AWARE INC /MA/
Form 10-K
February 19, 2019

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, 2018

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 every Interactive Data File required to be submitted 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 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, a smaller reporting company, or an emerging growth company. See the definitions of "large accelerated filer", "accelerated filer", "smaller reporting company" and "emerging growth company" in Rule 12b-2 of the Exchange Act.:

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

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act. ¨

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, 2018 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 $53,303,310.

The number of shares outstanding of the registrant's common stock as of February 11, 2019 was 21,571,150.

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 22, 2019 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, 2018

TABLE OF CONTENTS

PART I

PART II

PART III

PART IV

2

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, visa applicant 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) identity proofing 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, iris, and voice 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 biographic data, tokens, paper credentials, passwords, PIN codes, and magnetic access cards. Biometrics technology and products require algorithms for multiple distinct functions, such as feature finding, feature optimization, feature extraction, feature encoding, feature matching, and presentation attack detection (“PAD”), which is also referred to as liveness detection and spoof detection.

Application Areas: Identification and Authentication

Applications for biometrics typically fall into two primary areas: identification and authentication. Generally speaking, biometric identification attempts to answer the question “who are you?”, while biometric authentication attempts to answer the question “are you the person we know?”

Biometric Identification

Biometric identification involves the “one-to-many” comparison of a “probe” sample to thousands or even millions of biometric samples in a database, comprising a search to determine which samples, if any, are associated with the individual that belongs to the probe. Biometric identification systems typically operate in a client/server architecture, with some systems migrating to web-based, thin-client architectures. 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 consists of 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 and/or microphones for voice signals.

After biometric samples are captured, they are 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.

“Identity proofing” is a term used to describe a process by which identity information provided by an individual, such as a prospective customer or job applicant, is corroborated between multiple identity sources. Biometric identification can be used as part of identity proofing.

Biometric Authentication

Biometric authentication involves a “one-to-one” biometric comparison that serves to verify that a live biometric sample belongs to the same individual associated with a trusted stored sample. In this way, biometrics can be used to authenticate identity. Computing devices such as PCs, smartphones and tablets, are capable of: i) capturing biometric samples (e.g., fingerprints, facial and iris images, and voices); ii) processing and storing those samples in a secure area on the device or server; and iii) matching new live samples against the trusted stored samples. Once a biometric match is achieved, the subsequent software functions are analogous to password-based authentication. Mobile authentication can be implemented in either a device- or server-centric architecture, with biometric data analysis, matching, and storage occurring either on the device or on a central server, respectively.

“Tokens” are often used as an alternative or enhancement to passwords. An authentication token may be a hardware device that the user must have possession of to authenticate. Examples are a USB dongle, smart phone, or smart card. In the case of multifactor authentication, a device such as a smart phone or PC may be considered as a token providing the primary authentication factor, with biometric authentication serving as a second authentication factor. Mobile authentication can be incorporated into a mobile app such as a banking application as a password-free security mechanism. It may also be employed in an “out-of-band” fashion to secure access on a PC through a browser.

As biometric authentication is most typically an unattended process, some form of presentation attack detection (“PAD”) is an important feature of biometric authentication solutions. PAD features are designed to prevent “spoofing”, whereby a fraudster attempts to defeat a biometric security feature by impersonating the rightful user.

The rapid advance and adoption of mobile devices has had a substantial impact on the adoption of biometrics for authentication. Many leading mobile devices incorporate native biometric security sensors and technology, in which case third-party mobile applications are granted access to authentication results but not the raw biometric samples

used to authenticate.

In contrast, third party application providers can incorporate authentication functionality that makes use of multipurpose sensors such as the camera, microphone, and touchscreen. There are use cases where it is desirable to implement biometric security features that are independent of those provided natively by the device. Advantages include more control over the security level, security features, and user experience, as well as uniform functionality across different device models. Biometric authentication implemented on a mobile device may be used to gain access to online networks, systems, services, or accounts.

User authentication enabled by smartphones continues to evolve, and we expect to see further advances in smartphone security features and functionality. In the past few years, the FIDO® (Fast IDentity Online) Alliance, an industry consortium, has emerged to take a leading role in authoring and promoting technical standards for password-free multifactor authentication on mobile devices and desktops. The FIDO Alliance has developed specifications that define an open, scalable, interoperable set of mechanisms that supplant reliance on passwords to securely authenticate users of online services. The new standard for devices and browser plugins will allow any website or cloud application to interface with a broad variety of existing and future FIDO-enabled devices that the user has for online security. The FIDO Alliance has also established processes for accreditation of independent labs that will be able to analyze and identify products as “FIDO® Certified” in terms of interoperability, biometric matching performance, and security level.

Market Sectors: Government and Commercial

The market for biometrics may be segmented into government and commercial sectors. Principal government biometrics applications include border control, visa applicant 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) identity proofing 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.

There is commonality between how biometric technologies are used across government and commercial sectors. The primary consumers of biometric identification systems are government agencies, while the primary users of biometric authentication technology are consumers owning mobile devices. We believe that these sector-based distinctions are important to an understanding of Aware's business as the vast majority of our revenue is currently derived from government customers.

Government Sector

Local, state, and national governments throughout the world were early adopters of biometrics technology and continue to be the largest consumers of the technology. 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 live (suspect is known) or latent (suspect is unknown) biometrics samples to state or federal biometric search services;
- Background checks for employment screening;
- Driver's 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.

- Access control

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

Due to the nature of government applications, particularly those involving security and defense, government biometrics systems must be capable of accurately and rapidly searching 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.

Commercial Sector

The principal application of biometrics in commercial markets is user authentication, with identity proofing also emerging as an application. The types of users that may need to be authenticated or identified in commercial applications include customers, employees, contractors, visitors, healthcare patients, or other parties wishing to establish their identity towards gaining access to information, systems, bank accounts, credit card accounts, events, devices, or buildings.

In commercial markets, biometrics-based solutions compete with more traditional security methods including keys, cards, tokens, passwords, personal identification numbers ("PINs") and security personnel. 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 in place of or in addition to passwords. Biometrics solutions are also being considered in commercial markets as a means to enhance identity proofing, sometimes referred to "know-your-customer" ("KYC") and "know-your-employee" ("KYE") efforts. KYC and KYE processes are designed to corroborate the identity data claimed by prospective customers and employees with multiple independent sources.

The commercial market for biometrics technology remains nascent. 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, including potential privacy legislation; and iv) standardization efforts by various industry consortia and standards bodies.

Examples of commercial market applications include:

- User authentication for login and access to mobile devices, mobile apps, desktop computers, networks, and web-based 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.
- Identity proofing of prospective customers in the financial services industry.
- Identity proofing of candidates for pre-employment screening and background checks.
- Identification of undesirable customers in the gaming industry.

Market Segments: Consumer-Facing and Employee-Facing

The biometrics market may be further segmented into: i) a consumer-facing segment; and ii) an employee-facing segment.

Consumer-Facing segment – The primary applications in the consumer-facing segment are biometric identity proofing and authentication for the purpose of onboarding and authentication of customers of commercial organizations, and also for citizens by governments. Adoption of biometrics is stronger where the convenience of a password-free user experience is valued but there is also risk of fraud. Industries that fall into this category include financial services, retail, and healthcare. Government agencies similarly employ citizen-facing biometric identity proofing and authentication solutions in situations where there is potential risk of fraud, such as benefits disbursement and voting. Healthcare organizations use biometrics in a safety context to prevent patient misidentification and care delivery errors.

Employee-Facing segment – The primary applications in the employee-facing segment are identity proofing and authentication of employees as a means for screening of new employees, and for user authentication towards securing access for employees and contractors to digital assets against a breach. Applications for employee-facing biometrics are found in both the government and commercial sectors.

Delivery Models: Tools and Services, Solutions, Software as a Service

As with other technology products and services, there are different models for product and service delivery in the biometrics arena, including tools and services, solutions, and Software as a Service.

1. Tools and Services – Customers can choose to build their own biometric system using off-the-shelf subcomponents purchased a la carte and used to design, develop, and operate their own bespoke system. In doing so, a customer may or may not decide to also receive services to help with that process. Those services might come from a software provider or a third-party system integrator. These customers tend to have highly specific requirements and the scale to justify the cost of acquiring a custom-configured biometric system. Government agencies tend to be an example of this class of customer.

2. Solutions – Some organizations prefer a more complete and comprehensive solution that sources most or all system capability and services from a single supplier and requires less customization. Companies that offer identification/access solutions or biometric smart cards tend to be an example of this class of customer.

3. Software as a Service – Advances in cloud computing and browser technology have made Software as a Service, or "SaaS" an increasingly common delivery model of enterprise software. Benefits derived include lower up-front costs as well as lower maintenance and support risk. Biometric solutions can be provided as SaaS. Small and midsize commercial enterprises tend to be an example of this class of customer.

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.; 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. which was acquired by HID Global Corporation in 2018; 2) Suprema, Inc.; 3) HID Global Corporation ("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.

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 a 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) Idemia; 3) Gemalto NV ("Gemalto"); 4) NEC Corporation ("NEC"); 5) Cognitec Systems GmbH ("Cognitec"); 6) Neurotechnology; 7) Iritech, Inc. ("Iritech"); 8) Innovatrics s.r.o. ("Innovatrics"); 9) Nuance Communications, Inc.; 10) Precise Biometrics; 11) VoiceTrust GmbH.; 12) Eyelock; 13) BIO-key International, Inc.; 14) Zoloz (formerly known as EyeVerify, Inc.); 15) Iris ID; 16) Dermalog Identification Systems GmbH ("Dermalog"); 17) FacePhi Biometria; and 18) Sensory, Inc.

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) Science Applications International Corporation; 3) Hewlett-Packard Enterprise Services; 4) International Business Machines Corporation; 5) Fujitsu Limited; 6) Accenture plc; 7) Unisys Corporation; 8) Leidos, Inc.; and 9) 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) Idemia; 2) Gemalto; and 3) 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 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) Idemia; 3) RightPatient, Inc.; 4) Microsoft Corporation; 5) SkyBiometry (a spin-off from Neurotechnology); 6) BioID GmbH; and 7) VoiceIt Technologies, LLC.

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; 2) HID; 3) Entrust Datacard Corporation; and 4) Idemia.

Examples of companies that offer physical access control solutions that may incorporate biometrics include: 1) Honeywell International, Inc.; 2) Tyco International Ltd.; 3) LenelS2 (formed by combination of Lenel and S2 Security both of which were acquired by United Technologies Corp.); and 4) Stanley Security Limited.

Products and Services

Software products

We sell a broad range of biometrics software products that 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;
5. Analysis and processing of text-based identity data.

Our biometrics software products range from discrete “building blocks”, such as software development kits (“SDKs”), application program interfaces (“APIs”) and applications that customers can use to develop their own systems to more complete solutions that customers can use to reduce or eliminate their development times and exposure to software support and maintenance risks. Our products are described below.

1) Building Blocks: SDKs, APIs, Applications, and Subsystems

1a. Biometric Search & Matching SDKs

Our 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 line of biometric search and match SDKs is called Nexa™ and it includes Nexa|Fingerprint™, Nexa|Face™, Nexa|Iris™ and Nexa|Voice™. These products provide high-performance biometric algorithms for fingerprint, facial, iris and voice identification or authentication. The algorithms in these products convert images into biometric templates, which can then be compared to templates stored in databases to find matches.

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, BioSP, or Astra products. 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.

In addition to the Nexa line of biometric search and match SDKs, we also offer AwareXM™, an interoperable fingerprint matching SDK. Aware XM is an SDK that provides MINEX-certified, INCITS 378-compliant fingerprint minutiae extraction, template generation, and fingerprint authentication.

1b. Biometric Enrollment SDKs and APIs

Our suite of enrollment SDKs and APIs 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 and API products include:

- *Image Capture and Hardware Abstraction* – This group of products includes: i) LiveScan API; ii) PreFace™; iii) IrisCheck™; and iv) SequenceCheck™.

- *Data Formatting and Validation* – This group of products includes: i) NISTPack; ii) ICAOPack; and iii) PIVPack™.

- *Fingerprint Cards* – This group of products includes: i) AccuScan™; and ii) AccuPrint™, used for scanning and printing of fingerprint cards in accordance with FBI fingerprint image quality standards.

- *Image Compression* – This group of products includes: i) Aware WSQ1000; and ii) Aware JPEG2000 for standards-compliant compression and decompression of biometric images.

- *Mobile Enrollment and Matching* – Aware offers versions of several of our Windows-based products designed to operate on Android and iOS platforms. Our family of mobile SDKs includes: i) NexalFace™ Mobile; ii) NexalFingerprint™ Mobile; iii) PreFace™ Mobile; iv) LiveScan API Mobile; v) NISTPack Mobile; vi) WSQ1000 Mobile; vii) AwareXM™ Mobile; and FIDO® Suite. FIDO® Suite is a family of products that are certified by the FIDO Alliance and are interoperable with other FIDO-certified products. Our FIDO Suite includes: i) Aware FIDO® Face Authenticator; Aware FIDO® Face+Voice Authenticator; iii) Aware FIDO® Client; and iv) Aware FIDO® Server. These products are available for Android and iOS devices.

1c. Identity Text Analytics SDK - Inquire™

Inquire is a SDK that performs fuzzy text-based filtering, searching, matching, and linking functions towards discovery of useful information in identity data. Analysis of text-based identity data is naturally complementary to biometric verification and identification, and Inquire is optimized for processing and analysis of data that includes biometrics.

1d. Biometric Applications

Our products in this category combine user interfaces with multiple Aware software products to create more complete applications that operate on client workstations or mobile devices.

Enrollment Applications

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

URC|Mobile™ is a software application for capturing fingerprint and facial images on an Android smart phone or tablet using its onboard camera and a tethered fingerprint capture device. It is designed to be used by an enrollment attendant for rapid capture and quality assurance of biometric data and submission to a centralized biometric database for enrollment, search, or authentication.

Our fingerprint card products include FormScannerSE™ and FormScannerMB™. The two products are independent applications that may be used for scanning and processing of inked fingerprint cards.

- FormScannerSE is designed for one-at-a-time, assisted "scan and entry" processing of fingerprint cards, such as for manual data entry of previously scanned card batches. It can also be used for manual "rework" such as crop region adjustments.

- FormScannerMB is designed for "multi-batch" scanning of large volumes of cards in an automated fashion, and provides features useful for high-volume processing such as support for automatic document feeding and real-time image quality feedback.

Forensic Workstations

Our forensic analysis and quality assurance products include WorkbenchSuite™. WorkbenchSuite is a family of .NET workstation applications that are designed to be used by an operator to analyze and repair or otherwise process digital records containing biometric images and data. Each targets a particular use case and implements workflow carefully designed to best assist analysts in their task. The suite comprises:

- FingerprintWorkbench, which is used for forensic analysis, processing, and reporting of biometric fingerprint evidence comparison and search results.

- ForensicWorkbench, which is used for the categorization, processing, and standards-compliant formatting of biometric images and demographic data.

- SequenceWorkbench, which is used for the detection and assisted repair of fingerprint records containing sequence errors.

- CrosslinkWorkbench, which is used 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, which enables an analyst to analyze and process candidates returned from a biometric face search.

Application Components

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:

- FingerprintComponent, which is used to capture, verify image quality, and compress fingerprint images.
- PhotoComponent, which is used to capture, verify image quality, and manipulate facial images.
- ScanningComponent, which is used to scan forms such as inked fingerprint cards.
- PrintingComponent, which is used for printing FBI-quality fingerprint images on cards and forms.
- NISTComponent, which is used for biographic and textual data entry and formatting, NIST compliance checking, and submission.

1e. Biometric Subsystems

Biometric Services Platform - BioSP™

Our Biometric Services Platform product is called BioSP. BioSP is a service-oriented platform used to enable a biometric system with advanced biometric data processing and management functionality in a web services architecture. It provides workflow, data management and formatting, and other important utilities for large-scale fingerprint recognition, face recognition, and iris recognition systems. BioSP is well suited for applications that require the collection of biometrics throughout a distributed network, and subsequent aggregation, analysis, processing, distribution, matching, and sharing of data with other system components. BioSP is modular, programmable, scalable, and secure, capable of managing all aspects of transaction workflow including messaging, submissions, responses, and logging. BioSP makes extensive use of open-source components and is J2EE-compliant.

Cluster-Based Matching Platform - Astra™

Our cluster-based matching platform product offering is called Astra. Astra is used for large-scale fingerprint recognition, face recognition, iris recognition, and text-based name matching and identity resolution. It is a highly scalable biometric identification and authentication platform that performs one-to-many search or one-to-one match against large stores of biometrics and other identity data. It does so by deploying biometric and text data and matching algorithms across a cluster of multiple computing nodes.

2) Integrated Solutions

2a. Knomi™

In 2017, we introduced Knomi, a mobile biometric authentication framework offering face, voice and keystroke dynamics. The Knomi mobile biometric authentication framework is a collection of biometric SDKs running on mobile devices and a server that together enable strong, multi-factor, password-free authentication from a mobile device using biometrics. Knomi offers multiple biometric modality options, including facial recognition, keystroke dynamics, and voice authentication as means to authenticate. Banks or any other commercial enterprise can deploy Knomi to enhance their password-based authentication mechanisms, making login to their mobile applications more secure and convenient for their customers and employees. Knomi software components can be used in different combinations and configurations to enable either a server-centric architecture or a device-centric, FIDO® Certified implementation.

2b. AwareABIS™

AwareABIS is an Automated Biometric Identification System (“ABIS”) used for large-scale biometric identification and deduplication using fingerprint, face, and iris recognition. It is a highly scalable platform that performs one-to-many search or one-to-one match against large stores of biometrics and other identity data. It does so by deploying biometric data and matching algorithms across a cluster of multiple computing nodes. Extremely large biometric databases (tens of millions of records) cannot be stored or efficiently searched on a single computer. Distributing the data and biometric comparison tasks across multiple machines enables even extremely large databases to be searched in only seconds. AwareABIS enables not only massive biometric search tasks but complex filter, search, match, and link operations critical to data preparation and quality assurance functions such as identity resolution and data deduplication. AwareABIS is built upon several mature, high-performance, field-proven applications, platforms, and algorithms from Aware. Components are available a la carte depending on the application and system requirements.

2c. WebEnroll

WebEnroll is a browser-based biometric enrollment and data management solution available as an enhanced version of BioSP™ (Biometric Services Platform) that utilizes BioComponents for capture of biographic data, fingerprints and facial images in a browser. Each BioComponent performs advanced biometric image autocapture as well as capture device hardware abstraction. Once images are captured, they are submitted to BioSP, where configurable workflows and modular software applications are used for processing, routing, and storage of each transaction. Biometric verification or identification can be added with Nexa or one of several third-party matchers integrated with BioSP, or an external matching service.

2d. Indigo

Indigo™ is Aware's family of turnkey biometric solutions, available as traditional software licenses or as cloud-based software-as-a-service. Indigo solutions are designed to deliver useful functionality and powerful biometric matching performance out-of-the-box, without requiring integration and configuration. They are built upon Aware's time-tested, market-leading software components for biometric enrollment, analysis, and matching.

3) 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.

Sales and Marketing

As of December 31, 2018, we had a total of 10 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 2018, 2017, and 2016 was derived from unaffiliated customers. In 2018, two customers represented 20% and 13% of total revenue. In 2017, one customer represented 17% of total revenue. In 2016, two customers represented 21% and 13% of total revenue. 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 continue 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 involve