California Department of Justice

Bureau of Criminal Identification and Investigative Services

Client Services Program
Live Scan Support Section

Private Service Provider Application Packet

Thank you for your interest in becoming a Private Service Provider and being a part of the Department of Justice's Applicant Communication Network

Pursuant to California Penal Code section 11077.2, the Office of the Attorney General was required to establish an Applicant Communication Network (ACN) to facilitate the submission of requests for Criminal Offender Record Information (CORI) to the Department of Justice (DOJ) for employment, licensing, certification, custodial child placement, and adoption purposes, effective July 1, 2004. Since its establishment, the ACN has enabled Private Service Providers (PSP) in California to connect to the DOJ for purposes of transmitting electronic applicant fingerprint transactions.

This packet will provide you with an understanding of the connection process and help you determine whether you would be able to connect to the ACN and submit Applicant fingerprints to the DOJ, as a PSP. The requirements for applying to become a PSP and establishing a connection to the DOJ's ACN are as follows:

- The business owner(s) must possess a valid "Fingerprint Roller Certificate" issued pursuant to California Penal Code section 11102.1. A copy of the Fingerprint Roller Certificate and the Departmental letter accompanying the certificate must be submitted to the DOJ for the Owner or each member of a Partnership or Corporation and for all employees operating the live scan device on behalf of the business. Certification information can be accessed on the Attorney General's Website at www.oag.ca.gov/fingerprints/finger_cert or by e-mailing fpcert@doj.ca.gov.

- The business owner(s) must provide a Live Scan Service Provider Security and Disclosure Certification form (Appendix A) with **original signature**. Additionally, a signed Security and Disclosure Certification form must be provided, with **original signature**, for each member of a Partnership or Corporation and for all employees operating the live scan device on behalf of the business.

- The business owner(s) must agree to all requirements set forth in the "Terms and Conditions for Private Service Providers in California" which establish the minimum internal controls deemed necessary by the DOJ to adequately protect the security and stability of the applicant communication network and the privacy rights of individual applicants. The "Terms and Conditions for Private Service Providers in California" are included in this application packet and must be submitted with **original signature**.

- The business owner(s) must establish a DOJ Billing Account for processing State and Federal CORI requests and their associated fingerprint fees. The Billing Account Application is included in this application packet. **Payment is due upon receipt of the monthly DOJ Accounting invoices. The Department strongly recommends establishing a separate bank account for the government fees you will be collecting on behalf of the DOJ and FBI. Failure to pay will result in the disconnection of your device(s) and permanently disable your billing number.**

- The business owner(s) must provide a copy of a valid City or County issued business license, showing clear indication of the owner's name, business name and business address.

Upon receipt of the required documents listed above, in one complete and accurate packet, the DOJ will conduct a more extensive background check utilizing various resources, in order to assist in determining the pre-approval or denial of all PSP applications. Once pre-approval is determined the following must be provided to the DOJ in order to complete the full application process:

- The business owner(s) is responsible for purchasing or leasing all hardware and software and must only use hardware and software that is currently approved and certified by the DOJ, the National Institute of Standards and Technology and the Federal Bureau of Investigation (FBI). A listing of California Certified Vendors is provided in this application packet. **You MUST contact the Live Scan Support Section, which provides oversight to PSPs, prior to purchasing any hardware or software from a third party not on the California Certified Vendors list provided in this application packet. If you do not comply with this requirement, the Department will not allow connection of your live scan device to the DOJ's ACN.**

- As a PSP, you must connect to the ACN through a California Certified Peer Service Provider. A Peer Provider guarantees their server prevents the editing, altering or changing of any record data transmitted; provides reasonable assurance that duplicate records are not forwarded to the DOJ; protects against outside access to sensitive data by their clients or general public through accidental or deliberate intrusion; has sufficient storage capacity to ensure all records are transmitted to the DOJ within 24 hours of receipt. The Peer Provider server is required to be located in a secure area, such as Data Centers which provide controlled access points and a Secure ID and entry process. Installation in an open area allowing physical access to anyone without authorization and without the completion of a secure access process is a security violation and should be immediately reported. The main security requirement for a PSP to indirectly connect to the applicant communication network includes:

  - Encryption utilizing a minimum 128 bit key and if a firewall is required, it should be at a minimum of EAL2 of the federally adopted common criteria. This requirement is best accomplished via a secure Virtual Private Network. A dial-up connection generally will not meet these requirements.

NOTE: For all authorized PSP's, the DOJ allows only one initial live scan device to be connected to the DOJ. After 6 months from the date your first device has been put into production, you may submit a request for the connection of an additional device(s) to livescansupport@doj.ca.gov. Approval or denial is determined based on billing history, device error rates and adherence to the Private Service Provider Terms and Conditions.

Private Service Provider

Terms & Conditions

California Department of Justice
Bureau of Criminal Identification and Investigative Services

Applicant Communication Network

Terms and Conditions for Private Service Providers in California

Private Service Providers (PSP) in California, approved by the Department of Justice (DOJ) to establish and maintain a connection to the DOJ Applicant Communication Network (ACN) for purposes of transmitting non-criminal justice requests for Criminal Offender Record Information (CORI) to the DOJ.

1. Definitions

For purposes of this document, terms are defined as follows:

1.01 **Applicant** - Any person who, as a condition of obtaining a license, certificate, permit, or employment, is required to submit his/her fingerprints to the DOJ for a criminal background check.

1.02 **Applicant Information** - Personal and confidential information, regarding an Applicant, including fingerprint images, Social Security Number, California Driver's License, or any other personal identification numbers provided by or collected from an Applicant, which is relevant and necessary to accomplish an electronic fingerprint transaction for transmission to the DOJ.

1.03 **Live Scan** - A computer-based device that allows for the capture of digitized fingerprint images and Applicant data, and the electronic transmission of fingerprint images and data to centralized computers at the DOJ.

1.04 **Network** - The electronic communication system, established by the DOJ pursuant to section 11077.2 of the California Penal Code, to facilitate the transmission of requests for criminal offender record information (CORI) from Private service Providers in California.

1.05 **Operator** - Any person who operates a live scan device and/or provides Applicant fingerprinting services on behalf of a DOJ-approved Provider.

1.06 **Provider** - A private fingerprint service provider in California, approved by the DOJ to establish a connection to the DOJ Applicant Communication Network for purposes of transmitting electronic Applicant transactions for criminal offender record information to the DOJ for employment, licensing, certification, or custodial child placement purposes.

1.07 **Provider Representative** - The person duly authorized to represent the Provider and act on its behalf, with defined authority for implementing and ensuring ongoing compliance with all requirements set forth in these Terms and Conditions. The Provider Representative must be a California resident and is subject to the Certification requirements set forth in section 3.02 of this document. For the purposes of the duties

and responsibilities set forth in this document, the Provider Representative and the Provider shall be considered to be one and the same.

2. Scope

2.01 This document establishes the minimum internal controls deemed necessary by the DOJ to adequately protect the security and stability of the Network, and the privacy rights of individual Applicants. The Provider may impose any additional, more stringent controls it deems necessary and/or appropriate.

2.02 The Terms and Conditions apply to all personnel, equipment, software, systems, networks, communication links, and facilities supporting and/or acting on behalf of the Provider.

2.03 Approval to establish and maintain connectivity to the Network, either directly or indirectly, shall be contingent upon full compliance at all times with all requirements set forth in this document. Failure or refusal to fully comply with all requirements herein may result in the temporary or permanent termination of the Provider's direct connection to the Network, ability to transmit electronic fingerprints to the DOJ through an indirect Network connection, or ability to forward electronic fingerprints to the DOJ on behalf of other DOJ-approved Provider(s).

3. Personnel Security

3.01 The Provider shall be responsible for the actions of any person or entity acting on its behalf and/or providing services in support of it.

3.02 Unless exempted under the provisions of section 11102.1(a) of the California Penal Code, the Provider, and every Operator providing services on a Provider's behalf, shall possess and maintain a valid Fingerprint Roller Certificate issued by the DOJ. The Provider shall not allow any Operator to provide fingerprint services on its behalf unless he/she possesses a valid Fingerprint Roller Certificate. A copy of the Fingerprint Roller Certificate must be displayed in full view of the Applicant, for the Provider(s) and every Operator providing fingerprint services on a Provider's behalf.

3.03 The Provider shall maintain a current list of all Operators providing fingerprint services on its behalf. A copy of the list shall be provided to the DOJ upon request.

4. Site Security

4.01 All hardware and software associated with the capture and/or transmission of Applicant fingerprints to the DOJ shall be adequately secured at all times to reasonably protect against theft, damage, and/or unauthorized access or use by any person.

5. Information Security

5.01 Applicant information is confidential and the use of this information for any purpose other than the purpose for which it was expressly provided by the Applicant is strictly prohibited. Violation of an Applicant's absolute right to privacy may subject the

Provider and/or its Operator(s) to criminal and/or civil liability, and may result in termination of the Provider's connectivity as cited in Section 2.03.

5.02 Except as expressly authorized by the DOJ, Applicant information shall not be replicated, sold, shared, modified, archived, stored, or used to supplement any existing data base, file, record or report, or create any new database, file, record or report.

5.03 A Provider forwarding electronic fingerprint records to the DOJ on behalf of another DOJ- approved Provider is strictly prohibited from stripping or extracting any data from the records it forwards, except as expressly authorized in writing by the DOJ.

5.04 Applicant information, as defined in Section 1.02, shall not be collected or transmitted outside of the State of California.

5.05 Applicant information, as defined in Section 1.02, shall be collected and verified by the Live Scan Operator conducting the transaction.

5.06 The Live Scan Operator shall reasonably verify the identity of each Applicant by comparison to valid (unexpired) photo identification, presented at the time of fingerprinting, to the appearance of the Applicant, and to the information contained on the Request for Live Scan Services form. Fingerprint services shall not be provided to any Applicant who does not present proper and valid photo identification, and whose identity cannot be reasonably verified through this comparison.

5.07 Once a transaction has been transmitted, the Provider is strictly prohibited from using a previously captured fingerprint image for any purpose other than resubmitting a record that was rejected by the DOJ due to faulty data.

5.08 Applicant fingerprint transaction records may be temporarily retained in an electronic storage medium, within the live scan device, pending successful transmission of the record to the DOJ. In no event, however, may any Applicant fingerprint image or record be retained, in either electronic or hard copy form, for longer than 30 calendar days from the date of the initial transmission of the fingerprint record to the DOJ or immediately upon the Provider no longer conducting business; whichever one comes first. Civil Code section 1798.81 states, "A business shall take all reasonable steps to destroy, or arrange for the destruction of a customer's records within its custody or control containing personal information which is no longer to be retained by the business by (1) shredding, (2) erasing, or (3) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means."

5.09 Every person who, in the course of their normal duties, collects, processes, facilitates, or supports the transmission of Applicant fingerprints to the DOJ, or who manages, administers, accesses, develops, or maintains the systems supporting the Agency, shall be required to sign a DOJ Security and Disclosure Certification form, acknowledging that they understand their responsibilities for protecting confidential Applicant information, the restrictions concerning the use of such information, and the penalties for misuse. Signed originals of the Certification forms shall be mailed to the DOJ and a copy must be retained by the Agency and shall be made available to the DOJ upon request.

6. System Security

6.01 A dedicated system shall be utilized for transmitting electronic Applicant fingerprints to the DOJ. The Provider shall not use the system to run any other business application(s), unless expressly authorized by the DOJ in advance.

6.02 The Provider shall obtain DOJ approval prior to establishing any network linkage to another DOJ-approved Provider (Peer to Peer), for the purpose of accomplishing an indirect connection to the Network.

6.03 Any network linkage authorized by the DOJ pursuant to section 6.02, which allows electronic Applicant fingerprints to be transmitted from the Live Scan Provider, and forwarded to the DOJ through another Provider's direct connection to the Network (Peer to Peer relationship) via WAN, LAN, or Internet, shall be secured by a firewall to provide a point of defense, and a controlled and audited access to servers, from both inside and outside of the network.

6.04 The DOJ-approved transmission path, which enables connectivity to the Network, originating from the Live Scan Provider, and transversing through any inter-connected systems, and ultimately terminating at the DOJ, shall not be modified in any way without advance notice to, and express written approval from the DOJ.

6.05 All equipment used for transmitting and/or forwarding electronic Applicant fingerprints to the DOJ shall be segregated and screened against unauthorized use. Data integrity must be maintained in order to detect the unauthorized creation, alteration, or deletion of Applicant data or images.

6.06 All unused user or system accounts shall be removed or disabled.

7. Security Violations

7.01 All security violations or suspected security violations shall be immediately reported to the DOJ. Reports of security violations shall include the date of the incident(s), the parties involved (if known), the nature and scope of the incident and any action(s) taken, including steps to protect against future violations.

7.02 The DOJ reserves the right to investigate all reported or suspected security violations and to take any action it deems appropriate and/or necessary to protect the security and stability of the Network and the privacy rights of individual applicants, including termination of the Provider's connection to the Network as cited in Section 2.03.

8. Quality Control

8.01 Remedial training may be required if, at any time, the DOJ determines that the rate of record rejects due to poor image quality, or data errors, exceeds acceptable levels. Failure to obtain appropriate training and resolve unacceptable fingerprint record reject levels in a timely manner may result in termination of the Provider's connectivity to the Network as cited in Section 2.03.

8.02 The Provider shall only utilize hardware and software that is currently certified and approved by the DOJ for the Applicant software type, the National Institute of Standards and Technology, and the Federal Bureau of Investigation (FBI).

8.03 All equipment associated with the capture and transmission of electronic Applicant fingerprint records shall be maintained in good working condition at all times.

8.04 All manufacturer software upgrades, including the installation of any patches deemed necessary by the manufacturer shall be applied in a timely fashion and remain current.

8.05 All DOJ customization software upgrades and the DOJ validation table updates shall be applied in a timely fashion and remain current.

8.06 All Applicant fingerprint records shall be transmitted to the DOJ within 24-hours from the time the fingerprints were obtained from the Applicant.

8.07 Except as specifically provided herein, a provider shall not transmit or forward an applicant fingerprint transaction to the DOJ more than one time. The Provider shall be responsible for applicable DOJ and FBI processing fees associated with any duplicate transaction it transmits to the DOJ through its direct network connection, including any duplicate transaction that it allows to be forwarded on behalf of another DOJ approved Provider (Peer to Peer relationship).

8.08 Upon the DOJ's request, a DOJ approved Provider forwarding electronic Applicant fingerprints on behalf of another Provider (peer to peer relationship) shall disable a Provider's connection to the Network as cited in Section 2.03.

8.09 The Provider shall maintain a log of all Applicant fingerprint transactions. The log shall clearly identify the name of the Operator who performed each transaction, the name of the Applicant fingerprinted, the date the Applicant was fingerprinted, the type of photo identification presented and the Applicant Tracking Identifier (ATI) number associated with the transaction. The Provider shall maintain the log for a minimum of one year from the date of the oldest transaction, and shall make the log available to the DOJ upon request. Access to the log shall be controlled by the Provider.

8.10 The Provider shall retain a copy of the "Request for Live Scan Service" form associated with each Applicant fingerprint transaction for a period of 12 months, for purposes of security and review. The copies shall be stored in a locked storage medium to reasonable protect against theft, damage, or access by any unauthorized person. The copies shall be destroyed by cross-cut shredding after the 12-month retention period has elapsed or immediately upon the Provider no longer conducting business; whichever one comes first. Civil Code section 1798.81 states, "A business shall take all reasonable steps to destroy, or arrange for the destruction of a customer's records within its custody or control containing personal information which is no longer to be retained by the business by (1) shredding, (2) erasing, or (3) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means."

9. Fees

9.01 The Provider shall establish a billing account with the DOJ for purposes of collecting and remitting the DOJ and FBI processing fees.

9.02 The DOJ and FBI processing fees that are not billable to the requesting entity shall be collected by the Provider at the time fingerprint services are rendered to the Applicant. All processing fees shall be remitted to the DOJ in a timely manner by the Provider. Failure to remit payment in a timely manner may result in termination of the Provider's Network connection as cited in Section 2.03.

9.03 The Provider may charge the Applicant a separate fingerprint rolling fee as compensation for its services. The amount of the fee and accepted method of payment shall be determined by the Provider.

9.04 Any Applicant who returns to the Provider to be reprinted because his/her initial fingerprint submission was rejected due to poor fingerprint image quality, shall not be charged an additional rolling fee by the Provider. The Applicant may, however, be charged a rolling fee if the original fingerprint transaction was performed by a different service Provider.

10. Audits

10.01 The Provider shall be subject to periodic, unannounced, on-site visits by the DOJ to audit for compliance with the provisions of the Terms and Conditions, and any applicable laws, regulations, policies, practices, or other requirements deemed necessary by the DOJ. The audits shall be reasonable in both scope and length, and shall occur during the Provider's normal business hours. Audits will be conducted in a manner that is least disruptive to the Provider's business operations.

10.02 Failure to cooperate, and/or refusal to provide documents, logs, lists, files, records or any other information requested by the DOJ, may result in the temporary or permanent termination of the Provider's connection to the Network as cited in Section 2.03.

11. Miscellaneous Provisions

11.01 These Terms and Conditions do not confer, grant, or authorize any rights or privileges to any entity or person other than the Provider and the Provider's authorized representative.

11.02 All reports, notices, requests, and/or correspondence shall be forwarded by First Class Mail to:

California Department of Justice
Bureau of Criminal Identification and Investigative Services
Client Services Program
P.O. Box 903417
Sacramento, CA 94203-4170

California Department of Justice
Applicant Communication Network

Agreement to Terms and Conditions for Private Service Providers in California

Provider (Business Name): _____

Provider Representative (Owner): _____

Physical Address: _____

Mailing Address (If Different): _____

Telephone Number: _____ Facsimile Number: _____

Email Address: _____

The Provider's connection to the Department of Justice (DOJ) Applicant Communication Network is contingent upon implementation of, and adherence at all times, to all requirements set forth in the Terms and Conditions, including any changes thereto.

The DOJ reserves the right to amend or modify the Terms and Conditions, and/or impose additional requirements and/or restrictions, at any time it deems necessary to protect the stability and security of the Network.

The DOJ reserves the right to terminate the Provider's connection to the Network at any time, without prior notice, if it has reason to believe that the security or stability of the Network has been, or will be, compromised in any way.

This Agreement is not effective unless, and until approved by the DOJ, and signed by both parties.

In signing this Agreement, I certify that I have read and understand the foregoing Terms and Conditions for establishing and maintaining a connection to the DOJ Applicant Communication Network, and agree to and accept responsibility for compliance with all requirements therein.

_____ _____
Provider Representative (Printed Name) Title

_____ _____
Signature of Provider Representative Date

Approved:

_____ _____
DOJ Representative (Printed Name) Title

_____ _____
Signature of DOJ Representative Date

Live Scan Service Providers
Security and Disclosure Certification

Individuals providing live scan fingerprinting services collect and have access to personal Applicant information, including fingerprint images, which are considered to be confidential under California law. The California Department of Justice (DOJ) is committed to protecting the privacy rights of individuals and protecting personal information from unauthorized access, use, or disclosure.
As an individual providing live scan fingerprinting services on behalf of _____ (***Business Name***), you are responsible for understanding and complying with the following duties and responsibilities related to the protection, use and handling of confidential information.

1) You may request and collect only that information which is necessary to perform an applicant live scan transaction.

2) You may not deliberately enter false or incomplete data or images, or omit or modify existing valid data in an attempt to affect the outcome of an Applicant's criminal history background check.

3) You are strictly prohibited from using any personal Applicant information for any purpose other than the purpose for which the information was expressly provided by the Applicant. You may not share, replicate, compile, remove, delete, alter, or disclose information collected from or regarding Applicants.

4) You may not remove materials from the area approved for the placement and use of a live scan device and accompanying secured storage areas without specific authorization from the DOJ. The only exception to this is during the use of a portable live scan device, when materials are transported to and from the site where the live scan device is used.

5) You must take reasonable precautions to protect Applicant information from unauthorized access. These reasonable precautions include, but are not limited to: ensuring that any live scan device is inaccessible when unattended; ensuring that unauthorized persons are not allowed to view the screen of a live scan device; storing materials containing confidential information in a secure place; and immediately reporting unauthorized or suspicious individuals or activities to the Live Scan Provider or to the DOJ.

I have read and understand the duties, responsibilities, and restrictions stated above, and have received a copy. I understand that failure to comply with these policies may result in administrative action up to and including criminal and/or civil prosecution in accordance with applicable statutes.

_____	_____
Printed Name of Owner or Employee	Title
_____	_____
Signature of Owner or Employee	Date

BCII LS SD 01(4-2004)

BILLING ACCOUNT APPLICATION
PRIVATE SERVICE PROVIDER

Print Form Reset Form

Type of Application:

- ☐ New
- ☐ Updated
- ☐ Owner/Business Name Change

Business Type:

- ☐ Sole Proprietorship (complete sections A, B, and E)
- ☐ Partnership (complete sections A, C, and E)
- ☐ Corporation (complete sections A, D, and E)

ALL INFORMATION MUST BE COMPLETED LEGIBLY.
COMPLETE EACH REQUIRED SECTION IN ITS ENTIRETY.
INCOMPLETE APPLICATIONS WILL BE RETURNED.

SECTION A - Business Information (All Business Types)

Business Name: _____

Billing Address: _____

City: _____ State: _____ ZIP Code: _____

Authorized Representative: _____

Telephone Number: _____ Facsimile Number: _____

Electronic Mail Address: _____

Existing LSID Number(s) (if applicable): _____

SECTION B - Sole Proprietorship

Owner's Name: _____

Telephone Number: _____ Social Security Number: _____

Federal Tax Identification Number (if applicable): _____

SECTION C - Partnership

Federal Tax Identification Number: _____

COMPLETE THE FOLLOWING FOR EACH BUSINESS PARTNER. ATTACH ANOTHER SHEET FOR ADDITIONAL NAMES.

Name: _____ Title: _____

Telephone Number: _____ Social Security Number: _____

Name: _____ Title: _____

Telephone Number: _____ Social Security Number: _____

BILLING ACCOUNT APPLICATION
PRIVATE SERVICE PROVIDER

SECTION D - Corporation

Federal Tax Identification Number: _____

COMPLETE THE FOLLOWING FOR EACH CORPORATE OFFICER. ATTACH ANOTHER SHEET FOR ADDITIONAL NAMES.

Name: _____ Title: _____

Telephone Number: _____

Name: _____ Title: _____

Telephone Number: _____

Name: _____ Title: _____

Telephone Number: _____

Name: _____ Title: _____

Telephone Number: _____

Corporate Name: _____ Telephone Number: _____

Address: _____ City: _____ State: _____ Zip Code: _____

SECTION E - Acknowledgment (All Business Types)

I, the undersigned, have the authority to conduct business for the business listed above. I confirm that all the information on this application is true and correct. I give my permission to the Department of Justice (DOJ) to research and confirm all information provided and to request a credit report at any time. I understand this is an agreement to collect and remit for DOJ the processing fees associated with the electronic transmission of state and/or federal criminal offender record information requests, including fees incurred by duplicate transmissions or other errors on the part of the above business or its representative(s). I agree to the terms of this agreement and understand it will remain in effect until written cancellation is provided by either party with 30 days notice. Failure to remit payment in a timely manner may result in the DOJ utilizing all information provided on this billing account application for collection purposes and disconnection of live scan service.

Name: _____ Title: _____

Signature: _____ Date: _____

DOJ Use Only

Received Date: _____ ORI #: _____ Input Date: _____

Account #: _____ ACN #: _____ Input By: _____

California Department of Justice

Certified
Peer Service Providers
& Live Scan Vendors

California Certified
Peer Providers

3M COGENT, INC.
Contact: Corey Kennedy or Mitch Lattimer
Phone: (626) 325-9740
E-mail: capspsales@cogentsystems.com

BIOMETRICS4ALL, INC.
Contact: Piet Lesage or Edward Chen
Phone: (714) 568-9888 Ext. 110 or 168
E-mail: sales@biometrics4all.com

G2 SOLUTIONS, INC.
Contact: Mark Morrison
Phone: (866) 202-2342
Fax: (866) 350-4860
E-mail: g2info@g2sinc.com

LIVE SCAN CALIFORNIA
Contact: Darrin Scheidle or Lisa
Phone: (888) 793-1112, Option 2
E-mail: darrin-psp@livescanca.net

California Certified
Live Scan Vendors

3M COGENT, INC.
www.cogentsystems.com
Phone: (626) 325-9740
Fax: (626) 325-9740
E-mail: capspsales@cogentsystems.com

BIOMETRICS4ALL, INC.
www.biometrics4all.com
Phone: (714) 568-9888 Ext. 175
E-mail: sales@biometrics4all.com

CROSSMATCH
www.crossmatch.com
General Information, Sales and Supplies
Phone: (562) 622-1650
Technical Support
Phone: (866) 276-7761

MORPHO TRAK *(Formerly Printrak)*
www.morpho.com
Phone: (800) 734-6241
Email:cscenter@morpho.com

MORPHO TRUST USA (IDENTIX, INC.)
www.L1id.com
Phone: (206) 283-3009
Fax: (206) 283-0671
E-mail: genos@L1id.com

CERTIFIX LIVE SCAN
www.certifixlivescan.com
Phone: (800) 710-1934 Ext. 4
E-Mail: sales@certifixlivescan.com

DATAWORKS PLUS
www.dataworksplus.com
Phone: (925) 240-9010 or (864) 672-2789
Fax: (864) 672-2787
E-mail: sales@dataworksplus.com
Western Sales Contact:
Todd Pastorini (925) 240-9010
tpastorini@dataworksplus.com

COMPUTER DEDUCTIONS INC.
www.cdi-hq.com
Phone: (916) 987-3600
Fax: (916) 987-3606
E-Mail: clew@cdi-hq.com

In Summary:

The following documents must be submitted to the DOJ in a single complete packet, in order for your application to be processed for **Pre-Approval**:

- ☐ Copy of Fingerprint Roller Certificate and accompanying DOJ letter for the Owner or each member of a Partnership or Corporation and for all employees operating your live scan device on behalf of your business;
- ☐ Original signed Agreement to Terms and Conditions;
- ☐ Original signed Security and Disclosure Certification form (Appendix A) for the Owner or each member of a Partnership or Corporation and for all employees operating your live scan device on behalf of your business;
- ☐ Copy of your Business License;
- ☐ Original signed Billing Account Application.

PLEASE NOTE: If you are applying as a Partnership or Corporation, each member must sign the Agreement to Terms and Conditions and provide copies of their Fingerprint Roller Certificate and accompanying DOJ letter.

Please be advised, the pre-approval process can take up to 60 days from the receipt of a complete and accurate application. Once you have received a pre-approval letter from the DOJ, Please submit the following items and allow an additional 60 days for processing:

- ☐ Copy of the Bill of Sale, Proof of Purchase or Lease Agreement for the live scan equipment (provided by the Vendor/Peer Provider);
- ☐ Live Scan Connection Diagram (provided by the Vendor/Peer Provider).

Mail all required documents to:

California Department of Justice
Bureau of California Identification and Investigative Services
Client Services Program
P.O. Box 903417
Sacramento, CA 94203-4170

For assistance and questions regarding live scan or the Private Service Provider Application, please contact livescansupport@doj.ca.gov.