AWARE INC /MA/
Form 10-K
February 12, 2016

UNITED STATES

SECURITIES AND EXCHANGE COMMISSION

Washington, D.C. 20549

FORM 10-K

Annual Report Pursuant to Section 13 or 15(d) of The

Securities Exchange Act of 1934

For the fiscal year ended December 31, 2015

Commission file number 000-21129

AWARE, INC.
(Exact Name of Registrant as Specified in Its Charter)

Massachusetts	**04-2911026**
(State or Other Jurisdiction of Incorporation or Organization)	(I.R.S. Employer Identification No.)

40 Middlesex Turnpike, Bedford, Massachusetts 01730
(Address of Principal Executive Offices)

(Zip Code)

(781) 276-4000
(Registrant's Telephone Number, Including Area Code)

Securities registered pursuant to Section 12(b) of the Act:

Title of Each Class	**Name of Each Exchange on Which Registered**
Common Stock, par value $.01 per share	**The Nasdaq Global Market**

Securities registered pursuant to Section 12(g) of the Act: **None**

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act. Yes ¨ No x

Indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or Section 15(d) of the Exchange Act.

Yes ¨ No x

Indicate by check mark whether the registrant (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. Yes x No ¨

Indicate by check mark whether the registrant has submitted electronically and posted on its corporate Web site, if any, every Interactive Data File required to be submitted and posted pursuant to Rule 405 of Regulation S-T (§ 232.405 of this chapter) during the preceding 12 months (or for such shorter period that the registrant was required to submit and post such files). Yes x No ¨

Indicate by check mark if disclosure of delinquent filers pursuant to Item 405 of Regulation S-K is not contained herein, and will not be contained, to the best of registrant's knowledge, in definitive proxy or information statements incorporated by reference in Part III of this Form 10-K or any amendment to this Form 10-K. x

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, or a smaller reporting company. See the definitions of "large accelerated filer", "accelerated filer", and "smaller reporting company" in Rule 12b-2 of the Exchange Act. (Check one):

Large Accelerated Filer ¨ Accelerated Filer x Non-Accelerated Filer ¨ Smaller Reporting Company ¨

Indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act). Yes ¨ No x

As of June 30, 2015 the aggregate market value of the registrant's common stock held by non-affiliates of the registrant, based on the closing sale price as reported on the Nasdaq Global Market, was approximately $58,926,193.

The number of shares outstanding of the registrant's common stock as of February 5, 2016 was 22,993,139.

DOCUMENTS INCORPORATED BY REFERENCE

Portions of the registrant's definitive Proxy Statement to be delivered to shareholders in connection with the registrant's Annual Meeting of Shareholders to be held on May 25, 2016 are incorporated by reference into Part III of this Annual Report on Form 10-K.

AWARE, INC.

FORM 10-K

FOR THE YEAR ENDED DECEMBER 31, 2015

TABLE OF CONTENTS

PART I

PART II

PART III

PART IV

PART I

FORWARD LOOKING STATEMENTS

Matters discussed in this Annual Report on Form 10-K relating to future events or our future performance, including any discussion, express or implied, of our anticipated growth, operating results, future earnings per share, market opportunity, plans and objectives, are "forward-looking statements" within the meaning of Section 27A of the Securities Act of 1933, as amended, and Section 21E of the Securities Exchange Act of 1934, as amended. These statements are often identified by the words "may," "will," "expect," "believe," "anticipate," "intend," "could," "estimate," or "continue," and expressions or variations. Such forward-looking statements are subject to risks, uncertainties and other factors that could cause actual results and the timing of certain events to differ materially from future results expressed or implied by such forward-looking statements. Factors that could cause or contribute to such differences include, but are not limited to, those discussed in the section titled "Risk Factors," set forth in Item 1A of this Annual Report on Form 10-K and elsewhere in this Report. The forward-looking statements in this Annual Report on Form 10-K represent our views as of the date of this Annual Report on Form 10-K. We anticipate that subsequent events and developments will cause our views to change. However, while we may elect to update these forward-looking statements at some point in the future, we have no current intention of doing so except to the extent required by applicable law. You should, therefore, not rely on these forward-looking statements as representing our views as of any date subsequent to the date of this Annual Report on Form 10-K.

ITEM 1. BUSINESS

Company Overview

Aware, Inc. ("Aware", "we", "us", "our", or the "Company") is a leading provider of software and services to the biometrics industry. We have been engaged in this business since 1993. Our software products are used in government and commercial biometrics systems to identify or authenticate people. Principal government applications of biometrics systems include border control, visitor screening, law enforcement, national defense, intelligence, secure credentialing, access control, and background checks. Principal commercial applications include: i) user authentication for login to mobile devices, computers, networks, and software programs; ii) user authentication for financial transactions and purchases (online and in-person); iii) physical access control to buildings, and iv) screening and background checks of prospective employees and customers.

Our products provide interoperable, standards-compliant, field-proven biometric functionality and are used to capture, verify, format, compress and decompress biometric images as well as aggregate, analyze, process, match and transport those images within biometric systems. We sell a broad range of software products for fingerprint, facial, and iris modalities. We also offer a variety of software engineering services, including: i) project planning and management; ii) system design; iii) software design, development, customization, configuration, and testing; and iv) software integration and installation. We sell our biometrics software products and services globally through systems integrators and OEMs, and directly to end user customers.

Aware was incorporated in Massachusetts in 1986. We are headquartered at 40 Middlesex Turnpike in Bedford, Massachusetts, and our telephone number at this address is (781) 276-4000. Our website address is *www.aware.com*. The information on our website is not part of this Form 10-K, unless expressly noted. Our stock is traded on the Nasdaq Global Market under the symbol AWRE.

Industry Background

Biometrics is the measurement of unique, individual physiological characteristics, such as fingerprints, faces, irises, and voices that can be used to determine or verify an individual’s identity. The biometrics industry offers technology that digitally captures and encodes biometric characteristics and then compares those characteristics against previously encoded biometric data to determine or verify an individual’s identity. Biometrics addresses the limitations inherent in traditional identification and authentication processes, such as paper credentials, passwords, PIN codes, and magnetic access cards.

The biometrics industry provides solutions for a broad range of government and commercial applications. Principal government biometrics applications include border control, visitor screening, law enforcement, national defense, intelligence, secure credentialing, access control and background checks. Principal commercial applications include: i) user authentication for login to mobile devices, computers, networks, and software programs; ii) user authentication for financial transactions and purchases (online and in-person); iii) physical access control to buildings; and iv) screening and background checks of prospective employees and customers.

We believe that government and commercial entities will continue to adopt and expand the use of biometrics-enabled solutions to address the limitations and vulnerabilities of traditional identification and authentication processes. We believe the following factors, among others, will contribute to the growth of biometrics solutions: i) government-mandated implementation of identification for employees, citizens, and foreign nationals to enhance national security; ii) military implementations for the identification of terrorists and other hostile persons; iii) increasing threats to personal security encountered in areas such as transportation; iv) government and commercial efforts to detect and reduce fraud and cybercrime; v) adoption of biometrics on mobile devices; and vi) the emergence and adoption of international biometrics standards.

The biometrics industry may be segmented into government and commercial sub-markets. While these markets are similar in many respects and share similar characteristics and technology, certain aspects of the markets are different. We believe that this market-based distinction is important to an understanding of Aware's business as the vast majority of our revenue is currently derived from government customers.

Government market

Governments throughout the world were early adopters of biometrics technology and continue to be the largest consumers of the technology. Biometrics technology is used by local, state, and national governments.

At the local and state level, biometrics technology is used in the following applications:

- Law enforcement applications that enable officers in the field to correctly identify potential suspects more reliably and efficiently by submitting biometrics samples to state or federal biometric search services;
- Background checks for employment screening;
- Drivers' licenses and identification cards; and
- Benefits issuance.

At the national level, biometrics technology is used in the following applications:

- Border control

National governments throughout the world have mandated increased spending on security measures, implemented new regulations and placed greater emphasis on technology to address growing security concerns. Immigration and border control agencies have taken steps to improve security in response to heightened concerns over public safety from the threat of terrorism. They use biometrics to help establish the identity of visitors upon application for a visa or upon arrival at border checkpoints. For example, the U.S. Office of Biometric Identity Management currently requires foreign visitors entering the United States to have their ten fingers scanned and a facial photograph taken to determine if they are present on a watch list. The European Union now mandates that e-passports include fingerprint data in addition to a digital photograph.

- Defense

Within military organizations, key applications of biometrics include: i) background checks of military personnel and contractors; ii) access control to physical and digital assets; and iii) identification of unknown and potentially hostile persons by a comparison of their biometric sample against a watch list.

- Law enforcement and background checks

Law enforcement agencies perform background checks that use biometrics to help confirm the identity of individuals who might be present in a biometric database. Background checks might also be provided as a service to other agencies within the government.

- Physical access control

Governments also use biometrics for physical access control by storing biometric data on a digital ID card and performing a match to verify that the holder of the card is the same person issued the card. Biometrics are also used for securing access to digital assets, where a biometric match might be required in addition to a password to gain access to a computer system.

Government biometrics systems typically operate on client/server-based computer networks. Enrollment workstations with peripheral capture devices are used to enroll individuals into biometrics systems. Enrollment involves the capture, processing, and formatting of “biometric samples.” A “biometric sample” is biometric data which may include: i) images of fingerprints, faces, or irises; ii) digital voice signals; or iii) some other electronic representation of a biometric characteristic. Examples of capture peripherals include: i) scanners for fingerprint images, ii) cameras for iris and facial images, iii) handheld devices for mobile capture of fingerprint, iris, and facial images, or iv) mobile phones for voice signals.

After biometric samples are captured, they are then transported in digital form to centralized matching systems for identification. Equipment used to perform these functions includes: i) servers to process and transport biometric samples; and ii) mainframe computers and servers to store and match those samples. In addition, military applications may employ handheld devices that are capable of capturing samples and matching those samples against sample databases that reside on the devices.

Due to the nature of government applications, particularly those involving security and defense, government biometrics systems must be capable of accurately and rapidly searching and matching biometric samples against large databases of stored samples. The ability to accurately and rapidly match samples against databases of millions of samples is critical because incorrect or delayed results could have severe adverse consequences. These requirements are an important distinguishing characteristic of the government market as compared to the commercial market.

Another characteristic that defines government markets can be seen in the difference between biometric identification and biometric verification. Biometric identification involves a one-to-many search of thousands or even millions of records to determine which, if any, record belongs to the individual in question. Government applications tend to involve biometric identification.

Biometric verification involves a one-to-one biometric comparison that serves to verify that both biometric samples belong to the same individual. One-to-one matches tend to require less algorithmic accuracy, speed, sensor fidelity, and computer processing power than “one-to-many” searches performed on large databases of stored biometric records. Commercial applications tend to involve biometric verification.

Commercial market

Biometrics-based solutions compete with more traditional security methods including keys, cards, personal identification numbers and security personnel in commercial markets. The adoption of biometrics by leading vendors of smartphones and other popular consumer products has increased users’ confidence and comfort with biometrics as a convenient and secure means of authentication. Biometrics solutions are also being considered in commercial markets as a means of increasing security and reducing fraud as part of “know-your-customer” and “know-your-employee” efforts. “Know-your-customer” initiatives are designed to verify the identity of customers before providing products or services. “Know-your-employee” initiatives are designed to verify the identity of employment candidates upon application for employment.

Notwithstanding these positive developments, commercial markets for biometrics technology are in the process of developing and evolving. The rate of adoption of biometrics in commercial markets depends upon a number of factors, including: i) the performance and reliability of biometric solutions; ii) costs involved in adopting and integrating biometric solutions; iii) public concerns regarding privacy; iv) potential privacy legislation; and v) standardization efforts by various industry consortia and standards bodies.

Principal biometrics applications in commercial markets involve the authentication and/or identification of individuals. The types of users that may need to be authenticated or identified in commercial applications include customers, employees, suppliers, visitors, patients, or other parties wishing to gain access to information, systems, bank accounts, credit card accounts, events, devices, buildings, or organizations.

Examples of commercial market applications include:

- User authentication for login and access to mobile devices, computers, networks, and software programs.
- User authentication for financial transactions in the financial services industry.
- User authentication for in-person or online purchases in the retail industry.
- User authentication for physical access to secured buildings and perimeters.

- User authentication of employees to access private patient information in the healthcare industry.
- Identity verification of patients in hospital and surgical settings.
- Identity verification of test takers in the educational testing industry.
- Identification of prospective customers in the financial services industry.
- Identification of candidates for pre-employment screening and background checks.
- Identification of undesirable customers in the gaming industry.

We believe that the commercial biometrics market may be further segmented into: i) a consumer mass market segment; and ii) an enterprise segment. While we believe this delineation serves a useful purpose in describing the current state of the market, it has its limitations because the two segments overlap.

Consumer mass market segment – This segment is dominated by biometrics-enabled smartphones. Many smartphones now contain fingerprint sensors and software that can: i) enroll and encode a fingerprint sample; ii) store the sample in a secure area on the phone; and iii) collect a live fingerprint and match it to the stored fingerprint sample. Once a biometric match is achieved, the subsequent software functions are analogous to password authentication. This type of biometric authentication is sometimes referred to as a “one-to-one” match and it requires a less complex and robust biometric match capability than that used in large client-server based biometrics systems.

Mobile biometrics authentication applications are largely controlled by smartphone manufacturers as this functionality is executed by smartphone operating systems and sensor hardware, as opposed to third-party applications running on the phone. Third party applications on smartphones are currently granted access to biometric authentication results, but may not necessarily have access to raw biometric samples, hardware, relevant security functions, or other smartphone capabilities. In contrast, authentication using facial or voice biometric modalities may be implemented in applications running on the phone, because these applications can make use of the camera and microphone on the device, which are generally granted broader access to third party developers.

User authentication and payment features enabled by smartphones continue to evolve, and we expect to see further changes in smartphone security features and functionality.

Enterprise segment – Enterprise biometrics systems are similar to government systems in that they typically operate in a client/server environment that: i) captures biometrics samples on a client PC; ii) stores those samples in a database on a server, and then, when queried; iii) matches live samples against stored samples. Mobile devices are likely to be used in conjunction with enterprise systems as we have seen a desire by customers to use smartphones as enrollment and access devices.

Opportunities and customer demand are beginning to emerge in the enterprise segment of the commercial market, but it remains a nascent and evolving market. We are beginning to see three potential types of opportunities, including:

1. Internal biometrics systems - Some customers want to purchase, install, and maintain custom or off-the shelf biometrics systems that they will operate. These customers tend to have a critical need or the scale to justify the cost of acquiring an internal biometrics system. Companies in the financial services industry would be an example of this class of customer.

2. Biometrics-as-a-service - Biometrics are often provided as services in government settings. For example, many traditional government biometrics systems can be considered a service provided to other government entities, such as those offered by the FBI to state and local law enforcement agencies.

Biometrics service providers have begun to offer pay-per-transaction biometrics service offerings in commercial markets. These services allow organizations to biometrically identify or verify employees, customers, or other individuals relevant to their business. A pay-per-transaction model may be potentially more financially attractive for some organizations as compared to the cost of purchasing, installing and maintaining internal biometrics systems.

3. Biometrically-enabled solutions – There are companies that offer products, systems, or solutions that are not principally marketed as biometrics products, but include biometrically-enabled components. These vendors represent an opportunity for core biometrics technology providers, because they generally do not own core biometrics technology. Examples of this class of customer would be companies that offer secure identification/access solutions or biometrics smart cards.

Biometrics industry participants

There are a large number of vendors that serve government and commercial biometrics markets. In order to provide an understanding of the biometrics industry and our role in it, we have categorized industry participants into categories that have been defined by us. While we believe our categorization is a reasonable representation of the industry, we acknowledge that: i) knowledgeable industry participants may define categories differently or classify vendors differently; and ii) not all companies involved in the industry were included. Accordingly, the classification that follows represents our perspective on the industry.

We believe that biometrics industry participants may be classified into the following categories:

1) Core technology suppliers
2) System integrators
3) Fully integrated solution suppliers
4) Biometrics-as-a-service providers
5) Vendors of biometrically-enabled solutions

Category descriptions and companies that offer products and services in each category are provided below. It should be noted that some companies appear in multiple categories.

1) Core technology suppliers

Core biometrics technology includes hardware and software products that enable: i) traditional biometrics systems used by government and commercial customers; ii) new biometric service offerings; and iii) biometrically-enabled functionality embedded in other products and solutions. Core biometrics technology includes three types of products: i) sensor products, ii) biometric capture devices, and iii) software products.

Sensor products

Biometrics sensors are primarily silicon-based devices that capture biometrics samples, such as fingerprints. Sensors are typically embedded in other devices, such as smartphones or biometric capture devices.

Examples of companies that offer biometric sensor products include: 1) Qualcomm Technologies, Inc. through its acquisition of UltraScan Corporation; 2) Sonavation, Inc.; 3) Synaptics, Inc.; 4) Fingerprint Cards AB; 5) Integrated Biometrics, LLC; and 6) Next Biometrics AS.

Biometric capture devices

Biometric capture devices are designed to capture and process biometric samples as their primary function. These products may be strictly hardware products or hardware products that also incorporate biometrics software.

Examples of companies that offer biometric capture devices include: 1) Cross Match Technologies, Inc.; 2) Suprema, Inc.; 3) HID Global Corporation through its 2014 acquisition of Lumidigm, Inc. (“HID”); 4) Iris ID Systems, Inc (“Iris ID”); 5) Precise Biometrics AB (“Precise Biometrics”); 6) Credence ID, LLC; 7) SecuGen Corporation; 8) IrisGuard, Inc. (“IrisGuard”); 9) Aurora Biometrics, Inc. (“Aurora Biometrics”); 10) EyeLock LLC (“EyeLock”); and 11) Tascent, Inc. through its 2015 acquisition of Aoptix Technology Identity Solutions’ business unit.

Software products

Biometrics software products provide functionality that captures, formats, stores, processes, or matches samples of fingerprints, faces, iris, voices and other modalities. Biometrics software is capable of operating on variety of equipment platforms, including personal computers, smartphones, biometric capture devices, hand-held devices, servers, and mainframe computers.

Examples of companies that offer biometrics software products include: 1) Aware, Inc.; 2) MorphoTrak and MorphoTrust, divisions of the Safran Group Company ("Safran Morpho"); 3) 3M Cogent Inc. ("3M Cogent"); 4) NEC Corporation ("NEC"); 5) Cognitec Systems GmbH ("Cognitec"); 6) Neurotechnology; 7) Iritech, Inc. ("Iritech"); 8) Innovatrics s.r.o. ("Innovatrics"); 9) M2Sys Technology ("M2Sys"); 10) SpeechPro, Inc.; 11) Agnitio S.L.; 12) Precise Biometrics; 13) Facebanx, a subsidiary of OhHi, Ltd; 14) VoiceTrust GmbH.; 15) Eyelock; 16) BIO-key International, Inc.; 17) VoiceVault Inc.; 18) EyeVerify, Inc.; 19) Iris ID; 20) IrisGuard; 21) Aurora Biometrics; 22) NexID Biometrics LLC.; and 23) Daon Trusted Identity Services ("Daon").

2) System integrators

System integrators purchase hardware and software technology from core biometrics technology vendors and incorporate those components into customized biometrics systems that they deliver to end-user customers. Historically those end-user customers have been governments, but in recent years system integrators have begun to serve commercial enterprise customers as well. System integrators include large multinationals with a broad range of expertise and the capacity to execute very large projects, as well as smaller system integrators that have more focused expertise on a particular market sector, technology, or geography. Some system integrators have developed their own biometric technologies that they deliver as part of their solutions.

Examples of companies that offer systems integration services include: 1) Northrop Grumman Corporation; 2) Lockheed Martin Corporation; 3) Science Applications International Corporation; 4) Hewlett-Packard Enterprise Services; 5) International Business Machines Corporation; 6) Fujitsu Limited; 7) Accenture plc; 8) Unisys Corporation; 9) Leidos, Inc.; and 10) ManTech International Corporation.

3) Fully integrated solutions suppliers

Fully integrated solutions suppliers are similar to systems integrators in that they deliver customized biometrics systems to government and commercial enterprise end-user customers. They differ from system integrators in that they use core hardware and software technologies that they developed in-house or acquired from others. Vendors in this category may purchase some third party software, but we believe such purchases represent a minor component of the overall systems they deliver.

There are three large global suppliers of fully integrated solutions, including: 1) Safran Morpho; 2) 3M Cogent; and iii) NEC. We believe these companies supply a large percentage of the biometric systems that are delivered to government customers around the world.

In addition to these three large suppliers, we would categorize Dermalog Identification Systems GmbH as a fully integrated solution provider, but one that operates on a smaller scale. Aware also has a product portfolio and services capability that enables us to deliver fully integrated solutions. We have acted in this capacity on a limited basis in the past and an element of our strategy is to grow this part of our business in the future.

4) Biometrics-as-a-service providers

Biometrics service providers have begun to offer a pay-per-transaction biometrics service offering. This service allows organizations to biometrically identify or verify employees, customers, or other individuals relevant to their business. A pay-per-transaction model may be potentially more financially attractive for some organizations as compared to the cost of purchasing, installing and maintaining internal biometrics systems.

Examples of companies offering biometrics services include: 1) Certibio Identidade Biometrica, a wholly-owned subsidiary of Certisign Certificadora Digital S.A. ("Certisign"); 2) Safran Morpho; and 3) Daon.

5) Vendors of biometrically-enabled solutions

Vendors of biometrically-enabled solutions provide products that are not principally marketed as biometrics products, but include biometric functionality. Biometrics capability is a feature, but not the chief function of these products. Such vendors represent a potential opportunity for core biometrics technology providers as some of them do not own core biometrics technology.

Examples of companies that offer biometrically-enabled smartphone products include: 1) Apple, Inc.; 2) Samsung Electronics Co., Ltd.; and 3) Google, Inc.

Examples of companies that offer secure identification/access solutions that incorporate biometrically-enabled components include: 1) Gemalto NV; 2) HID; 3) Entrust Datacard Corporation; and 4) Oberthur Technologies.

Examples of companies that offer physical access control solutions that may incorporate biometrics include: 1) Honeywell International, Inc.; 2) Tyco International Ltd.; 3) Lenel Systems International Inc.; and 4) Stanley Security Limited.

Products and Services

Software products

We sell a broad range of biometrics software products for fingerprint, facial, and iris modalities. Our software products enable important functions in biometrics systems, including:

1. Enrollment, analysis, and processing of biometric images and data on workstations or mobile devices.
2. Integration of peripheral biometric capture devices.
3. Centralized workflow, transaction processing, and subsystem integration.
4. Matching of biometric samples against biometric databases to authenticate or verify identities; and
5. Analysis and processing of text-based identity data.

Our biometrics software products range from discrete software blocks that customers can use to develop their own solutions to more complete applications that customers can use to reduce or eliminate their development times. We classify our biometrics software products into five product groups, including, i) Software Development Kits; ii) Enrollment Controls and Applets; iii) Applications; iv) Middleware/Workflow Server; and v) Cluster Computing Platform. Each of these product groups is described below.

1) Software Development Kits. Our software development kits or ("SDKs") consist of: i) multiple software libraries; ii) sample applications that show customers how to use the libraries; and iii) documentation. Customers use our SDKs to design and develop biometrics applications. Our SDK products may be categorized into three groups: i) Enrollment; ii) Search and Matching; and iii) Identity Data Management and Analytics. These products are described below.

SDK Group 1: Enrollment SDKs. Our suite of enrollment SDKs performs a variety of functions that are critical to biometric enrollment, including image capture, image quality assurance, image formatting, and image compression. Our enrollment SDK products include:

- Hardware abstraction, autocapture, and quality assurance products, including: i) LiveScan API; ii) PreFace™; iii) IrisCheck™; and iv) SequenceCheck™.

- Biometric data formatting, validation and reading products, including: i) NISTPack; ii) ICAOPack; and iii) PIVPack™.

- Fingerprint, facial, and iris image compression and decompression products, including: i) Aware WSQ1000; and ii) Aware JPEG2000.

- Fingerprint card scanning and printing products, including: i) AccuScan™; and ii) AccuPrint™.

- Mobile products for smartphones and tablets, including: i) NISTPack Mobile; ii) WSQ1000 Mobile; iii) ICAOPack Mobile; iv) PIVPack™ Mobile; v) AwareXM™ Mobile, and vi) PreFace™ Mobile.

- Application specific bundles, including CaptureSuite™ which is used for the development of applications for the capture of live scan or card scan fingerprint images.

SDK Group 2: Biometric Search and Match SDKs. Our Nexa™ line of biometric search and matching products for fingerprint, face and iris includes our Nexa|Fingerprint™, Nexa|Face™, and Nexa|Iris™ products. These products contain algorithms that convert images into biometric templates. A biometric template is a mathematical representation of a biometric image. Templates can then be compared to templates stored in databases to find matches. Our Nexa products also compare and match templates.

Each Nexa SDK can be deployed on a workstation or a server, either as a standalone biometric search/match API, or in combination with our other SDKs, applications, and BioSP product. Our SequenceCheck, PreFace, and IrisCheck SDKs may be used in concert with Nexa libraries to perform optional quality assurance and preprocessing for enhanced fingerprint, face, and iris search and match functionality.

Our biometric search and match SDKs also include our AwareXM™ product which extracts and matches MINEX-compliant fingerprint templates.

SDK Group 3: Text Search and Identity Analytics SDKs. We have two products in this SDK group, including: i) Inquire|Search™; and ii) Inquire|Resolve™. These products contain algorithms for text-based filtering, searching, matching, and linking functions to discover useful information in identity data. Product capabilities include: i) integrating and resolving identity-centric data across multiple data stores; ii) assessing data quality and detecting anomalies; iii) performing link analysis and relationship discovery; and iv) performing text-based pre- and post-filtering of biometric searches.

2) Enrollment Controls and Applets. This group of products consists of our BioComponents™ line of products. Our BioComponents products allow customers to develop biometric enrollment applications more quickly than if they purchased our SDKs. Each product in the group includes a user interface and one or more software libraries that perform a discrete set of functions, such as automated image capture, quality assurance, and capture hardware integration. BioComponents comprise modular, independent, self-contained software components that can operate either independently or in concert with one another. Specific BioComponents products and the functions they perform are:

- BiographicComponent enables highly configurable data entry of biographic and textual information.
- FingerprintComponent is used to capture, verify image quality, and compress fingerprint images.
- FaceComponent is used to capture, verify image quality, and manipulate facial images.
- IrisComponent is used to capture, segment, and verify image quality of iris images.
- TravelDocComponent is used to authenticate travel documents, such as passports and driver’s licenses.
- ScanningComponent is used to scan forms such as inked fingerprint cards.
- PrintingComponent is used for printing FBI-quality fingerprint images on cards and forms.
- SignatureComponent is used to collect handwritten signature images from an electronic signature pad.
- PackagingComponent allows access to the data sets from the other components.

3) Applications. Our products in this category combine user interfaces with multiple Aware software libraries and/or BioComponents to create more complete applications that operate on client workstations or mobile devices. Our application products and the functions they perform are:

- Universal Registration Client (“URC™”). URC is a configurable Windows-based application that performs a variety of biometric data capture, analysis, matching, formatting, and hardware abstraction functions.

- URC Mobile. URC Mobile is a software application for performing biometric enrollment, identification, and screening on mobile biometric devices, such as those used by military personnel in the field.

- FormScannerSE and FormScannerMB. These are two independent applications for scanning and processing of inked fingerprint cards.

-

FormScannerSWFT. This product is a version of FormScannerSE that is preconfigured for use in compliance with the "Secure Web Fingerprint Transmission" program of the U.S. Department of Defense.

- Forensic Workbench. Forensic Workbench is a software application for the categorization, processing, and standards-compliant formatting of biometric images and demographic data.

- Sequence Workbench. Sequence Workbench is a software application for the detection and assisted repair of fingerprint records containing sequence errors.

- CrosslinkWorkbench. CrosslinkWorkbench is an application that utilizes several Aware SDKs for assisting with identifying and repairing of crosslink errors in ANSI/NIST ITL transactions. Crosslinks are biometric records that erroneously contain data from different individuals.

- FaceWorkbench. FaceWorkbench provides a user interface and systematic workflow to enable an analyst to analyze and process the candidates returned from a biometric face search.

- WebEnroll. WebEnroll provides a reference application that uses BioComponents for browser-based enrollment of biographic data, fingerprints, facial images, and iris images.

4) Middleware/Workflow Server. Our Biometric Services Platform, or BioSP^{TM} product, is a service-oriented application used to enable workflow, subsystem integration, and biometric data processing and management. BioSP is suited for applications that require the collection of biometrics throughout a distributed network. BioSP is designed to be modular, programmable, scalable, and secure. It is used to manage transaction workflow, including messaging, submissions, responses, and logging.

Key BioSP features and functionality include:

- automated biometric image and data analysis, processing, formatting, quality assurance, and reporting.
- web services in support of a scalable, secure, service-oriented architecture.
- integration of biometric functions with other enterprise systems such as identity management, access management, card management, and AFIS/ABIS.
- One-to-one and one-to-many biometric matching for verification, identification, and duplicate checking.
- centralized system administration and user management.
- advanced reporting capabilities for fast troubleshooting of biometric capture problems.
- centralized configuration, distribution, and management of enrollment client software.
- support for fingerprint, facial, iris, and palm modalities.

5) Cluster Computing Platform. In 2015, we introduced our Astra^{TM} cluster computing platform. Astra is a software platform that performs large-scale identity-related security tasks, including: i) biometric search and match; ii) biometric authentication; and iii) identity analytics. Astra distributes computing operations across a cluster of computing nodes, enabling rapid search of very large biometric databases and execution of high volumes of biometric authentications. Astra is designed to be algorithm-independent, but also works seamlessly with other Aware products, including our Nexa, Inquire, and BioSP products.

Imaging products

In addition to our biometrics software products, we also sell products used in applications involving medical and advanced imaging. Our principal imaging product is Aware JPEG 2000, which is based on the JPEG2000 standard. The JPEG2000 standard is an image compression standard and coding system that was created by the Joint Photographic Experts Group committee in 2000. Our JPEG2000 product is used to compress, store, and display images. Those images are typically medical images.

Software maintenance

We also sell software maintenance contracts to many of our customers who purchase software licenses. These contracts typically have a one year term during which customers have the right to receive technical support and software updates, if and when they become available. Customers tend to renew maintenance contracts during the period of time that our software is being used in their biometrics systems.

Services

We offer a variety of software engineering services, including: i) project planning and management; ii) system design; iii) software design, development, customization, configuration, and testing; and iv) software integration and installation. Services are typically, but not always, sold in conjunction with software licenses.

Service engagement deliverables may include: i) custom-designed software products; ii) custom-configured versions of existing software products; iii) one or more subsystems comprised of software products that are integrated within a larger system; or iv) complete software solutions. In some cases, the software resulting from service engagements may form the basis for new or improved Aware software products.

Our customers for services include: i) government agencies; ii) large multinational systems integrators; iii) smaller systems integrators with a particular market, technology or geographic focus; and iv) commercial providers of products, solutions, and services. We provide services directly to end-users or indirectly to end-users through systems integrators. When we provide services to systems integrators, they are often engaged with the end-user as a prime contractor and are responsible for delivery of a complete solution, in which case we typically serve as a subcontractor assigned a subset of the total scope of work.

The scope of our services projects varies. A small project might involve configuration and testing of a single software product, taking a small team one month or less. A large project might involve delivery of a more complex solution comprised of multiple products and subsystems, requiring a larger team to conduct project management, system design, software customization and integration, and taking up to one year or more. Some projects are followed by subsequent projects that serve to change or extend the features and functionality of the initial system.

Hardware products

We developed a biometrics software system for a U.S. government customer under a Small Business Innovation Research ("SBIR") contract that began in 2008 and ended in early 2013. When the software development project ended in early 2013, we entered into a separate contract to supply hardware products incorporating the developed software. Hardware products sold to this customer integrate the developed software with: i) hardware purchased from third parties; ii) software purchased from third parties; and iii) some of our biometrics software products. While other customers could theoretically purchase the hardware products developed for this customer, we believe that it is unlikely that they will do so, because of the highly customized nature of the products.

Sales and Marketing

As of December 31, 2015, we had a total of 11 employees in our sales and marketing organization. In addition to our employee sales staff, we also engage third party sales agents to sell our products and services in foreign countries.

We sell our products and services through three principal channels of distribution:

i) Systems integrator channel – we sell to systems integrators that incorporate our software products into biometrics systems that are delivered primarily to government end users.

ii) OEM channel – we sell to hardware and software solution providers that incorporate our software products into their products.

iii) Direct channel – we also sell directly to government, and, to a lesser degree, to commercial customers.

All of our revenue in 2015, 2014, and 2013 was derived from unaffiliated customers. Revenue from Certisign Certificadora Digital S.A. represented 10%, 2%, and 0% of revenue during 2015, 2014, and 2013, respectively. Revenue from the U.S. Navy represented 9%, 24%, and 21% of total revenue during 2015, 2014, and 2013, respectively. Revenue from the U.S. Marine Corps represented 3%, 10%, and 3% of total revenue during 2015, 2014, and 2013, respectively. No other customer represented 10% or more of total revenue in any of those years.

Competition

The markets for our products and services are competitive and uncertain. We compete against: i) other companies that provide biometric software solutions; and ii) fully diversified companies that provide biometric software solutions and also act as systems integrators. We can give no assurance that: i) our products and services will succeed in the market; ii) that we will be able to compete effectively; or iii) that competitive pressures will not seriously harm our business.

Many of our competitors are larger than us and have significantly greater financial, technological, marketing and personnel resources than we do. At the other end of the competitive spectrum, we have seen increasing competition from smaller biometrics companies in foreign countries. These smaller foreign competitors have demonstrated a willingness to sell their biometrics software products at low prices.

We can give no assurance that our customers will continue to purchase products from us or that we will be able to compete effectively in obtaining new customers to maintain or grow our business.

Aware’s Strategy

Our strategy is to capitalize on our strong brand and reputation to sell biometrics software products and services into government and commercial markets. We intend to offer a broad portfolio of high quality products that are coupled with expert technical support and services. We expect to continue to employ a three-pronged distribution strategy using systems integrators, OEMs, and direct sales.

Our strategy for growing our biometrics business may include one or more of the following elements:

i) *Product strategy* – Our product strategy is to offer more complete biometrics solutions. We believe this strategy will allow us to us to sell more software and services into biometrics projects. We recognized the need to make this transition several years ago and developed new products to enable this strategy.

Our strategy to offer complete solutions involves:

- Product line expansion - Our aim is to expand our product portfolio by adding new products and increasing the functionality of existing products using our internal engineering teams. This means we may add resources to our engineering staff. To the extent we are unable to develop critical new technologies