THIRD AMENDMENT TO AGREEMENT
BETWEEN THE COUNTY OF SAN MATEO AND
CHANNEL PARITY INCORPORATED

THIS THIRD AMENDMENT TO THE AGREEMENT, entered into this _____ day of

_____, 20_____, by and between the COUNTY OF SAN MATEO, hereinafter

called "County," and CHANNEL PARITY INCORPORATED, hereinafter called

"Contractor";

W I T N E S S E T H:

WHEREAS, pursuant to Government Code section 31000, County may contract with independent contractors for the furnishing of such services to or for County or any Department thereof;

WHEREAS, the parties entered into an agreement on June 24, 2013 (the "Agreement") for Syntellect System in the amount of $100,000 for the term of June 1, 2013 through May 31, 2014; and

WHEREAS, on January 28, 2014, the parties amended the Agreement to provide system services for an additional twenty-five months, extending the term of the Agreement to June 30, 2016 and increasing the amount of funds by $300,000 for a total obligation of $400,000; and

WHEREAS, on November 23, 2015, the parties further amended the Agreement to upgrade MicroSoft Server 2003 with supported 2008 servers, increasing the amount of funds by $20,000 for a total obligation of $420,000; and

WHEREAS, on May 10, 2016 the parties further amended the Agreement to allow for the continuation of services while County issued a Request for Proposal for phone management system for the Benefits Eligibility Services Telecenter and Contact Call Center, extend the term to June 30, 2017, and add funds in the amount of $130,000 for a new total obligation of $550,000; and

WHEREAS, the parties now wish to further amend the Agreement to extend the term to June 30, 2018 and add funds in the amount of $130,000 for a new total obligation of $680,000 in order to allow for the continuation and update of services while County implements a new Voice Over Internet Protocol phone system for the Benefits Eligibility Services Telecenter.

NOW, THEREFORE, IT IS HEREBY AGREED BY THE PARTIES HERETO AS FOLLOWS:

1.   Section 2 – Contract Term – of the Agreement is amended to read as follows:

Contract Term The term of this Agreement shall be from June 1, 2013 to June 30, 2018, unless terminated earlier by the County.

2. Section 3 – Payments – of the Agreement is amended to read as follows:

Payments In consideration of the services rendered in accordance with all terms, conditions and specifications set forth herein and any Exhibit(s) or attachment(s) attached hereto, County shall make payment to Contractor in the manner specified herein and in Exhibit "B" "B1" and "B2". In the event that County makes any advance payments, Contractor agrees to refund any amounts in excess of the amount owed by County at the time of contract termination. County reserves the right to withhold payment if County determines that the quantity or quality of the work performed is unacceptable. This amendment extends services by an additional year in the amount of ONE HUNDRED THIRTY THOUSAND DOLLARS ($130,000). In no event shall total payment for services under this Agreement exceed SIX HUNDRED EIGHTY THOUSAND DOLLARS ($680,000).

3. Paragraph 20 – **Compliance with Living Wage** is hereby included in to the agreement as follows:

As required by Chapter 2.88 of the San Mateo County Ordinance Code, Contractor certifies all contractor(s) and subcontractor(s) obligated under this contract shall fully comply with the provisions of the County of San Mateo Living Wage Ordinance, including, but not limited to, paying all Covered Employees the current Living Wage and providing notice to all Covered Employees and Subcontractors as required under the Ordinance.

4. Attachment P— Personally Identifiable Information Requirements for County Contractors, Subcontractors, Vendors and Agents – is attached to the Agreement and its terms and conditions are incorporated by reference.

5. **All other terms and conditions of the Agreement dated June 24, 2013 and subsequent amendments between the County and Contractor shall remain in full force and effect.**

In witness of and in agreement with this amendment's terms, the parties, by their duly authorized representatives, affix their respective signatures:

For Contractor: **CHANNEL PARITY INCORPORATED**

Ron Rushing

_____   Date:___05/10/2017_____

Contractor's Signature

COUNTY OF SAN MATEO

By:_____

President, Board of Supervisors, San Mateo County

Date:_____

ATTEST:

By:_____

Clerk of Said Board

Attachment P
Personally Identifiable Information
Requirements for County Contractors, Subcontractors, Vendors and Agents

I.   Definitions

Personally Identifiable Information (PII), or Sensitive Personal Information (SPI), as used in Federal information security and privacy laws, is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. PII may only be used to assist in the administration of programs in accordance with 45 C.F.R. § 205.40, *et seq.* and California Welfare & Institutions Code section 10850.

a.   **"Assist in the Administration of the Program"** means performing administrative functions on behalf of County programs, such as determining eligibility for, or enrollment in, and collecting context PII for such purposes, to the extent such activities are authorized by law.

b.   **"Breach"** refers to actual loss, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other than authorized purposes have access or potential access to context PII, whether electronic, paper, verbal, or recorded.

c.   **"Contractor"** means those contractors, subcontractors, vendors and agents of the County performing any functions for the County that require access to and/or use of PII and that are authorized by the County to access and use PII.

d.   **"Personally Identifiable Information" or "PII"** is personally identifiable information that can be used alone, or in conjunction with any other reasonably available information, to identify a specific individual. PII includes, but is not limited to, an individual's name, social security number, driver's license number, identification number, biometric records, date of birth, place of birth, or mother's maiden name. PII may be electronic, paper, verbal, or recorded.

e.   **"Security Incident"** means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PII, or interference with system operations in an information system which processes PII that is under the control of the County or County's Statewide Automated Welfare System (SAWS) Consortium, or under the control of a contractor, subcontractor or vendor of the County, on behalf of the County.

f.   "**Secure Areas**" means any area where:

   i. Contractors administer or assist in the administration of County programs;
   ii. PII is used or disclosed; or
  iii. PII is stored in paper or electronic format.

II.   Restrictions on Contractor re Use and Disclosure of PII

a.   Contractor agrees to use or disclose PII only as permitted in this Agreement and only to assist in the administration of programs in accordance with 45 CFR § 205.50, *et seq.* and California Welfare & Institutions Code section 10850 or as otherwise authorized or required by law. Disclosures, when authorized or required by law, such as in response to a court order, or when made upon the explicit written authorization of the individual, who is the subject of the

PII, are allowable. Any other use or disclosure of PII requires the express approval in writing by the County. No Contractor shall duplicate, disseminate or disclose PII except as allowed in this Agreement.

b.   Contractor agrees to only use PII to perform administrative functions related to the administration of County programs to the extent applicable.

c.   Contractor agrees that access to PII shall be restricted to Contractor's staff who need to perform specific services in the administration of County programs as described in this Agreement.

d.   Contractor understands and agrees that any of its staff who accesses, discloses or uses PII in a manner or for a purpose not authorized by this Agreement may be subject to civil and criminal sanctions available under applicable Federal and State laws and regulations

III. <u>Use of Safeguards by Contractor to Protect PII</u>

a.   Contractor agrees to ensure that any agent, including a subcontractor, to whom it provides PII received from, or created or received by Contractor on behalf of County, agrees to adhere to the same restrictions and conditions contained in this Attachment PII.

b.   Contractor agrees to advise its staff who have access to PII, of the confidentiality of the information, the safeguards required to protect the information, and the civil and criminal sanctions for non-compliance contained in applicable Federal and State laws and regulations.

c.   Contractor agrees to train and use reasonable measures to ensure compliance by Contractor's staff, including, but not limited to (1) providing initial privacy and security awareness training to each new staff within thirty (30) days of employment; (2) thereafter, providing annual refresher training or reminders of the PII privacy and security safeguards to all Contractor's staff; (3) maintaining records indicating each Contractor's staff name and the date on which the privacy and security awareness training was completed; and (4) retaining training records for a period of three (3) years after completion of the training.

d.   Contractor agrees to provide documented sanction policies and procedures for Contractor's staff who fail to comply with privacy policies and procedures or any provisions of these requirements, including termination of employment when appropriate.

e.   Contractor agrees that all Contractor's staff performing services under this Agreement sign a confidentiality statement prior to accessing PII and annually thereafter. The signed statement shall be retained for a period of three (3) years, and the statement include at a minimum: (1) general use; (2) security and privacy safeguards; (3) unacceptable use; and (4) enforcement policies.

f.   Contractor agrees to conduct a background check of Contractor's staff before they may access PII with more thorough screening done for those employees who are authorized to bypass significant technical and operational security controls. Contractor further agrees that screening documentation shall be retained for a period of three (3) years following conclusion of the employment relationship.

g.   Contractor agrees to conduct periodic privacy and security reviews of work activity, including random sampling of work product by Contractor's staff by management level personnel who are knowledgeable and experienced in the areas of privacy and information

security in the administration of County's programs and the use and disclosure of PII. Examples include, but are not limited to, access to data, case files or other activities related to the handling of PII.

h.   Contractor shall ensure that PII is used and stored in an area that is physically safe from access by unauthorized persons at all times and safeguard PII from loss, theft, or inadvertent disclosure by securing all areas of its facilities where Contractor's staff assist in the administration of the County's programs and use, disclose, or store PII.

i.   Contractor shall ensure that each physical location, where PII is used, disclosed, or stored, has procedures and controls that ensure an individual who is terminated from access to the facility is promptly escorted from the facility by an authorized employee of Contractor and access is revoked.

j.   Contractor shall ensure that there are security guards or a monitored alarm system at all times at Contractor's facilities and leased facilities where five hundred (500) or more individually identifiable records of PII is used, disclosed, or stored. Video surveillance systems are recommended.

k.   Contractor shall ensure that data centers with servers, data storage devices, and/or critical network infrastructure involved in the use, storage, and/or processing of PII have perimeter security and physical access controls that limit access to only those authorized by this Agreement. Visitors to any Contractor data centers area storing PII as a result of administration of a County program must be escorted at all times by authorized Contractor's staff.

l.   Contractor shall have policies that include, based on applicable risk factors, a description of the circumstances under which Contractor staff can transport PII, as well as the physical security requirements during transport.

m.   Contractor shall ensure that any PII stored in a vehicle shall be in a non-visible area such as a trunk, that the vehicle is locked, and under no circumstances permit PII be left unattended in a vehicle overnight or for other extended periods of time.

n.   Contractor shall ensure that PII shall not be left unattended at any time in airplanes, buses, trains, etc., including baggage areas. This should be included in training due to the nature of the risk.

o.   Contractor shall ensure that all workstations and laptops, which use, store and/or process PII, must be encrypted using a FIPS 140-2 certified algorithm 128 bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk. It is encouraged, when available and when feasible, that the encryption be 256 bit.

p.   Contractor shall ensure that servers containing unencrypted PII must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review. It is recommended to follow the guidelines documented in the latest revision of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.

q.   Contractor agrees that only the minimum necessary amount of PII required to perform required business functions will be accessed, copied, downloaded, or exported.

r.   Contractor shall ensure that all electronic files, which contain PII data is encrypted when stored on any mobile device or removable media (i.e. USB drives, CD/DVD, smartphones, tablets, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm 128 bit or higher, such as AES. It is encouraged, when available and when feasible, that the encryption be 256 bit.

s.   Contractor shall ensure that all workstations, laptops and other systems, which process and/or store PII, must install and actively use an antivirus software solution. Antivirus software should have automatic updates for definitions scheduled at least daily. In addition, Contractor shall ensure that:

i.   All workstations, laptops and other systems, which process and/or store PII, must have critical security patches applied, with system reboot if necessary.
ii.   There must be a documented patch management process that determines installation timeframe based on risk assessment and vendor recommendations.
iii.   At a maximum, all applicable patches deemed as critical must be installed within thirty (30) days of vendor release. It is recommended that critical patches which are high risk be installed within seven (7) days.
iv.   Applications and systems that cannot be patched within this time frame, due to significant operational reasons, must have compensatory controls implemented to minimize risk.

t.   Contractor shall ensure that all of its staff accessing Personally Identifiable Information on applications and systems will be issued a unique individual password that is a least eight (8) characters, a non-dictionary word, composed of characters from at least three (3) of the following four (4) groups from the standard keyboard: upper case letters (A-Z); lower case letters (a-z); Arabic numerals (0-9) and special characters (!, @, #, etc.). Passwords are not to be shared and changed if revealed or compromised. All passwords must be changed every (90) days or less and must not be stored in readable format on the computer or server.

u.   Contractor shall ensure that usernames for its staff authorized to access PII will be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee within twenty- four (24) hours. Note: Twenty-four (24) hours is defined as one (1) working day.

v.   Contractor shall ensure when no longer needed, all PII must be cleared, purged, or destroyed consistent with NIST SP 800-88, Guidelines for Media Sanitization, such that the Personally Identifiable Information cannot be retrieved.

w.   Contractor shall ensure that all of its systems providing access to PII must provide an automatic timeout, requiring re-authentication of the user session after no more than twenty (20) minutes of inactivity.

x.   Contractor shall ensure that all of its systems providing access to PII must display a warning banner stating, at a minimum that data is confidential; systems are logged, systems use is for business purposes only by authorized users and users shall log off the system immediately if they do not agree with these requirements.

y.   Contractor will ensure that all of its systems providing access to PII must maintain an automated audit trail that can identify the user or system process which initiates a request for PII, or alters PII. The audit trail shall be date and time stamped; log both successful and failed accesses be read-access only; and be restricted to authorized users. If PII is stored in a database,

database logging functionality shall be enabled. The audit trail data shall be archived for at least three (3) years from the occurrence.

z.   Contractor shall ensure that all of its systems providing access to PII shall use role-based access controls for all user authentications, enforcing the principle of least privilege.

aa.   Contractor shall ensure that all data transmissions of PII outside of its secure internal networks must be encrypted using a Federal Information Processing Standard (FIPS) 140-2 certified algorithm that is 128 bit or higher, such as Advanced Encryption Standard (AES) or Transport Layer Security (TLS). It is encouraged, when available and when feasible, that 256 bit encryption be used. Encryption can be end to end at the network level, or the data files containing PII can be encrypted. This requirement pertains to any type of PII in motion such as website access, file transfer, and email.

bb.   Contractor shall ensure that all of its systems involved in accessing, storing, transporting, and protecting PII, which are accessible through the Internet, must be protected by an intrusion detection and prevention solution.

cc.   Contractor shall ensure that audit control mechanisms are in place. All Contractor systems processing and/or storing Personally Identifiable Information must have a least an annual system risk assessment/security review that ensure administrative, physical, and technical controls are functioning effectively and provide an adequate level of protection. Review shall include vulnerability scanning tools.

dd.   Contractor shall ensure that all of its systems processing and/or storing PII must have a process or automated procedure in place to review system logs for unauthorized access.

ee.   Contractor shall ensure that all of its systems processing and/or storing PII must have a documented change control process that ensures separation of duties and protects the confidentiality, integrity and availability of data.

ff.   Contractor shall establish a documented plan to enable continuation of critical business processes and protection of the security of PII kept in an electronic format in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this Agreement for more than twenty-four (24) hours.

gg.   Contractor shall ensure its data centers with servers, data storage devices, and critical network infrastructure involved in the use, storage and/or processing of PII, must include environmental protection such as cooling, power, and fire prevention, detection, and suppression.

hh.   Contractor shall establish documented procedures to backup PII to maintain retrievable exact copies of PIII. The documented backup procedures shall contain a schedule which includes incremental and full backups, storing backups offsite, inventory of backup media, recovery of PII data, an estimate of the amount of time needed to restore PII data.

ii.   Contractor shall ensure that PII in paper form shall not be left unattended at any time, unless it is locked space such as a file cabinet, file room, desk or office. Unattended means that information may be observed by an individual not authorized to access the information. Locked spaces are defined as locked file cabinets, locked file rooms, locked desks, or locked offices in facilities which are multi-use, meaning that there are Contractor's staff and non-Contractor

functions in one building in work areas that are not securely segregated from each other. It is recommended that all PII be locked up when unattended at any time, not just within multi-use facilities.

jj.   Contractor shall ensure that any PII that must be disposed of will be through confidential means, such as cross cut shredding or pulverizing.

kk.   Contractor agrees that PII must not be removed from its facilities except for identified routine business purposes or with express written permission of the County.

ll.   Contractor shall ensure that faxes containing PII shall not be left unattended and fax machines shall be in secure areas. Faxes containing PII shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them and notify the sender. All fax numbers shall be verified with the intended recipient before send the fax.

mm. Contractor shall ensure that mailings containing PII shall be sealed and secured from damage or inappropriate viewing of PII to the extent possible. Mailings that include five hundred (500) or more individually identifiable records containing PII in a single package shall be sent using a tracked mailing method that includes verification of delivery.

IV.   Reporting of Breaches Required by Contractor to County; Mitigation

a.   Contractor shall report to County within one business day of discovery, to the County contact listed in this agreement by email or telephone as listed in the of unsecured PII, if that PII was, or is, reasonably believed to have been accessed or acquired by an unauthorized person, any suspected security incident, intrusion or unauthorized access, use or disclosure of PII in violation of this Agreement, or potential loss of confidential data affecting this Agreement.

b.   Contractor understands that State and Federal Law requires a breaching entity to notify individuals of a breach or unauthorized disclosure of their PII. Contractor shall ensure that said notifications shall comply with the requirements set forth in California Civil Code section 1798.29, and 42 U.S.C. section 17932, and its implementing regulations, including but not limited to, the requirement that the notifications be made without unreasonable delay and in no event later than sixty (60) calendar days.

c.   Contractor agrees to promptly mitigate, to the extent practicable, any harmful effect that is known to Contractor stemming from a use or disclosure of PII in violation of the requirements of this Agreement, including taking any action pertaining to such use or disclosure required by applicable Federal and State laws and regulations.

V.   Permitted Uses and Disclosures of PII by Contractor

Except as otherwise limited in this schedule, Contractor may use or disclose PII to perform functions, activities, or services for, or on behalf of, County as specified in the Agreement; provided that such use or disclosure would not violate the Privacy Rule if done by County.

VI.   Obligations of County

a.   County shall provide Contractor with the notice of privacy practices that County produces in accordance with California Welfare and Institutions Code section 10850, as well as any changes to such notice.

b.   County shall notify Contractor of any changes in, or revocation of, permission by Individual to use or disclose PII, if such changes affect Contractor's permitted or required uses and disclosures.

c.   County shall notify Contractor of any restriction to the use or disclosure of PII that County has agreed to in accordance with California Welfare and Institutions Code section 10850.

VII. Permissible Requests by County

County shall not request Contractor to use or disclose PII in any manner that would not be permissible under the Privacy Rule if so requested by County, unless Contractor will use or disclose PII for, and if the Agreement provides for, data aggregation or management and administrative activities of Contractor.

VIII. Duties Upon Termination of Agreement

a.   Upon termination of the Agreement, for any reason, Contractor shall return or destroy all PII received from County, or created, maintained, or received by Contractor on behalf of County that Contractor still maintains in any form. This provision shall apply to PII that is in the possession of subcontractors or agents of Contractor. Contractor shall retain no copies of the PII.

b.   In the event that Contractor determines that returning or destroying PII is infeasible, Contractor shall provide to County notification of the conditions that make return or destruction infeasible. Upon mutual Agreement of the Parties that return or destruction of PII is infeasible, Contractor shall extend the protections of the Agreement to such PII and limit further uses and disclosures of such PII to those purposes that make the return or destruction infeasible, for so long as Contractor maintains such PII.

IX. Miscellaneous

a.   **Regulatory References.** A reference in this Attachment to a section in the Personally Identifiable Information Privacy Rule means the section as in effect or as amended, and for which compliance is required.

b.   **Amendment.** The Parties agree to take such action as is necessary to amend this Schedule from time to time as is necessary for County to comply with the requirements of the Privacy Rule and in accordance 45 CFR § 205.40, *et seq*. and California Welfare and Institutions Code section 10850.

c.   **Survival.** The respective rights and obligations of Contractor under this Attachment shall survive the termination of the Agreement unless and until the PII is destroyed or returned to the County.

d.   **Interpretation.** Any ambiguity in any provision in this Attachment shall be resolved in favor of a meaning that permits County to comply with the Privacy Rule.

e.   **Reservation of Right to Monitor Activities.** County reserves the right to monitor the security policies and procedures of Contractor.