the Settlement Agreement.
- ***Preparation, Filing and Reporting of Taxes:*** ILYM Group, Inc. will ensure taxes are filed in accordance to all federal, state and local employment tax returns. All taxes associated with the settlement will be paid on time to tax authorities. All filings and returns (e.g., 1099s, W-2s, etc.) will be done properly and timely with the appropriate authorities. All QSF steps and obligations with federal, state and/or local law will be followed.

CASE CONCLUSION

- ***Data Manager Final Report:*** All database and electronic documentation will be sent in reports weekly and at the conclusion of the Administration engagement. Call center activity, e-claims, mailed, and faxed claims will be included in all reporting.
- ***Project Manager Final Report:*** All case and class related information will be provided on a weekly basis and at the conclusion of the Administration engagement. Mailing and media final analysis, exclusions, objections, and all other claims processing outcomes, status reports and final court documentations will be included.
- ***Affidavits:*** ILYM Group, Inc. will provide all affidavits in support of analysis and media reach, final approvals and settlement. Expert Testimony and Media Methodologies will be determined.
- ***Document Retention:*** Unless otherwise directed, ILYM Group, Inc. will destroy all undeliverable notices on the effective date of the settlement or when the case is no longer subject to appeal. ILYM Group, Inc. will correspond for one year after the final distribution or until the case is no longer subject to appeal.

EXHIBIT B



Report on ILYM Group, Inc.'s Description of the
Class Action Administrative Services System and the
Suitability of the Design of Controls
Relevant to Security and Confidentiality
as of February 29, 2024

SOC 2[®]



This report is not to be copied or reproduced in any manner without the expressed written approval of ILYM Group, Inc. The report, including the title page, table of contents, and exhibits, constitutes the entire report and should be referred to only in its entirety and not by its component parts. The report contains proprietary information and is considered confidential.

ILYM | GROUP, Inc.
SETTLEMENT ADMINISTRATION EXPERTS

TABLE OF CONTENTS

I.	INDEPENDENT SERVICE AUDITOR’S REPORT	
II.	ILYM GROUP, INC.’S MANAGEMENT ASSERTION	
II-A.	CLARUS IT SOLUTIONS, INC.’S MANAGEMENT ASSERTION	
III.	DESCRIPTION OF ILYM GROUP, INC.’S CLASS ACTION ADMINISTRATIVE SERVICES SYSTEM	8
IV.	OTHER RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION SYSTEMS, AND MONITORING CONTROLS	13
V.	SUBSERVICE ORGANIZATIONS	19
VI.	INDEPENDENT SERVICE AUDITOR’S DESCRIPTION OF CONTROLS	21



I. INDEPENDENT SERVICE AUDITOR'S REPORT

To the Management of ILYM Group, Inc.:

Scope

We have examined ILYM Group, Inc.'s ("ILYM" or the "Company") accompanying description of the class action administrative services system, including IT related managed services provided by and controls operated by Clarus IT Solutions, Inc. ("Clarus IT" or "Clarus") entitled "Description of ILYM Group, Inc.'s Class Action Administrative Services System" ("description") as of February 29, 2024, based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) ("description criteria") and the suitability of the design of ILYM's controls, including the controls designed by ILYM and operated by Clarus IT, stated in the description as of February 29, 2024, to provide reasonable assurance that ILYM's service commitments and system requirements were achieved based on the trust services criteria relevant to security and confidentiality ("applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Clarus IT is an independent subservice organization providing IT related managed services to ILYM. The description includes those elements of the IT related managed services provided to ILYM and the controls designed by ILYM and operated by Clarus IT that are necessary for ILYM to achieve its service commitments and system requirements based on the applicable trust services criteria.

ILYM uses other subservice organizations: Microsoft Azure, to provide cloud-based hosting services; and Todyl, for MXDR and SOC monitoring services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at ILYM, to achieve ILYM's service commitments and system requirements based on the applicable trust services criteria. The description presents ILYM's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of ILYM's controls. The description does not disclose the actual controls at these subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service organization's responsibilities

ILYM is responsible for its service commitments and system requirements and for designing and implementing controls within the system to provide reasonable assurance that ILYM's service commitments and system requirements were achieved. ILYM has provided the



accompanying assertion entitled “ILYM Group, Inc.’s Management Assertion” (“assertion”) regarding the class action administrative services system as of February 29, 2024, about the description and the suitability of the design of controls stated therein. ILYM is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization’s service commitments and system requirements.

Subservice organization’s responsibilities

Clarus IT has provided the accompanying assertion titled “Clarus IT Solutions, Inc.’s Management Assertion” about the description and the controls stated therein. Clarus IT is responsible for preparing the portion of the description related to the IT managed services provided to ILYM and the Clarus IT assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; and implementing, operating, and documenting controls designed by ILYM, which enable ILYM to achieve its service commitments and system requirements.

Service auditor’s responsibilities

Our responsibility is to express an opinion on the description and on the suitability of the design of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed to provide reasonable assurance that the service organization’s service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization’s system and the suitability of the design of controls involves the following:

- Obtaining an understanding of the system and the service organization’s service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service



organization achieved its service commitments and system requirements based on the applicable trust services criteria

- Evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

Inherent limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. The projection to the future of any conclusions about the suitability of the design of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Other matter

We did not perform any procedures regarding the operating effectiveness of controls stated in the description and, accordingly, do not express an opinion thereon.

Opinion

In our opinion, in all material respects:

- a. The description presents ILYM's class action administrative services system that was designed and implemented as of February 29, 2024, in accordance with the description criteria.
- b. The controls stated in the description, including the controls designed by ILYM and operated by Clarus IT, were suitably designed as of February 29, 2024 to provide reasonable assurance that ILYM's service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated effectively as of February 29, 2024, and if subservice organizations applied the complementary controls assumed in the design of ILYM's controls as of February 29, 2024.



Restricted use

This report is intended solely for the information and use of ILYM, user entities of ILYM's class action administrative services system as of February 29, 2024, business partners of ILYM subject to risks arising from interactions with the class action administrative services system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

IS Partners, LLC

IS Partners, LLC
Dresher, Pennsylvania
May 10, 2024

II. ILYM GROUP, INC.'S MANAGEMENT ASSERTION

We have prepared the description entitled “Description of ILYM Group, Inc.’s Class Action Administrative Services System” (“description”) as of February 29, 2024, based on the criteria for a description of a service organization’s system in DC section 200, *2018 Description Criteria for a Description of a Service Organization’s System in a SOC 2[®] Report* (AICPA, *Description Criteria*) (“description criteria”). The description is intended to provide report users with information about the class action administrative services system that may be useful when assessing the risks arising from interactions with ILYM’s system, particularly information about system controls that ILYM has designed and implemented to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security and confidentiality (“applicable trust services criteria”) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

ILYM uses a subservice organization, Clarus IT, to provide IT related managed services. ILYM’s description includes a description of Clarus IT’s managed services used by ILYM, including the controls of ILYM and the controls designed by ILYM and operated by Clarus IT that are necessary for ILYM to achieve ILYM’s service commitments and system requirements based on the applicable trust services criteria. Clarus’ assertion is presented in section II-A.

ILYM uses other subservice organizations: Microsoft Azure, to provide cloud-based hosting services; and Todyl, for MXDR and SOC monitoring services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at ILYM, to achieve ILYM’s service commitments and system requirements based on the applicable trust services criteria. The description presents ILYM’s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of ILYM’s controls. The description does not disclose the actual controls at these subservice organizations.

We confirm, to the best of our knowledge and belief, that

- a. The description fairly presents ILYM’s class action administrative services system that was designed and implemented as of February 29, 2024, in accordance with the description criteria.
- b. The controls stated in the description, including the controls designed by ILYM and operated by Clarus IT, were suitably designed to provide reasonable assurance that ILYM’s service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated effectively as of February 29, 2024, and if the subservice organizations applied the complementary controls assumed in the design of ILYM’s controls as of February 29, 2024.



II-A. CLARUS IT SOLUTIONS, INC.'S MANAGEMENT ASSERTION

Clarus IT Solutions, Inc. provides IT related managed services to ILYM. The services provided by Clarus IT are part of ILYM's class action administrative services system. We have prepared the portion of the accompanying description of ILYM's class action administrative services system titled "Description of ILYM Group, Inc.'s Class Action Administrative Services System" ("description") as of February 29, 2024, disclosing Clarus IT's managed services provided to ILYM, based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2[®] Report* (AICPA, *Description Criteria*) ("description criteria"). The description is intended to provide report users with information about ILYM's class action administrative services system that may be useful when assessing the risks arising from interactions with ILYM's system, particularly information about system controls that ILYM has designed and implemented to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security and confidentiality ("applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

We confirm, to the best of our knowledge and belief, that

- a. The description presents Clarus IT's managed services made available to ILYM as of February 29, 2024.
- b. Clarus IT's controls stated in the description, which were designed by ILYM, were operating as of February 29, 2024, based on the applicable trust services criteria.

III. DESCRIPTION OF ILYM GROUP, INC.'S CLASS ACTION ADMINISTRATIVE SERVICES SYSTEM

Company Overview

ILYM Group, Inc. (“ILYM” or the “Company”) is an organization that is dedicated to exceeding client expectations while delivering exceptional value and service. ILYM provides consultative expertise, professionalism and experience in the areas of Class Action Administration, Legal Notification and Media Representation, and Class Data Management.

ILYM’s Services Overview

ILYM supports clients and provides high level services listed below.

- Class Settlement Administration and Claims Processing
- Consultation of Pre-Settlement Administration
- Finalization of Documentation and Court Filings
- Fund Distribution and Tax Reporting
- Class Data Management
- Proactive Legal Notification and Media Center
- Scalable Call Center

Clarus IT’s Services Overview

Clarus IT is a technical consulting company that specializes in Managed IT Services focused on small to medium-sized businesses. Clarus’ services provided to ILYM are listed below.

- Managed IT Services
- IT Consulting
- CRM Consulting

Principal Service Commitments and System Requirements

ILYM designs its processes and procedures related to its class action administrative services. Those objectives are based on the service commitments that ILYM makes to user entities, the laws and regulations that govern the provision of its services, and the financial, operational, and compliance requirements that ILYM has established for the services.

Service commitments to user entities are documented and communicated in Administrative Services Agreements (“ASAs”) as well as in the description of the service offering provided online. ILYM’s commitments to privacy are communicated online and are documented. Service commitments are generally standardized and include, but are not limited to:

- Confidentiality provisions regarding proprietary technical and business information of both ILYM and its customers.
- Implementing a formal escalation process approved by the customer for issues that fall outside of ILYM Customer Service Representatives’ purview,
- Define and manage the delivery of services including resources and scheduling.

In achieving its service commitments and system requirements, ILYM has implemented various controls to ensure security, confidentiality, and privacy such as:

- Use of an MFA protected portal for member online services,
- Role-based access controls and continuous review and monitoring of key applications and the network,
- Security monitoring infrastructure including intrusion detection, centralized log management and alerting,
- Geographically separated data centers that provide strong physical security controls,
- Incident response program designed to minimize the impact of incidents and protect resources.

ILYM establishes operational requirements that support the achievement of service commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in ILYM's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained.

Components of the System Used to Provide Services

ILYM's Class Action Administrative Services system is comprised of the following five components:

- Infrastructure (systems and networks)
- Software (utilities)
- People (management, class settlement administrators and support staff)
- Procedures (automated and manual)
- Data (transactions streams, files, databases, and tables)

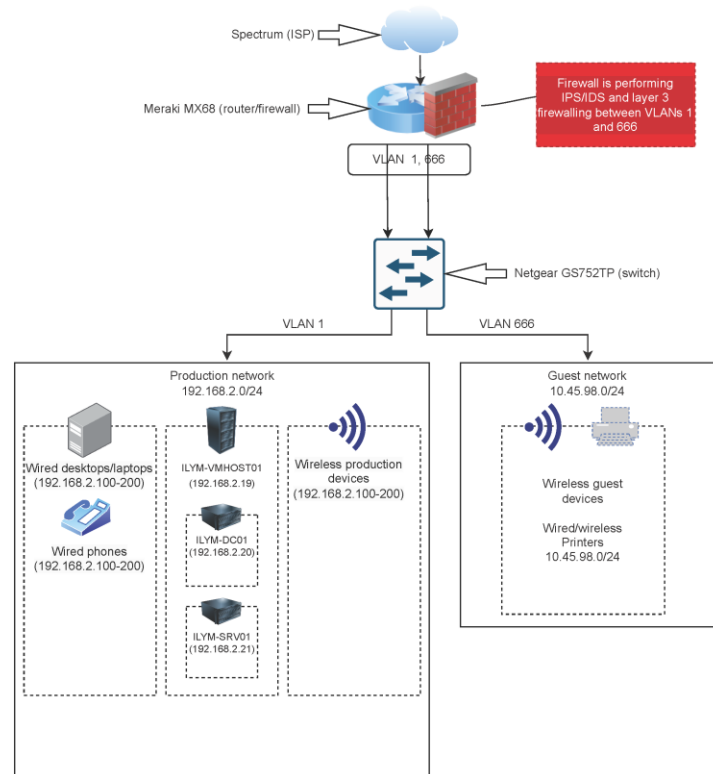
The following sections of this description define each of these five components comprising ILYM's Class Action Administrative Services system.

Infrastructure

ILYM's class action administrative services are hosted on-premises in the ILYM datacenter. Secure file sharing is hosted in the Microsoft Azure cloud platform.

ILYM's online services are hosted in the nearest Azure geographical region. Azure Regions provide multiple physically separated and isolated Availability Zones which are connected with low latency, high throughput, and highly redundant networking. ILYM Group takes advantage of these Availability Zones to provide highly available, fault-tolerant, and scalable services, with automatic fail-over. ILYM uses multiple data centers for redundancy and disaster recovery.

ILYM's main office in Tustin, CA has a network supported with routers, switches, firewalls, layer 2 routing protocols.



Internal computing operations such as on-premise and cloud infrastructure monitoring, integrated testing, and Business Intelligence Systems are supported on systems manufactured by Dell. These systems can access the Azure cloud infrastructure with web browsers like Google Chrome and Microsoft Edge.

ILYM uses active directory for on-premises identity and access management. Privileged access is limited to system administrators for access to active directory and for support of the ILYM information systems. This minimizes the risk of changes to the environment. It also ensures that access is well documented in CloudTrail logs, to support alerting and forensics.

Software

ILYM uses a variety of off-the-shelf and custom software to deliver services to its customers. The key off-the shelf software used includes:

- *Microsoft Authenticator* – Microsoft Authenticator is a Two Factor Authentication (TFA) tool used to ensure secure access to cloud/ online services.
- *Microsoft Teams* – Used for group chat, direct messaging and online meetings. It is the medium of communication at ILYM.
- *Microsoft Azure* – Used for online services hosting platform for ILYM.
- *Microsoft Office 365 and associated software/services (Office, Sharepoint, One Drive*

- *Dynamics CRM* – primary database for tracking Cases and Class Members
- *Microsoft SQL Server* – Used for data translation tools and data processing
- *Todol* – SOC/SIEM/MXDR
- *Bit Defender* – Centrally managed antivirus and malware

People

ILYM operates a hierarchical organizational structure as described below:

- Executive Management is located in Tustin, California. ILYM's office houses the key executives, such as the CEO, CFO, President, EVP, AVP. Specifically, these perform the following responsibilities:
 - The CEO is responsible for the overall strategic leadership of ILYM.
- On-site staff and remote staff include Department Managers and Assistant Managers, Team Leads, Department Specialists, Project Managers, Programmers and IT Support Specialists.

Procedures

ILYM has developed and maintained policies and procedures following to support the operation and controls over the class action administrative services system. The policies and procedures are provided to appropriate personnel and users. Policies and procedures are based on the Center for Internet Security ("CIS") framework. Specific examples of the relevant policies and procedures include the following:

- Access Control
- Change Management
- Data Classification and Management
- Employee Handbook
- Information Security
- Incident Management
- Risk Management
- Vendor Management Procedures and Questionnaire

Data

Acquisition, Classification, Encryption, and Handling

ILYM has defined policies and procedures directing employees and contract staff on the appropriate handling of information to ensure that it is protected from unauthorized access, modification, disclosure or deletion, and to mitigate the risk of loss of customers or public confidence, and the direct monetary loss due to fines and penalties imposed by regulatory bodies. All information resources (including data and systems) are protected, from their origination to their destruction, according to their level of sensitivity, criticality, and business "need to know."

Data owned, used, created, or maintained by the company is classified into the following three (3) categories:

- **RESTRICTED** – This classification applies to the most sensitive business or authorized personal information that is intended for use strictly within select organization business groups. Its unauthorized disclosure would seriously and adversely impact the organization, its customers, its business, and its partners.
- **PRIVATE** – This classification applies to sensitive business information that is intended for use only within the organization. Its unauthorized disclosure could adversely impact the organization or its customers, suppliers, business partners, or users.
- **GENERAL** – This classification applies to information that has been approved by the organization management for release internally and with verified external partners. By definition, there is no such thing as unauthorized internal disclosure of this information, and it may be disseminated internally without potential harm.

ILYM policies require that company records, regardless of format, must be retained for specific periods of time and then disposed of in accordance with laws, regulatory requirements, industry requirements, or specific business need.

ILYM policies and procedures clearly define the disposal of both electronic and hardcopy media that stores company information classified as Restricted, Private or General. ILYM maintains disposal policies for electronic media. This policy also applies to sanitizing electronic media and equipment for reuse within the company. For hardcopy information, the policy addresses the requirement to destroy documents so the information on them cannot be recovered.

ILYM policies dictate the use of encryption to protect sensitive data, both in storage and in transmission. The policy conforms to all applicable provincial regulations, or applicable industry requirements pertaining to protection of sensitive and confidential information that require encryption.

ILYM has implemented procedures to support the use of cryptographic techniques, including secret key and public key techniques. Also, sensitive data that is encrypted in storage or during transmission is done so using strong cryptographic techniques and protocols based on current best practices that meet or exceed the federal, state, or provincial regulation, or applicable industry requirements. Password and keys are not transmitted together with the information and wireless networks transmitting sensitive data or connected to data environments containing sensitive data use current practices that meet or exceed the federal, state, or provincial regulation, or applicable industry requirements.

Disclosure of Security Incidents

ILYM diligently responds to alerts received from various monitoring tools deployed at the perimeter of the network, within the network and applications. As of the examination date, ILYM did not have any security incidents significant enough to trigger external communications.

IV. OTHER RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION SYSTEMS, AND MONITORING CONTROLS

The management of ILYM has established a system of internal controls aligned with the integrated framework established by the Committee of Sponsoring Organizations (“COSO”). The following processes describe management’s approach to addressing the COSO integrated framework.

ILYM believes in maintaining a well-trained staff capable of exceeding customers’ expectations. As a result, numerous qualitative and quantitative elements are implemented and utilized throughout the organization. These elements, which are permeated within the organization’s control structure, consist of the following:

Boundaries of the System

The boundaries of the system are the physical and logical perimeters of that portion of an entity’s operations that are used to achieve management’s business objectives of the system. The boundaries include all components of the system for which the entity is responsible, including those provided by vendors or other third parties.

The boundaries or aspects of the System covered by the Description are depicted below.

Control Environment

ILYM’s control environment reflects the overall attitude, awareness, and actions of ILYM management, and other stakeholders concerning the importance of control and its emphasis within the entity.

The organizational structure, separation of job responsibilities by departments and business function, documentation of policies and procedures are the methods used to define, implement and assure effective operational controls. At ILYM’s headquarters, the staff have an active involvement. Processes and procedures are monitored and performed, and oversight is administered by management.

Personnel Policies and Procedures

ILYM has formal hiring standards and guidelines that are designed to assist in the selection and retention of qualified applicants for specific job responsibilities. Hiring policies include experience requirements, age verification, and completion of all application forms, background checks, and personal reference checks. All employees will be assigned Security Awareness Training at the time of hire and annually. This training system tracks completion of assignments and verifies understanding of the training. The ILYM employee handbook which contains areas related to employee conduct, terminations and sanctions, hiring practices, management responsibilities and safety information is provided to employees at time of hire and reviewed and updated annually.

Employee training is accomplished through on-the-job training, in-house training and external education programs. ILYM utilizes departmental training courses. ILYM managers are

responsible for ensuring that required training is completed and for encouraging employee training and development on an annual basis.

Management Control Philosophy

ILYM's management is committed to maintaining the highest levels of ethics and integrity. Management endeavors to foster this culture by promoting cooperation, coordination, communications and alignment of interests within and among the ILYM employees, clients and involved parties. As a matter of policy, all ILYM employees are required to review the ILYM employee handbook and all updates upon their release. Senior management formally meets at least annually to discuss all aspects of ILYM business and operations. Each department also meets regularly to discuss current matters.

Segregation of Duties

ILYM maintains appropriate segregation of duties that must be applied to all processes related to designated applications, systems and network infrastructure.

ILYM maintains roles and job responsibilities that assign and monitor job function by employee to ensure not only that there is a proper segregation of duties within roles and responsibilities, but that critical functions also have primary and secondary owners, in the case of the primary owner being unavailable.

Asset Management

An asset inventory is maintained by the managed service provider. Additions, removals, and decommissioned assets are logged and recorded in the asset inventory tool.

No information technology asset may be placed into service in the Company's network or other infrastructure without being inventoried. Inventory records of all critical technology assets are maintained so long as ILYM continues to own or lease the asset, as well as retired and disposed assets.

The inventory records are kept in an asset tracking system and are reviewed for accuracy annually at minimum. Periodic checks of the system are also made to verify accuracy of the assets. Each asset is matched to a serial number record in the electronic asset management system.

Security Awareness Training

ILYM personnel are assigned security awareness training initially upon hire and annually while an employee at ILYM. This training incorporates information related to the security of ILYM and client information. Employees can find all current policies related to security on the ILYM SharePoint site.

Responsibility and accountability for the ILYM system security policies are defined and are communicated to personnel responsible for implementing them via the ILYM SharePoint site.

Risk Assessment Process

ILYM serves a wide range of clients in an even wider range of configurations that constantly

challenge its established security policy and procedures. ILYM's risk assessment processes generally consist of the following elements:

- Assessing the sufficiency of corporate policies, procedures, systems, tools and other arrangements in place to control risk;
- Identifying potential risks in existing or emerging technology, products, security and services;
- Identifying potential sources of risk and recommending areas for management to develop and implementing policies and procedures that mitigate the identified risk areas;
- Monitoring and evaluating the operating effectiveness of existing controls in light of changes resulting from growth, new or modified systems, new personnel and or roles, and external security risk factors;
- Monitoring the environment to determine risks were assessed accordingly and remediated where necessary.

Risk Management

Risk assessment reviews are performed at least annually, in conjunction with Clarus IT, to identify potential threats of disruption to system operations which would impair system. This risk assessment may include changes to the IT specific areas of access management, change management, employee risks, access to PII, new security risks, and changes to user requirements. Results of these risk assessments are reviewed by Senior Management. If necessary, ILYM updates applicable policies based on its assessment of the risks associated with the identified threats. As part of the regular risk assessment, management tracks, prioritizes, and discusses material for potential security vulnerabilities and issues. Milestones and potential remediation steps are documented as part of the risk assessment.

Information and Communication Systems

ILYM has developed and implemented documented security policies and procedures for information security. These policies and procedures are reviewed, updated and approved on an annual basis or more frequently as merited by significant business, operational and/or technical changes. Management has assigned responsibility for the maintenance and enforcement of the security policy to the CEO. Senior management, as part of strategic planning, considers developments in technology as well as the impact of applicable laws and regulations on the entity's security policy. All policies and procedures, including those relevant to security and confidentiality are accessible by staff on the company intranet.

Monitoring Controls

Automated tools provide real-time monitoring and notification of suspected wrongdoing and vulnerability exploitation in a range of ILYM technology aspects including network, production environment, operating system security parameters, potential security breaches via an intrusion detection system, and firewalls.

Monitoring for administrative access, event logs, and changes to systems are enabled for the environment. Whenever certain operational thresholds are reached, the monitoring system alerts Clarus IT personnel, who assess and review the log files as appropriate.

Systems are implemented to monitor key operational metrics and to notify appropriate personnel when certain operational thresholds are reached. To help prevent and mitigate downtime and customer impact, the monitoring of these key operational metrics is automated. This monitoring includes but is not limited to storage and drive space availability, CPU and memory utilization, required patches and updates, and anti-virus alerts.

Logical and Physical Access

ILYM maintains system policies that manage access to applications, systems, hardware and the execution of automated functions. These policies encompass all ILYM employees, contractors, consultants, temporaries and other non-employee staff requiring access.

ILYM procedures dictate the process of requesting and assigning logical access rights. Logical access is provisioned according to the principle of role. Level of access to infrastructure and systems needed per job responsibilities is granted. The duties related to the creation of access rights are segregated between the individual with authority to determine who has access to systems and data and the individual assigning the access rights in order to minimize the risk of fraudulent activity. ILYM uses role-based group access to restrict access to system resources and restricts access to the resources to the users' granted permissions to that respective resource based on job responsibilities and/or relationship to the entity. On-boarding and Off-boarding procedures and checklists are sent to the managed service provider who in turn provisions or removes access based on the checklist. All access not explicitly authorized is forbidden.

All logical access uses authentication for the individual application system being accessed using a valid and unique user ID which is authenticated by an associated password. Shared accounts are not used to support the system. On an annual basis, access reviews are performed by ILYM and changes resulting from the review are sent to the managed service provider so updates can be made.

Multi-factor authentication is required for access to environments that host production systems.

ILYM maintains password configurations which establish a general minimum standard for passwords that includes the creation of strong passwords, protection of passwords, and the frequency of renewing passwords. The configurations apply to all individuals, employees and non-employees, who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any ILYM facility, has access to the network, or stores any non-public information.

The password standards also dictate how IT manages the process of creating and communicating passwords. Resetting, deleting and modifying passwords or user IDs, credentials, and other identifier objects must only be done by authorized members of the managed service provider.

Physical access to corporate facilities is secured with a keypad system and specific keycode entry which is specific to each employee. No longer are change codes necessary. The Kisi system is utilized with SSO integration with Office 365. When a user is terminated/leaves, they lose access when their Office 365 account is disabled.

Incident Response

ILYM has a documented Incident Response policy for the identification and mitigation of breaches in security and confidentiality and for incidents that may result in the interruption of system or service availability. The policy includes a process for staff members to submit observations and concerns directly to senior management via phone, in person, and includes a documented report.

The policy outlines that when a potential incident related to system security and confidentiality is detected or reported, a defined incident management process is initiated by authorized personnel. Corrective actions are implemented in accordance with defined policies and procedures, and all incidents, including open incidents, are tracked by management in the documented plan of actions and milestones matrices until they are resolved. Closed incidents, including those addressing security, availability, and/or confidentiality system related policies, are reviewed by management for appropriate resolution.

For any confirmed incidents or major updates that affect the security and confidentiality of customer data, including the handling, destruction, maintenance, storage, back-up, and distribution or transmission of confidential information, ILYM staff have been designated to communicate with customers, legal authorities, and the public as appropriate.

Network Security

ILYM maintains a configuration that applies to network devices including but not limited to cloud and on-premises infrastructure, firewalls, routers, switches, network security devices, and network monitoring devices.

Administrative access to cloud and on-premises infrastructure, hardware, O/S, virtualization, database and other system and component configuration settings is restricted to a limited number of staff members according to job responsibilities.

Anti-Virus and Malware

Access to administer anti-virus/anti-malware mechanisms is limited to a small number of Managed Services IT staff and cannot be removed or altered on workstations. Local firewall attributes of the AV product lock down the local workstation and laptop ports. AV monitoring is performed by members of the Managed Services IT team. IT personnel receive notification via a centrally managed console of any detected/quarantined items, as well as signature updates/scanning failures.

Patch Management

ILYM maintains procedures around the patch management process. All patches are implemented within on a monthly basis. The patching procedure applies to all equipment that is owned or leased by ILYM such as servers, workstations, laptops, software, and network devices.

Change Management

ILYM policies dictate the configuration and change management processes to help ensure the systematic proposal, review, justification, and implementation of changes to the ILYM infrastructure to reduce the risk to customer and employee impacting errors and to mitigate the risk of malicious software or hardware being introduced by the change. All changes made to the infrastructure are tracked using Dynamics PSA.

The Change Management policy is reviewed and updated annually and whenever a policy change is required. Production environments are logically segregated from non-production environments. Patches are applied, at minimum, to workstations and servers on a monthly basis.

Business Continuity and Disaster Recovery

ILYM has a Business Continuity Plan (BCP) with detailed procedures to help ensure that ILYM maintains high availability while ensuring information confidentiality and security. At minimum, a tabletop test is conducted annually for disaster recovery. The test is recorded and reviewed by management. Documentation, including a checklist, is maintained which accounts for results of the test and areas of improvement.

The Business Continuity and Disaster Recovery Plan identifies critical infrastructure, systems, technology components, personnel, data, resources and restoration timeframes based on a business impact analysis. Business continuity and disaster recovery roles and responsibilities are defined in the policy, procedures, and plan. Should the entity's office locations be rendered non-viable for personnel work, provisions are in place for a shift to remote work for all ILYM personnel.

Periodic testing is conducted to ensure that members of the ILYM team are knowledgeable in their responsibilities and that recovery objectives can be satisfactorily met.

Following a BCP/DR actual event, a post-incident meeting is conducted to review results, identify root cause items and enact an improvement plan based on lessons learned. Should any needed changes to infrastructure or technology components be identified following a BCP/DR test or event, changes are proposed.

V. SUBSERVICE ORGANIZATIONS

ILYM uses subservice organizations to perform certain functions that support the delivery of services. The scope of this report does not include the controls and related trust services criteria at the carved-out subservice organizations. The following is a description of the services provided by the subservice organizations and the controls that are expected to be implemented.

Subservice Organization	Services Provided
Microsoft Azure	Infrastructure Hosting
Todyl	MXDR and SOC Monitoring Services

The following table presents controls that are assumed to be implemented by the carved-out subservice organizations, which ILYM has identified as necessary to achieve certain trust services criteria stated in the system description.

Trust Services Criteria	Complementary Subservice Organization Controls
<i>CC4.1 – The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.</i>	- Scheduled tasks that do not process as expected are followed-up periodically and resolved. - Operations and security personnel follow defined processes for resolving and escalating reported events.
<i>CC6.1 – The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.</i>	- Logical access to offline storage, backup data, systems and media requires authorization, and access is reviewed periodically. - Firewalls and intrusion prevention systems are used and configured to prevent unauthorized access. The events are logged and reviewed. - Intrusion detection systems (IDS) are in place to monitor Web traffic and identify potential patterns or threats. - All access to system components requires that users are authenticated through unique user IDs and passwords.
<i>CC6.2 – Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.</i>	The subservice organizations restrict access to databases that are fully hosted and managed by ensuring access to the system is restricted to authorized personnel using role-based access and access control lists, performing periodic user access reviews, and access is removed in a timely manner when no longer needed.
<i>CC6.4 – The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.</i>	- Physical security policies and procedures are in place to guide personnel regarding restricting access to the facility. - Physical access to secure areas (server rooms, data centers, etc.) is restricted to authorized personnel, and entry or access to physical assets remain locked.

Trust Services Criteria	Complementary Subservice Organization Controls
<i>CC6.5 – The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity’s objectives.</i>	- Physical security policies and procedures are in place to guide personnel regarding discontinuing logical and physical protections over physical assets. - Physical access to secure areas (server rooms, data centers, etc.) is restricted to authorized personnel, and entry or access to physical assets remain locked.
<i>CC6.6 – The entity implements logical access security measures to protect against threats from sources outside its system boundaries.</i>	- Firewalls and intrusion prevention systems are used and configured to prevent unauthorized access. The events are logged and reviewed. - Intrusion detection systems (IDS) are in place to monitor Web traffic and identify potential patterns or threats.
<i>CC6.7 – The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity’s objectives.</i>	- Secure data transmission protocols are used to encrypt sensitive and confidential data when transmitted over public networks. - A mobile device management system is in place to manage the mobile supporting services.

Monitoring of Subservice Organizations

The subservice organizations are periodically assessed to determine if they perform services for ILYM relevant to the SOC 2 criteria used by the company to create its own annual SOC 2 audit report. ILYM works directly with the subservice organization Clarus IT, to ensure that ILYM’s SOC 2 trust services criteria are directly met by the carved-out subservice organizations own SOC 2 controls and complementary user-entity controls. ILYM also works directly with Clarus IT to ensure that control system definitions and reporting periods align to support ILYM’s obligations to its users for SOC 2 reporting.

VI. INDEPENDENT SERVICE AUDITOR'S DESCRIPTION OF CONTROLS

Key	Control Activity	Reference Links
I-1 ILYM Control	IL YM has an employee handbook which is reviewed and updated annually.	CC1.1 ; CC1.5
I-2 ILYM Control	New hires must undergo a background check as part of the onboarding process.	CC1.1
I-3 ILYM Control	New hires are required to sign an employment contract which includes confidentiality notices and disclosure of information requirements.	CC1.1
I-4 ILYM Control	The entity has an established Information Security policy. The policy is reviewed at least annually.	CC1.1 ; CC1.3 ; CC1.5 ; CC2.2
I-5 ILYM Control	As part of IL YM Group, Inc.'s risk assessment processes, risks around vendor access to data are assessed.	CC1.3 ; CC1.4 ; CC3.2 ; CC9.2
I-6 ILYM Control	Roles and responsibilities for the governance of information security and classification of data within IL YM Group, Inc. are formally documented and communicated internally through the Data Management policy.	CC1.3 ; CC1.4 ; CC5.3 ; CC9.2
I-7 ILYM/Clarus Control	Quarterly reviews are held to communicate and align on relevant security threats, program performance, and resource prioritization.	CC1.3 ; CC4.1 ; CC5.2 ; CC5.3 ; CC7.1 ; CC7.2 ; CC7.4
I-8 ILYM Control	The Executive Management team Charter is formally documented and outlines the roles and responsibilities to the team.	CC1.2
I-9 ILYM Control	All personnel are enrolled in security awareness training at least annually. Records of training completion are documented and retained for tracking purposes.	CC1.4

Key	Control Activity	Reference Links
I-10 ILYM/Clarus Control	Technical documentation (functional architecture diagram and security architecture documentation) for internal users is available on the company's intranet site. This documentation delineates the boundaries of the system.	CC2.1
I-11 ILYM Control	Security policies are made available to employees on an internal online document repository.	CC2.1 ; CC2.2
I-12 Clarus Control	ILYM Group, Inc.'s assets are logged and have designated owners.	CC2.1 ; CC6.1
I-13 ILYM Control	Customer responsibilities are described on the customer website in the "Terms of Use" tab.	CC2.3
I-14 ILYM Control	A formally documented Risk Management policy is in place and updated annually.	CC2.3 ; CC3.1
I-15 ILYM Control	A client contact form is available on the public facing website. Clients can address any questions including security related issues.	CC2.3
I-16 ILYM Control	The entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	CC3.1 ; CC3.2 ; CC3.3 ; CC3.4
I-17 ILYM Control	Identified risks are rated using a risk evaluation process and ratings are reviewed by management.	CC3.1 ; CC3.2 ; CC3.3 ; CC3.4
I-18 ILYM Control	ILYM Group, Inc. conducts penetration tests annually.	CC4.1 ; CC5.1 ; CC6.8 ; CC7.1 ; CC7.2
I-19 ILYM/Clarus Control	Management prepares a remediation plan to formally manage the resolution of findings identified from the annual penetration test.	CC4.2 ; CC5.1 ; CC9.1

Key	Control Activity	Reference Links
I-20 ILYM/Clarus Control	A Business Continuity Plan is in place and available to employees. The plan is tested annually to validate that availability requirements can be met in the event of a business interruption.	CC5.1 ; CC7.5
I-21 Clarus Control	A data restore is completed at least quarterly to validate data can be recovered.	CC5.1 ; CC7.4 ; CC7.5 ; CC9.1
I-22 ILYM Control	Client questionnaires are utilized in conjunction with the annual risk assessment to develop and review control activities.	CC5.2
I-23 Clarus Control	ILYM Group, Inc. maintains an inventory of system devices, which is reconciled annually.	CC6.1
I-24 ILYM/Clarus Control	A termination form for logical access that is no longer required in the event of a termination is documented and sent to the IT service provider. Access is revoked within one business day.	CC6.1 ; CC6.2 ; CC6.3
I-25 Clarus Control	Multi-factor authentication is required for access to environments that host production systems.	CC6.1 ; CC6.6
I-26 Clarus Control	A role-based security process has been defined with an access control system that is required to user roles when possible.	CC6.1
I-27 Clarus Control	Password complexity standards are established to enforce control over access control software passwords.	CC6.1
I-28 Clarus Control	System security is configured to require users to change their password upon initial sign-on and every 365 days thereafter.	CC6.1
I-29 Clarus Control	ILYM Group, Inc. performs account and access reviews annually.	CC6.1 ; CC6.3

Key	Control Activity	Reference Links
I-30 ILYM/Clarus Control	In the event of a modification of access (i.e., role change, request for different access rights), newly administered access rights are documented and tracked.	CC6.2 ; CC6.3
I-31 ILYM/Clarus Control	In the event of a new hire, new user access rights are initiated by managers and tracked through the new hire form which is sent to the MSP.	CC6.2 ; CC6.3
I-32 ILYM/Clarus Control	Physical access that is no longer required in the event of a termination or role change is revoked. A ticket is opened with the MSP to disable access.	CC6.4
I-33 ILYM/Clarus Control	ILYM Group, Inc. performs physical access account reviews at least annually; corrective action is taken where applicable.	CC6.4
I-34 ILYM/Clarus Control	Physical access to corporate facilities is secured with a keypad system and entry mechanism (Keycard or Phone App) which is specific to each employee.	CC6.4
I-35 ILYM Control	The sharing of access codes and tailgating are prohibited by policy.	CC6.4
I-36 Clarus Control	An asset decommission log is maintained to account for physical assets that are no longer in use.	CC6.5 ; C1.2
I-37 Clarus Control	ILYM maintains a data wipe process for all company owned laptops. Upon user termination, company laptops are retrieved and wiped clean of all user and client information.	CC6.5 ; C1.2
I-38 ILYM Control	Formal data retention and disposal procedures are in place to guide the secure disposal of the company's and customers' data.	CC6.5 ; C1.2

Key	Control Activity	Reference Links
I-39 ILYM Control	A data classification policy which includes a data management lifecycle and identification of restricted and private information, is reviewed and approved by management.	CC6.5 ; C1.1
I-40 Clarus Control	User IDs, passwords, and multi-factor access requirements, are utilized to reduce the risk of unauthorized access.	CC6.6
I-41 Clarus Control	Network traffic to and from untrusted networks passes through a policy enforcement point; firewall rules are established in accordance to identified security requirements and business justifications.	CC6.6
I-42 Clarus Control	Changes to firewall hardening standards can only be performed by the Managed Service Provider.	CC6.6
I-43 Clarus Control	A Secure Sockets Layer (SSL) protocol is utilized to encrypt data transmitted to Internet-facing servers.	CC6.6 ; CC6.7
I-44 ILYM/Clarus Control	A current network diagram (including wireless networks) exists and is updated whenever there are network changes or reviewed annually.	CC6.6
I-45 Clarus Control	Data in transit and at rest is encrypted.	CC6.7
I-46 Clarus Control	Storage for workstations and laptops is encrypted. Removable media for workstations and laptops are disabled where present. Exceptions for removable media permissions are tracked via email.	CC6.7
I-47 Clarus Control	The ability to install software on workstations and laptops is restricted to IT support personnel.	CC6.8

Key	Control Activity	Reference Links
I-48 Clarus Control	Antivirus software is configured to receive an updated virus signature at least daily.	CC6.8
I-49 Clarus Control	Antivirus software is installed on workstations, laptops, and servers supporting such software.	CC6.8
I-50 Clarus Control	ILYM Group, Inc. logs critical information system activity.	CC6.8 ; CC7.1 ; CC7.2
I-51 Clarus Control	Critical systems are monitored in accordance to predefined security criteria and alerts are sent to authorized personnel. Confirmed incidents are tracked to resolution.	CC7.2 ; CC7.3
I-52 Clarus Control	Backups are performed as per the defined schedule and backup logs are retained as per defined retention limit.	CC7.2
I-53 Clarus Control	An online ticketing tool is utilized to log and track incidents. Incidents are worked by the security team from opening through resolution.	CC7.3 ; CC7.4
I-54 ILYM Control	ILYM Group, Inc. defines policies and procedures for incident management. The policy is reviewed and approved annually.	CC7.3
I-55 Clarus Control	Production environments are logically segregated from non-production environments.	CC8.1
I-57 ILYM Control	The Change Management policy is reviewed and updated annually and whenever a policy change is required.	CC8.1
I-58 Clarus Control	Patches are applied, at minimum, to workstations and servers on a monthly basis.	CC8.1

Key	Control Activity	Reference Links
I-59 ILYM Control	Confidentiality commitments reflecting the organization's needs for the protection of information are included in applicable client agreements.	C1.1

Reference Table to the AICPA's Trust Services Criteria

Criteria	Criteria Description	Control Activity
CC1.0 Control Environment		
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	I-1 ; I-2 ; I-3 ; I-4
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	I-8
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	I-4 ; I-5 ; I-6 ; I-7
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	I-5 ; I-6 ; I-9
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	I-1 ; I-4
CC2.0 Communication and Information		
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	I-10 ; I-11 ; I-12
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	I-4 ; I-11

Criteria	Criteria Description	Control Activity
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	I-13 ; I-14 ; I-15
CC3.0 Risk Assessment		
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	I-14 ; I-16 ; I-17
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	I-5 ; I-16 ; I-17
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	I-16 ; I-17
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	I-16 ; I-17
CC4.0 Monitoring Activities		
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	I-7 ; I-18
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	I-19
CC5.0 Control Activities		

Criteria	Criteria Description	Control Activity
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	I-18 ; I-19 ; I-20 ; I-21
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	I-7 ; I-22
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	I-6 ; I-7
CC6.0 Logical and Physical Access Controls		
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	I-12 ; I-23 ; I-24 ; I-25 ; I-26 ; I-27 ; I-28 ; I-29
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	I-24 ; I-30 ; I-31
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	I-24 ; I-29 ; I-30 ; I-31
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	I-32 ; I-33 ; I-34 ; I-35

Criteria	Criteria Description	Control Activity
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	I-36 ; I-37 ; I-38 ; I-39
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	I-25 ; I-40 ; I-41 ; I-42 ; I-43 ; I-44
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	I-43 ; I-45 ; I-46
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	I-18 ; I-47 ; I-48 ; I-49 ; I-50
CC7.0 System Operations		
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	I-7 ; I-18 ; I-50
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	I-7 ; I-18 ; I-50 ; I-51 ; I-52
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	I-51 ; I-53 ; I-54

Criteria	Criteria Description	Control Activity
CC7.4	The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.	I-7 ; I-21 ; I-53
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	I-20 ; I-21
CC8.0 Change Management		
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	I-55 ; I-57 ; I-58
CC9.0 Risk Mitigation		
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	I-19 ; I-21
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	I-5 ; I-6
C1.0 Additional Criteria for Confidentiality		
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	I-39 ; I-59
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	I-36 ; I-37 ; I-38

EXHIBIT C

Complaint Filed: February 22, 2023

Hearing Date: May 19, 2025

Trial Date: Not Set

E-Service Provider: CaseAnywhere

ILYM | GROUP, Inc.

SETTLEMENT ADMINISTRATION EXPERTS

Case Name: Grentz v. American Airlines

Friday, February 21, 2025

Requesting Attorneys Name:

E-Mail:

ILYM Contact:

E-Mail:

Contact Number:

Daniel Brome

dbrome@nka.com

Sean Stonehouse

sean.stonehouse@ilymgroup.com

408.691.5605

Estimate For Administrative Solutions: Class & PAGA

KEY ASSUMPTIONS	
Total Number of Class Members	2,000
Estimated Percentage of Remails	15%
Certified Spanish Translation	No
ILYM Group Static Website	Yes
Case Duration (Years)	1

Summary Estimate: ILYM Group Fees & Expenses

Case Startup:	\$650.00
Project Management & Noticing:	\$2,650.00
Notification & Mailing:	\$5,980.00
Distribution (Includes EIN, Bank Acct * /QSF Setup):	\$5,750.00
Case Conclusion:	\$725.00

Total ILYM Fees & Expenses: \$15,755.00



Case Name: Grentz v. American Airlines

Friday, February 21, 2025

Requesting Attorneys Name: Daniel Brome

Activity	Rate Type	Unit Cost	Volume	Amount
CASE STARTUP				
Initial Setup - Import and Formatting of Data*	Hourly	\$150.00	2	\$300.00
Programming of Class Database	Hourly	\$175.00	2	\$350.00
Subtotal				\$650.00

**ILYM assumes that data will be in a standard format. Client will be notified immediately if not in standard format to correct data or ILYM can convert to standard format @ \$150.00 per hour.*

PROJECT MANAGEMENT				
Project Manager (Case notification and maintenance)	Hourly	\$120.00	4	\$480.00
Staff Hours for Processing Returned Mail	Hourly	\$70.00	2	\$140.00
Staff Hours for Processing Opt-Outs, Disputes & Objection(s)	Hourly	\$70.00	2	\$140.00
Report Processing	Hourly	\$70.00	2	\$140.00
NCOA	Flat Rate	\$500.00	1	\$500.00
Toll Free Customer Service Representative (IVR)	Flat Fee	\$500.00	1	\$500.00
Static Website	Flat Fee	\$750.00	1	\$750.00
Weekly Reports	Flat Rate	\$750.00	1	Waived

Subtotal \$2,650.00

Fulfillment of Notice (9 pages), English	Per Piece	\$1.75	2,000	\$3,500.00
USPS First Class Postage	Per Piece	\$0.69	2,000	\$1,380.00
Re-Mails (Forward/Skip trace Undeliverables)	Per Piece	\$2.00	300	\$600.00
Email Notification & Delivery	Flat Fee	\$500.00	1	\$500.00

Subtotal \$5,980.00

ILYM | GROUP, Inc.
SETTLEMENT ADMINISTRATION EXPERTS

Case Name: Grentz v. American Airlines

Friday, February 21, 2025

Requesting Attorneys Name: Daniel Brome

Activity	Rate Type	Unit Cost	Volume	Amount
DISTRIBUTION (Includes EIN, Bank Acct * /QSF Setup)				
Distribution Setup & Management	Hourly	\$150.00	2	\$300.00
Account Reconciliation & Distribution Reporting	Hourly	\$125.00	2	\$250.00
Check, Stub & Release - Print & Mail (1099)	Per Check	\$1.00	2,000	\$2,000.00
USPS First Class Postage	Per Piece	\$0.64	2,000	\$1,280.00
Re-Mails (Forward/Skip trace Undeliverables up to 10%)	Per Piece	\$1.50	200	\$300.00
Preparation of Taxes	Hourly	\$120.00	1	\$120.00
Annual Filing of Tax Return	Per Year	\$1,500.00	1	\$1,500.00

**Additional Bank fees may apply*

Subtotal \$5,750.00

CASE CONCLUSION				
Data Manager Final Reporting	Hourly	\$100.00	1	\$100.00
Process Unclaimed Funds to Cy Pres	Flat Fee	\$500.00	1	\$500.00
Declaration	Hourly	\$125.00	1	\$125.00

Subtotal \$725.00

TOTAL CASE ESTIMATE: \$15,755.00

Total Case Estimate (To Not Exceed): \$15,755.00

All services to be provided by ILYM Group, Inc. (hereinafter, "ILYM") to Client shall be subject to the following terms and conditions:

Services: Subject to the terms hereof, ILYM agrees to provide the Client with Administration Services (hereinafter, "services") as specified in the Proposal provided to Client to which these Terms and Conditions are attached. The estimate is in good faith and does not cover any applicable taxes and fees. The estimate does not make provision for any services or class members/size not delineated in the request for proposal or stipulations. Such services do not in any way constitute legal services or advice. ILYM is performing its services as an Independent Contractor and neither it nor its employees shall be deemed to be employees of the Client.

Mailing and Data Conversion: ILYM's database administration assumes the Client will provide complete data that includes all information required to send notifications and complete the administration process. Data must be provided in a complete, consistent, standardized electronic format. ILYM's standard format is Microsoft Excel, however, ILYM may accept other formats at its discretion. Further developments or enhancements to non-standardized data will be billed to Client by ILYM on a time and materials basis, according to ILYM's Standard Rates.

Charges for Services: Charges to the Client for services shall be on a time and materials basis at our prevailing rates, as the same may change from time to time. Any fee estimates set forth in the proposal are estimates only, based on information provided by Client to ILYM. Actual fees charged by ILYM to Client may be greater or less than such estimate, and Client shall be responsible for the payment of all such charges and expenses in accordance with Section 5 hereof. Charges incurred related to resolving post distribution withholdings and related corrective files due to voids and re-issues of payments and related correspondence with state and federal taxing authorities will not be charged to the Client to the extent that funds are received from the taxing authorities offset these charges. ILYM may derive financial benefits from financial institutions in connection with the deposit and investment of settlement funds with such institutions, including without limitation, discounts on eligible banking services and fees, and loans at favorable rates.

Indemnification: Client will indemnify and hold ILYM (and the officers, employees, affiliates and agents harmless against any Losses incurred by ILYM, arising out of, in connection with, or related to (i) any breach of the terms by Client; (ii) the processing and handling of any payment by ILYM in accordance with Client's instructions, including without limitation, the imposition of any stop payment or void payment on any check or the wrongful dishonor of a check by ILYM pursuant to Client's instructions.

Payment of Charges: ILYM reserves the right to request payment of postage charges and 50% of the final administration charges at the start of the case. ILYM bills are due upon receipt unless otherwise negotiated and agreed to with the Client. In the event settlement terms provide that ILYM is to be paid out of the Settlement Fund, ILYM will request that Counsel endeavor to make alternate payment arrangements for ILYM charges that are due at the onset of the case. The entire remaining balance is due and payable at the time the Settlement Account is funded by, or no later than the time of disbursement. Decisions of the court and actions of the parties, including disapproval or withdrawal of a settlement, do not affect the Client's liability to ILYM for payment of services. Services are not provided on a contingency fee basis.

Confidentiality: ILYM maintain reasonable and appropriate security measures and safeguards to protect the security and confidentiality of Client data provided to ILYM by Client in connection herewith. Should ILYM ever be notified of any judicial order or other proceedings in which a third party seeks to obtain access to the confidential data created by or for the Client, ILYM will promptly notify the Client, unless prohibited by applicable law. The Client shall have the option to (1) provide legal representation at the Client's expense to avoid such access or (2) promptly reimburse ILYM for any of its costs, including attorneys' fees, reasonably incurred in avoiding, attempting to avoid or providing such access and not paid by the entity seeking the data. If ILYM is required, pursuant to a court order, to produce documents, disclose data, or otherwise act in contravention of the obligations imposed by this Agreement, or otherwise, with respect to maintaining the confidentiality, proprietary nature and secrecy of the produced documents or disclosed data, ILYM will not be liable for breach of said obligation.

Data Rights: ILYM does not convey nor does the Client obtain any right in the programs, system data, or materials utilized or provided by ILYM in the ordinary course of business in the performance of this Agreement.

Document Retention: Unless directed otherwise in writing by Client, ILYM will destroy undeliverable mail on the effective date of the settlement or the date that the disposition of the case is no longer subject to appeal or review, whichever is later. ILYM will maintain claim forms and other correspondence for one year after final distribution of funds or benefits, or until the date that the disposition of the case is no longer subject to appeal or review, whichever is later.

Limitation of damages: ILYM is not responsible to the Client for any special, consequential or incidental damages incurred by Client. Any liability of ILYM to the Client shall not exceed the total amount billed to the Client for the particular services that give rise to any loss.

Termination: The services to be provided under this Agreement may be terminated, at will by the Client upon at least 30 calendar days' prior written notice to ILYM. The Client's obligation to pay for services or projects in progress at the time of notice of withdrawal shall continue throughout that 30 day period. ILYM may terminate this Agreement (i) with 10 calendar days' prior written notice, if the Client is not current in payment of charges or (ii) in any event, upon at least 3 months' prior written notice to the Client.

Notice: Any notice required or permitted hereunder shall be in writing and shall be delivered personally, or sent by registered mail, postage prepaid, or overnight courier service to the responsible officer or principal of ILYM or the Client, as applicable, and shall be deemed given when so delivered personally, or, if mailed, five days after the date of deposit in United States mail, or, if sent by courier, one business day after delivery to such courier service.

Force Majeure: To the extent performance by ILYM of any of its obligations hereunder is substantially prevented by reason of any act of God or by reason of any other matter beyond ILYM's reasonable control, then such performance shall be excused and this Agreement, at ILYM's option, be deemed suspended during the continuation of such condition and for a reasonable time thereafter.

Waiver of Rights: No failure or delay on the part of a party in exercising any right hereunder will operate as a waiver of, or impair, any such right. No single or partial exercise of any such right will preclude any other or further exercise thereof or the exercise of any other right. No waiver of any such right will be effective unless given in a signed writing.

Jurisdiction: The parties hereto submit to the jurisdiction of the Court of the applicable case for purposes of any suit, action or proceeding to enforce any provision of, or based on any right arising out of, this Agreement. The parties hereto hereby waive any objection to the laying of venue of any such suit, action or proceeding in the Court.

Entire Agreement: These terms and conditions and the proposal embody the entire agreement between the parties with respect to the subject matter hereof, and cancels and supersedes all prior negotiations, representations, and agreements related thereto, either written or oral, except to the extent they are expressly incorporated herein. No changes in, additions to, or waivers of, the terms and conditions set forth herein will be binding upon any party, unless approved in writing by such party's authorized representative.