DIRECTORY OF IDENTITY MANAGEMENT AND PROOFING PRODUCTS

The Directory of Identity Management and Proofing Products (“The Directory”) is designed to provide industry with information on solutions that provide a service which confirms the authenticity of the government photo identification and matches the result to the image or video of a person.

The Directory is based on service providers who have completed a self-attestation of survey questions designed to gauge the extent to which their solutions are aligned with DIACC’s Digital Identity Ecosystem Principles.

Background and why is this important.

In June 2019, Canada’s regulatory environment moved to accepting innovative technologies to allow for reporting entities to use identification document capture and comparison tools to meet the requirements of anti-money laundering efforts. Reporting entities include Banks, Insurers, Securities, Realtors, Accountants, Notaries, Dealers in precious metals and money services businesses that are required to identify persons in a business relationship (plus other requirements). Additional tools to perform identification in a digital channel remain available using the credit bureau information and dual records from other reliable sources (e.g., Utility providers or regulated financial services).

Stakeholders and Benefits.

For service providers, this Directory provides awareness of the new Canadian marketplace expectations and new customers. The addition of these markets to start using applications to assess identification documents and verify identity is expected to expand the demand for digital identity solutions in Canada.

For consumers, more choice in how they provide identification. This empowerment of a new wave of sophisticated tools currently in use around the world may empower Canadian commerce to reduce customer friction and provide a secure tool for a person to both provide and access their own information and property.

For reporting entities; a centralized list of service providers and the start of an assessment process. To adopt these tools, reporting entities (for example banks, insurers, and security dealers) will be required to perform a risk assessment and document this exercise prior to use of the technology in their anti-money laundering programs. This survey will include many of the common questions used in the assessment of digital identification tools from an anti-money laundering perspective.

The Directory will be hosted by the DIACC and available free of charge to meet the objectives listed above. The Directory will also be provided to regulatory bodies to raise awareness of innovations in the marketplace available for regulated reporting entities to use. Membership in the DIACC is strongly encouraged for service providers and those interested in supporting the digital identity community in Canada.

DISCLAIMER

The information contained in the Directory is for general information purposes only. While DIACC endeavours to keep the information up to date and correct, DIACC makes no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, certification or compliance status, suitability or availability with respect to the Directory or the information, products, services, or related graphics contained on the Directory for any purpose. Any reliance you place on such information is therefore strictly at your own risk.

In no event will DIACC, and its members, be liable for any loss or damage including without limitation, indirect or consequential loss or damage, or any loss or damage whatsoever arising from loss of data or profits arising out of, or in connection with, the use of the Directory.

A. ABOUT THE SERVICE PROVIDER

A1. Please provide a brief description about your company: (250 words) *

Applied Recognition is a software company that is leveraging facial biometrics technology to enable digital transactions and secure access. As a pioneer in the facial biometrics industry, we have industry recognized solutions for identity verification and authentication. Our customers embed our technology into their existing workflow solutions to enable digital and security transformations in their organizations.

Our enterprise solutions include:
Ver ID Identity
Identity proofing that is the critical gateway enabling remote enrollment by combining identity document verification with biometric face recognition digitally.

Ver ID Authentication
Face factor authentication that augments security compliance and minimizes cyber and security risk by replacing and/or augmenting password requirements with facial biometric recognition to validate the intended user as a requirement to access computers, networks, applications and physical locations.

Applied Recognition has created a multi-purpose enterprise software that is an on-premises solution for organizations that want to enhance and secure their digital strategies, enable customer access to services and dramatically decrease their cyber risk vulnerabilities. Our software easily integrates with a variety of business applications. We offer software development kits for Windows, macOS, Android and iOS platforms, as well as server and API services. We are committed to providing biometric solutions that help protect people, their credentials, and their transactions.

A2. Please provide a brief description about your ID Capture technology: (250 words) *

We offer two options of deployment that can support ID verification workflows;
1) Mobile SDKs for Android and iOS
2) Server API for processing ID document images and selfies
Both offer support for a wide variety of ID documents.

Features of the above products include:
1) Mobile SDKs
• Designed to be integrated with an existing app to add ID verification and/or face authentication capabilities. Completely flexible implementation.
• Native interfaces for Java/Android and Swift/iOS; plus, Cordova, React Native and Flutter plug-ins
• All data encrypted and stored locally by default; optionally you can export data from the SDK to push to back-end servers.
• Supports real-time selfie capture and patented liveness detection
• Support document validation for fraud detection. See below under the Server API for the various tests performed.
• Hardened SDK to eliminate risk of hacking on a rooted phone.

For passports:
• Reading of the passport chip (ICAO standard) on NFC capable phones. Provides a higher level of ID validation for passports.

2) Server API
• Supports mobile camera capture of driver's license or passport documents. If the user begins session on the desktop; methods are provided to migrate the user to the mobile browser via QR code scanning.
• We provide sample JavaScript code and libraries for integrating the client portion into an existing web app.
• Employs advanced machine learning to do the following with each image for Driver's Licenses;
• Identify the jurisdiction for the document
• Perform an OCR scan of the document front
• Scan the PDF417 barcode on the back of a driver's license
• Compare the OCR text with the barcode content on an object by object basis
• Analyze the entire front image for brightness, contrast and focus
• Scan the front of the document for a face with suitable recognition quality
• Analyze the region around the face to assign an authenticity score – taking into account the copy protection techniques employed by the majority of US States and Canadian provinces
• Provide an overall Pass, Review, or Fail classification for the document
• Return all extracted data via the API call to the host application

For passports
• Identify the jurisdiction for the document
• Perform an OCR scan of the document main page including MRZ

A3. Please provide a brief description about complementary products or services: (250 words)

Our core Face Authentication and Liveness technology can be integrated into different solutions and workflows to validate identity and secure access.

The same face template used for identity validation can be used across the enterprise for secure access. It can be used in the various use cases to secure high value transactions or locations.

This capability can be integrated into kiosks to provide physical access solutions like Time & Attendance, Employee Access, Guest Access, etc. and digital solutions for access to desktops/laptops, network access, and different areas of the enterprise applications.

A4. What other solutions does your organization offer to help with identity verification and authentication?Note: what is the list of complimentary products and services.

- [ ] 3rd Party Data Source Validation (sanctions/AML political and corrupt person scanning)
- [x] Biometrics Authentication Methods (voice, pattern, behaviour, etc.)
- [x] Credential Based Authentication
- [ ] Credit Bureau Validation
- [ ] Credential Management (Issuance and Receipt)
- [x] Country Signer Certificate Authentication
- [ ] Device Fingerprinting (e.g., device attributes to assess a digital identity)
- [x] Digital signing of records
- [x] Digital Wallets
- [ ] Email Risk Assessment – association of name and address with email
- [x] Face ID in lieu of Credentials
- [x] Identity Access Management Integrations
- [ ] Knowledge based authentication/question-based authentication
- [ ] One-Time Password/Push Notification
- [ ] Telecom Validation (Enstream in Canada, Telesign in the US)
- [ ] Other

Additional Comments

A5. Please list any other service providers which include your technology which are available in Canada (indirectly able to use your service).

This information is currently not publicly available, but can be provided under NDA.

A6. Please provide your contact information for inquiries related to this survey including websites, emails, social media or other methods. *

Pankaj Gogia, pankaj.gogia@appliedrecognition.com

A7. Please provide a link to any blog posts which may be available about your company (please include DIACC Spotlights or blog posts as well).

N/A

B. ROBUST, SECURE, SCALEABLE

Digital identity solutions must be robust enough to ensure it is secure, available, and accessible at all times. Full time services access also requires redundancy and disaster recovery tools.

B1. Is the organization a member of the DIACC? *

- ○ Not a member
- ○ Considering Membership
- ○ Board Level
- ◉ Sustaining
- ○ Adopting

B2. Is your model self-attested to be compliant with the Pan-Canadian Trust Framework™ (PCTF)? To learn more about the PCTF, please contact info@diacc.ca *

- (●) Yes
- ( ) In progress
- ( ) Undecided
- ( ) Not planning on it

B3. Does the organization participate in IdentityNORTH Conferences?

- (●) Yes
- ( ) No

B4. Where are do you operate Internationally? (check all that apply) *

- [x] Canada
- [x] US
- [x] Mexico, Central America, and Caribbean
- [x] Europe
- [x] Asia
- [ ] Africa
- [ ] Oceania
- [x] South America

Additional comments

C. IMPLEMENT, PROTECT, AND ENCHANCE PRIVACY BY DESIGN

C1. Does your product currently in production comply with Privacy laws in the following? *

- [x] Canada
- [x] Quebec
- [x] Brazilian General Data Protection Law (LGPD)
- [x] California Privacy Legislation (CCPA)
- [x] EU (GDPR)
- [x] UK
- [x] Australia (APPs)

Additional comments

D. INCLUSIVE, OPEN, AND MEETS BROAD STAKEHOLDER NEEDS

D1. Which languages does your application support? (check all that apply) *

- [x] English
- [x] Canadian French
- [x] Other

D2. Which languages do you provide technical support in? (check all that apply) *

- [x] English
- [ ] Canadian French
- [ ] Other

D3. Does your application design address web content accessibility guidelines and is certified to: *

- [ ] WCAG (Web Content Accessibility Guidelines)
- [ ] WCAG 2.0 (ISO/IEC40500)
- [ ] WCAG 2.1
- [ ] Been tested to Ontario's AODA compliance
- [ ] Not Yet
- [x] Other

Additional comments

In process of testing against various guidelines

E. PROVIDES CANADIANS CHOICE, CONTROL, AND CONVENIENCE

E1. In addition to Canadian passports and driver's licenses issued by provinces, territories and the Canadian department of defence, does your application currently support. (Note: Canadian citizenship card not added to the list as there are limited security features (e.g., no barcode and not reissued since 2012). The laminated (certificate Indian Status card) does not have a barcode or security features and accordingly, is not recommended for this process). *

- [x] Ontario Health card (only to be used for health purposes)
- [ ] Quebec Health card
- [x] Provincial Photo ID cards (Alberta, Manitoba, New Brunswick, Newfoundland, Labrador, Nova Scotia, Ontario, Prince Edward Island, British Columbia, and Saskatchewan)
- [ ] Canada/US Nexus (Trusted Traveller)
- [x] Canadian Permanent Resident card
- [ ] Secure Indian Status card
- [ ] In Process

E2. Globally, how many countries or regions can your service assess Passports (for example: 150)

186

E3. Globally, how many countries or regions can your service assess National ID cards (for example: 100)

120

E4. Globally, how many total identification records* can your service assess? (Example: *includes above and other records, 1000)

526

E5. Globally, how many countries or regions can your service assess Driver's Licenses (for example, 500) Note: if a jurisdiction has 3 versions of the same Driver's License, please only count it as 1 jurisdiction for this question

151

Additional comments

F. BUILT ON OPEN STANDARDS-BASED PROTOCOL

Digital identity solutions must be robust enough to ensure it is secure, available, and accessible at all times. Full time services access also requires redundancy and disaster recovery tools.

F1. On which platforms are your solutions available? (check all that apply) *

- [x] Apple App store
- [x] Google app store
- [x] Windows/Microsoft application
- [x] Embedded within client's application
- [x] In-person scanner - hardware
- [ ] Not at this time
- [ ] Other

F2. Please list all Accreditations, Certifications, and Standards that your organization complies with (check all that apply) *

- [ ] FIDO® Certified
- [ ] HIPAA - Self-attestation to meet the requirements of Health Insurance Portability and Accountability Act (USA)
- [ ] ISO/IEC 27001 - an international standard for information security management
- [ ] ISO/IEC 27018:2019 - Code of practice for protection of personally identifiable information (PII) in public clouds
- [ ] ISO 30107-3 - Biometric Presentation Attack Detection
- [x] NIST 800-63 series - Self-attestation to meet the requirements of NIST Digital Identity guidelines
- [ ] SOC 2 Type 1 (at point of time) - Service Organization Control
- [ ] SOC 2 Type 2 (over a 6-month period) - Service Organization Control
- [ ] Not at this time
- [ ] Other

F3. Does the solution utilize open standard protocols such as: *

- [ ] OAUTH2
- [ ] OPENID CONNECT 1.0
- [ ] SAML
- [x] Not at this time

Additional comments

G. INTEROPERABLE WITH INTERNATIONAL STANDARDS

G1. Confirm if you have an imaging standard for photos and facial capture (check all that apply) *

- [x] Passport Image Standard (ISO IEC19794-5)
- [x] PNG
- [x] JPEG
- [ ] GIF
- [ ] TIFF
- [ ] Proprietary standards
- [ ] Other, please describe

Additional Comments

H. COST EFFECTIVE AND OPEN TO COMPETITIVE MARKET FORCES

H1. What is the cost-model? (check all that apply) *

- [x] Flat fee for time period
- [x] Pay per use model
- [x] Mixed model of flat fee and usage
- [ ] Other

Additional comments

H2. What size of organizations have adopted your vendor's solution(s)? (check all that apply) *

- [ ] Government and public sector
- [x] Large organizations (Over 500 employees)
- [x] Small organizations (Under 500 employees)
- [ ] Consumer direct
- [ ] Other

Additional Comments

I. ABLE TO BE INDEPENDENTLY ASSESSED, AUDITED, AND SUBJECT TO ENFORCEMENT

I1. How does the application capture the image of a live person? (check all that apply) *

- [x] Via computer webcam picture
- [ ] Via computer webcam video
- [x] Via computer webcam interactive video
- [x] Via mobile device picture
- [ ] Via mobile device video
- [x] Via mobile device interactive video
- [ ] Other

I2. Does the application perform a liveness detection or genuine presence test and how? (check all that apply) *

- [x] Yes, actions to be performed by person (active liveness check)
- [ ] Yes, live video capture and/or motion detection (passive liveness check)
- [ ] Yes, session can be reviewed by a live human checker
- [ ] Not at this time
- [ ] Other

I3. Does the application read the machine-readable portion of the photo identification documents as applicable? *

- (●) Yes, recorded and used for validation (the information read from the machine-readable portion is compared to the text on the identity document)
- ( ) Yes, recorded only without validation
- ( ) No

I4. Does the application read the facial biometric (ICAO 9303) NFC chip of machine-readable passports? (check all that apply) *

- [x] Android ready now
- [ ] Android within next 3 months
- [ ] Apple ready now
- [x] Apple ready within 3 months
- [ ] Not at this time
- [ ] Other

I5. Does the application verify that the chipped ID document has been authenticated? (e.g., Country signer, Active Authentication, etc.)? *

- ○ Yes
- ◉ No

I6. Does the application connect with any government sources to confirm the legitimacy of the record? *

- ○ Yes
- ◉ No

I7. Does the application check to confirm the expiry date of the document is not prior to the date of the validation? (As applicable; a requirement from Canadian Anti-Money Laundering regulations) *

- ◉ Yes
- ○ No

I8. Does the application test the algorithm (if applicable) for the unique identifiers against the ones used by the identification document provider? *

- ◉ Yes, when applicable (e.g., Ontario Driver's License has the first letter of the identification number matching the first letter of the surname)
- ○ No

I9. Is the application able to parse the following data fields needed for relying parties to use the process for Anti-Money Laundering requirements in Canada? (Note: The fields for AML requirements in Canada as follows: name, address (if on document), date of birth, reference number of identification document, expiry date, date and time of identification validation, type of identification, jurisdiction of identification document, and country of identification document). *

- (●) Yes
- ( ) No

I10. What physical identification security features does your solution test against a database of expected results? (check all that apply) *

- [x] Character spacing
- [x] Document size
- [ ] Document modifications (e.g., cut corner)
- [x] Document shape
- [x] Font position
- [x] Font size
- [x] Font type
- [x] Holograms
- [x] Image frequency
- [x] Image positioning
- [x] Image size
- [x] Markers (logos, symbols or watermarks) positioning
- [x] Markers (logos, symbols or watermarks) size
- [ ] Position and size of magnetic stripe
- [ ] Raised lettering
- [ ] Ultraviolet images
- [ ] Other

Additional Comments

J. MINIMIZES DATA TRANSFER BETWEEN AUTHORITATIVE SOURCES AND WILL NOT CREATE NEW IDENTITY DATABASES

J1. Where is the identification information ultimately stored? (check all that apply) *

- [x] By the person being identified (e.g., stored digital identity on their device)
- [ ] By the vendor on behalf of the subject (e.g., Identity network stores the encrypted access of the digital identity for the person being identified)
- [ ] By the vendor as directed by the entity receiving the identification information (e.g., financial institution)
- [x] By the entity receiving the identification information (e.g., financial institution)
- [ ] Any of the above
- [ ] Other

J2. Does the information stay within Canada for the entire session for Canadian issued identification (e.g., in transit not related to storage)? *

- (●) Yes
- ( ) No

J3. Does the ID network encrypt all information in the mobile application in transit? *

- (●) Yes
- ( ) No

J4. What option do they have for the storage information? (check all that apply) *

- [x] Major cloud providers with Canadian server locations
- [x] Major cloud providers with International server locations
- [x] Private clouds
- [ ] Other

J5. What option do they have for the delivery of service? (check all that apply) *

- [x] Major cloud providers (SaaS) with Canadian server locations
- [x] Major cloud providers with International server locations
- [x] Private clouds
- [x] On premise with customer's data center
- [x] Mobile Integrations (Customer within their own app via SDK)
- [x] Mobile Integrations (Vendor application)
- [x] Web Integrations (Customer within their own app via SDK)
- [x] Web Integrations (Vendor application)
- [ ] Other

Additional comments