VASCO DATA SECURITY INTERNATIONAL INC
Form 10-K
March 13, 2015
Table of Contents

UNITED STATES

SECURITIES AND EXCHANGE COMMISSION

Washington, D.C. 20549

FORM 10-K

FOR ANNUAL AND TRANSITION REPORTS PURSUANT TO

SECTIONS 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934

(Mark One)

[x] ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(D) OF THE SECURITIES EXCHANGE ACT OF 1934

FOR THE FISCAL YEAR ENDED DECEMBER 31, 2014

or

[ ] TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934

FOR THE TRANSITION PERIOD FROM _____TO_____

Commission file number 000-24389

VASCO Data Security International, Inc.

(Exact Name of Registrant as Specified in Its Charter)

DELAWARE	**36-4169320**
(State or Other Jurisdiction of	**(IRS Employer**
Incorporation or Organization)	**Identification No.)**

1901 South Meyers Road, Suite 210

Oakbrook Terrace, Illinois 60181

(Address of Principal Executive Offices)(Zip Code)

Registrant s telephone number, including area code:

(630) 932-8844

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

Title of each class	Name of exchange on which registered
Common Stock, par value $.001 per share	**NASDAQ Capital 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 by 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 15(d) of the 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. [ ]

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 definition of large accelerated filer, accelerated filer and smaller reporting company in Rule 12b-2 of the Exchange Act.

Large accelerated filer ____ Accelerated filer __X__ Non-accelerated filer ____ Smaller reporting company ____
(do not check if 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, 2014, the aggregate market value of voting and non-voting common equity (based upon the last sale price of the common stock as reported on the NASDAQ Capital Market on June 30, 2014) held by non-affiliates of the registrant was $341,424,343 at $11.60 per share.

As of February 27, 2015, there were 39,671,888 shares of common stock outstanding.

DOCUMENTS INCORPORATED BY REFERENCE

Certain sections of the registrant s Notice of Annual Meeting of Stockholders and Proxy Statement for its 2015 Annual Meeting of Stockholders are incorporated by reference into Part III of this report.

Table of Contents

TABLE OF CONTENTS

This report contains trademarks of VASCO Data Security International, Inc. and its subsidiaries, which include VASCO, the VASCO V design, Digipass as a Service, MYDIGIPASS.COM, DIGIPASS, VACMAN, aXsGUARD, Cronto and IDENTIKEY.

Cautionary Statement for Purposes of the Safe Harbor Provisions of the Private Securities Litigation Reform Act of 1995

This Annual Report on Form 10-K, including Management s Discussion and Analysis of Financial Condition and Results of Operations and Quantitative and Qualitative Disclosures About Market Risk contains forward-looking statements within the meaning of Section 21E of the Securities Exchange Act of 1934, as amended and Section 27A of the Securities Act of 1933, as amended concerning, among other things, our expectations regarding the prospects of, and developments and business strategies for, VASCO and our operations, including the development and marketing of certain new products and services and the anticipated future growth in certain markets in which we currently market and sell our products and services or anticipate selling and marketing our products or services in the future. These forward-looking statements (1) are identified by use of terms and phrases such as expect , believe , will , anticipate , emerging , intend , plan , could , may , estimate , goal , possible , potential , project , and similar words and expressions, but such words and phrases are not the exclusive means of identifying ther and (2) are subject to risks and uncertainties and represent our present expectations or beliefs concerning future events. VASCO cautions that the forward-looking statements are qualified by important factors that could cause actual results to differ materially from those in the forward-looking statements. These risks, uncertainties and other factors have been described in greater detail in this Annual Report on Form 10-K and include, but are not limited to, (a) risks specific to VASCO, including demand for our products and services, competition from more established firms and others, pressure on price levels and our historical dependence on relatively few products, certain suppliers and key customers, (b) risks inherent to the computer and network security industry, including rapidly changing technology, evolving industry standards, increasingly sophisticated hacking attempts, increasing numbers of patent infringement claims, changes in customer requirements, price competitive bidding, and changing government regulations, and (c) risks of general market conditions, including, currency fluctuations and the uncertainties resulting from turmoil in world economic and financial markets Thus, the results that we actually achieve may differ materially from any anticipated results included in, or implied by these statements. Except for our ongoing obligations to disclose material information as required by the U.S. federal securities laws, we do not have any obligations or intention to release publicly any revisions to any forward-looking statements to reflect events or circumstances in the future or to reflect the occurrence of unanticipated events.

PART I

Item 1 - *Business*

VASCO Data Security International, Inc. was incorporated in the State of Delaware in 1997 and is the successor to VASCO Corp., a Delaware corporation. Our principal executive offices are located at 1901 South Meyers Road, Suite 210, Oakbrook Terrace, Illinois 60181; the telephone number at that address is 630 932 8844. Our international headquarters in Europe is located at World-Wide Business Center, Balz-Zimmermannstrasse 7, CH-8152, Glattbrugg, Switzerland; the phone number at this location is 41 (0)43 555 3500. Our principal operations offices in Europe are located at Koningin Astridlaan 164, B-1780 Wemmel, Belgium and the telephone number at that address is 32 (0)2 609 9700. Unless otherwise noted, references in this Annual Report on Form 10-K to VASCO , company , we , our , and us refer to VASCO Data Security International, Inc. and its subsidiaries.

Additional information on the company, our products and services and our results, including the company s annual report on Form 10-K, quarterly reports on our Form 10-Q, current reports on Form 8-K, and amendments to those reports filed with the Securities and Exchange Commission (the SEC) are available, free of charge, on our website at https://www.vasco.com. You may also read and copy any materials we file with the SEC at the SEC s Public Reference Room at 100 F Street, NE, Washington, DC 20549. You may obtain information on the operation of the Public Reference Room by calling the SEC at 1-800-SEC-0330. Our reports are filed electronically with the SEC and are also available on the SEC s website (http://www.sec.gov).

General

VASCO is an IT security company that designs, develops and markets security solutions that secure and manage access to digital assets and protect transactions. VASCO is a world leader in providing two-factor authentication and digital signature solutions to financial institutions. VASCO solutions secure access to data and applications on-premise in global enterprises and in the cloud, and provide tools for application developers to easily integrate security functions into their web-based and mobile applications. Two-factor authentication (also known as 2FA) strengthens the process of verifying the identity of users by means of a combination of two different components. These components may consist of something that the user knows, such as username, and another item that the user possesses, such as a VASCO hardware or software authenticator that generates a one-time password (OTP). Two-factor authentication is a type of multi-factor authentication. VASCO s security solutions include both open standards-based and proprietary solutions, some of which are patented products and services used for authentication, digitally signing transactions and documents, and identity management in Business-to-Business (B2B), Business-to-Employee (B2E) and Business-to-Consumer (B2C) environments.

Historically, we have focused on two target markets, the banking and/or financial services market (which we refer to as the Banking Market or Banking) and the enterprise and application security market (which we refer to as the Enterprise and Application Security Market or Enterprise and Application Security). Our target markets include all applications where individuals use a username and password to access assets, information, and transactions that have value.

In this increasingly connected world, online and mobile application owners and users benefit from our expertise in two-factor authentication, transaction signing, and application security. Our convenient and proven security solutions enable trusted interactions between businesses, employees, and consumers across a variety of online and mobile platforms.

In order to grow in this rapidly evolving market, VASCO has developed a growth strategy. Our strategy includes the following;

Bringing the next generation of authentication and digital signature technologies to our customers to coincide with their authentication refresh cycles,

Driving increased demand for our products in new applications and new markets,

Increasing the adoption of our Authentication-as-a-Service and cloud-based solutions,

Continuing to expand our client base in segments beyond our core business, and

Acquiring security technology companies that either expand our technology portfolio or our customer base.

Our newest product offerings add risk-based solutions using a scoring mechanism to our existing authentication product lines. The risk-based solutions are being integrated into our on-premise, cloud-based, and mobile solutions. This enables us to offer our customers security that is appropriate for their task or transaction.

The number of people using the internet via computers, tablets, and smart phones continues to grow at a rapid pace. Consumers are embracing online and mobile purchasing and banking in ever-increasing numbers. Organizations of all types have an increasing number of employees and business partners accessing protected resources from remote locations. New business paradigms such as these introduce new security risks for all participants, especially banks, merchants, and online service providers. Large and powerful criminal hacking organizations have emerged. The criminal activities of private and state-sponsored hacking organizations has driven an increased need for security solutions and the expansion of regulations requiring organizations to improve their security measures to protect against hacking attacks and breaches. Several governments worldwide have recognized the risk associated with using fixed passwords for internet applications and have issued specific rules requiring two-factor authentication for online banking security. We anticipate that this trend may continue and that governments in other countries could prepare similar guidance or rules in order to protect their citizens online assets.

Our Background

Our predecessor company, VASCO Corp., entered the data security business in 1991 through the acquisition of a controlling interest in ThumbScan, Inc., which we renamed as VASCO Data Security, Inc. In 1996, we expanded our computer security business by acquiring Lintel Security NV/SA, a Belgian corporation, which included assets associated with the development of security tokens and security technologies for personal computers and computer networks. Also in 1996, we acquired Digipass NV/SA, a Belgian corporation, which was also a developer of security tokens and security technologies and whose name we changed to VASCO Data Security NV/SA in 1997.

In 1997, VASCO Data Security International, Inc. was incorporated and in 1998, we completed a registered exchange offer with the holders of the outstanding securities of VASCO Corp. In December 2006, we opened our international headquarters in Zurich, Switzerland. In 2007, we established wholly-owned sales subsidiaries in Brazil and Japan. In 2008 and 2009, we established wholly-owned sales subsidiaries in Mumbai, India and Bahrain, respectively. In 2011, we completed the establishment of our wholly-owned sales subsidiary in China and received our trade license for a new subsidiary in Dubai, United Arab Emirates.

Since the 1998 exchange offer, we have engaged in ten acquisitions and one disposition. Our most recent acquisitions have included Cronto Limited and Risk IDS Limited.

In May, 2013, we acquired Cronto Limited (Cronto), a provider of secure visual transaction authentication solutions for online banking. Cronto s patented solution offers a robust, yet simple way to assure

that a financial transaction has not been compromised, or hacked. The Cronto solution has been integrated into VACMAN Controller and IDENTIKEY Server, VASCO s security platforms that support VASCO s entire family of strong authentication and e-signature products.

In May 2014, we acquired Risk IDS, a provider of risk-based authentication solutions to the global banking community. The platform is designed to evaluate the profile of the user requesting access to the system to determine the risk profile associated with the transaction. It features a real-time analysis engine that uses rules and statistical techniques to improve real-time fraud detection. The Risk IDS solution is being integrated into our family of strong authentication and e-signature products.

Our Approach

We believe that security solutions for authentication, digital signature, and identity management that protect access to financial accounts and internal and cloud applications as well as the integrity of transactions, must be broad in scope and address all of the critical aspects of data security. The market requirements for security continue to evolve and we are responding by expanding our solutions beyond traditional authentication to include more channels such as mobile and ATM security. We believe that effective security solutions must address and assimilate issues relating to the following:

Speed and ease of implementation, use, and administration,

Reliability,

Interoperability within diverse applications on-premise and in the cloud,

Scalability, and

Overall cost of ownership.

Accordingly, we have adopted the following approach to data security in designing our products:

Where appropriate, we incorporate industry-accepted, open and non-proprietary protocols. This permits interoperability between our products and multiple platforms, products, and applications widely in use.

We minimize the effort required for implementation and integration with existing legacy applications and infrastructure.

We try to offer a more attractive total cost of ownership than competing products and services.

We support a wide variety of devices used to gain access to applications through the internet including personal computers, smart phones, tablets, and other personal devices.

We develop products that are designed to provide a balance between ease of use and the strength of the underlying authentication technology used. Our single sign-on product allows users to access multiple applications using one credential. Some of our client products use quick-response (QR) codes that allow a user to minimize key strokes by optically scanning a QR code that may be encrypted, thus increasing the strength of the security being used.

- We provide multiple choices to our customers with our cloud service platforms. By using our authentication platform, customers can deploy two-factor authentication quickly.

As a result of this approach, we believe that we are a leading provider of two-factor authentication, digital signature, and identity management security solutions that can help reduce customers losses to fraud and hacking.

Table of Contents

Our Products and Services

Our authentication product line provides a flexible and affordable means of authenticating users to networks and to web-based and mobile applications. Our products calculate dynamic passwords, also known as one-time passwords (OTP), that authenticate users logging onto networks or other applications. In addition, our products can be used to calculate digital signatures to protect electronic transactions and the integrity of the contents of such transactions.

Multi-factor authentication consists of several factors:

What the user knows (such as a username or a PIN code);

What the user has (such as a DIGIPASS authenticator, hardware or software version); and

Who the user is (biometrics).

Our product family is currently based on the first two factors. Using our solution, to enter a remote system, access protected applications, or digitally sign a transaction, the user needs the following:

Knowledge of either a username or a PIN code, and

An authenticator, either a DIGIPASS hardware authenticator or a DIGIPASS software authenticator downloaded onto existing compatible device.

Both factors help ensure that the correct person is being granted access to an application, protected data, or signing a transaction, instead of a hacker. This helps reduce fraud and protect valuable assets.

VASCO s primary product and service lines include three categories of solutions; Host System products, which is typically a component of an organization s IT infrastructure, Client Authenticators, which are devices used by end users for authentication, and Developer Tools, which are used by application developers to increase the security of their mobile applications.

Host System products:

VACMAN Controller: Core host system software authentication platform, combining all technologies on one unique platform;

IDENTIKEY Authentication Server: Software that adds full server functionality to the VACMAN core authentication platform;

Cloud Services: Authentication and digital signature software services for web and mobile application developers run on VASCO s servers. This includes our DIGIPASS as a Service solution for cloud-based authentication services primarily for enterprise customers and our MYDIGIPASS solution for end user authentication in the cloud

Client Authenticator Products:

DIGIPASS Hardware Authenticators: A broad family of multi-application hardware authenticators in a variety of form factors and feature sets to meet the diverse security needs of clients across multiple vertical markets. The hardware form factors include one-button, e-signature, card reader, PKI, and Bluetooth enabled devices.

DIGIPASS Software Authenticators: These are authenticators that run on existing non-VASCO devices, such as PCs, mobile phones, tablets, etc. Built around our cornerstone DIGIPASS API, software authenticators include DIGIPASS for Apps (a library of security APIs for mobile applications), DIGIPASS for Mobile (a security application for mobile devices), DIGIPASS for Web (for web browsers), DIGIPASS for Windows (desktop application) and Virtual DIGIPASS (Server-Side generated OTP).

Table of Contents

Developer Tools:

In addition to being a client authentication device when downloaded onto a mobile device, DIGIPASS for Apps is also a comprehensive software development kit (SDK) that allows software developers to quickly and easily integrate application security elements and other security features into mobile applications.

We offer our Host System products in one of two models, an on-premise model or an in-the-cloud services model:

1. Our on-premise model, which is our traditional approach to the market, allows a customer to license our host system software for installation on their on-premise systems in their applications. Similarly, our customers purchase or license hardware or software authenticators that are distributed to the users of their systems or applications. Our on-premise model is ideally suited to instances where the application owner needs to control all critical aspects of security, which is often the case where there is either a high transaction value or a high frequency of use. Under our traditional approach, the client devices can generally only be used with one host system application.

Banking

Enterprise VPN Access

Enterprise Single Sign-on

2. Our in-the-cloud services model includes two product offerings that use the same operational platform:

a) DIGIPASS as a Service (DPaaS) is our cloud-based service offering that was announced in October 2010 with a focus on the needs of customers in the Enterprise and Application Security market. By using our DPaaS authentication platform, business customers can deploy two-factor authentication more quickly and incur less upfront costs when compared to an on-premise solution. DPaaS is targeted towards B2B and B2E applications (e.g., employees of companies logging into third party applications operated in the cloud or accessing corporate data and resources stored in the cloud).

b) MYDIGIPASS (MDP) is our cloud-based service offering that was announced in April 2012 with a focus on the needs of B2B and B2C. MDP facilitates password management while adding an additional level of security to the login procedure. By using our MDP platform, consumers using B2C applications have convenient access to these applications with increased security. The MDP platform may also provide benefits for eGovernment and eID applications by providing authentication for citizens that are accessing government applications online.

MYDIGIPASS Security in the Cloud

Detailed Product Descriptions:

VACMAN Controller

The VACMAN product line incorporates a range of strong authentication utilities and solutions designed to allow organizations to add DIGIPASS strong authentication into their existing networks and applications.

In order to provide the greatest flexibility, without compromising functionality or security, VACMAN solutions are designed to integrate with most popular hardware and software. Once integrated, the VACMAN components become largely transparent to the users, minimizing rollout and support issues.

VACMAN is the backbone of VASCO s product strategy towards the banking and e-commerce markets. VACMAN encompasses all four authentication technologies (passwords, dynamic password technologies, certificates, and biometrics) and allows our customers to use any combination of those technologies simultaneously. VACMAN is natively embedded in or compatible with the solutions of over 100 VASCO solution partners.

Designed by specialists in system access security, VACMAN makes it easy to administer a high level of access control and allows our customers to match the level of authentication security used with their perceived risk for each user of their application. Our customer simply adds a field to his or her existing user database, describing the authentication technology used and, if applicable, the unique DIGIPASS assigned to the end user of their application. VACMAN takes it from there, automatically authenticating the logon request using the security sequence the user specifies, whether it s a one-time password using either response-only or a challenge/response authentication scheme or an electronic signature.

VACMAN allows the user the freedom to provide secure remote access to virtually any type of application. VACMAN is a library requiring only a few days to implement in most systems and supports all DIGIPASS functionality. Once linked to an application, VACMAN automatically handles login requests from any user authorized to have a DIGIPASS.

IDENTIKEY Authentication Server

IDENTIKEY Authentication Server is an off-the-shelf centralized authentication server that supports the deployment, use, and administration of DIGIPASS strong user authentication. IDENTIKEY is based on VASCO s core VACMAN technology.

IDENTIKEY Authentication Server is available in a Banking Edition and three versions for the Enterprise and Application Security market that can be easily upgraded.

The Banking Edition provides robust protection against man-in-the-middle (MITM) attacks, the highest security, and verified fit into existing PCI-DSS environments without reducing compliancy. This version includes:

- RADIUS functionality,
- Web filter support for access to in-house applications (OWA, RDWA, CWI, Receiver),
- Two-Factor Authentication for protection of access to internet banking applications,
- e-signature for validation of financial transactions, and
- Licenses for up to seven servers.

The three versions available to the Enterprise and Application Security market include:

The Standard Edition includes Remote Authentication Dial In User Service (RADIUS) functionality for a single licensed server. It targets small and medium-sized business (SMB) wanting to secure their remote access infrastructure at the lowest total cost of ownership.

The Gold Edition offers web filters to secure Outlook Web Access (OWA) and Citrix Web Interface (CWI), additional to the RADIUS support. This version includes licenses for a primary and a back-up server. It is an ideal solution for SMBs that want to offer more functionality and assure availability for their employees.

The Enterprise Edition is our most comprehensive solution, offering:

RADIUS for remote access to the corporate network,

Web filter support for access to in-house applications (OWA, CWI),

Simple Object Access Protocol (SOAP) for protection of internet based business applications (e.g. portals, extranet, e-commerce websites, partner services, etc.), and

Licenses for up to seven servers.

The Enterprise Edition is the optimum solution for SMBs that want to secure more than remote access by using the same DIGIPASS device to secure additional applications at little to no extra cost. It also addresses the need of large enterprises to set up a pool of replication servers to share the authentication load and assure high-availability, especially when securing an increased number of customers and partners who use web-hosted applications.

IDENTIKEY Appliance and IDENTIKEY Virtual Appliance

IDENTIKEY Appliance is a standalone authentication solution that offers strong two-factor authentication for remote access to a corporate network or to web-based in-house business applications. It comes in a standard 19 inch rack mountable slim fit design. The appliance verifies DIGIPASS/IDENTIKEY authentication requests from RADIUS clients and web filters and can easily be integrated with any infrastructure. It features a web based administration interface as well as an auditing and reporting console.

IDENTIKEY Virtual Appliance is a virtualized authentication appliance that secures remote access to corporate networks and web-based applications.

IDENTIKEY Federation Server

IDENTIKEY Federation Server is a server appliance that provides an identity and access management platform. It is used to validate user credentials across multiple applications and disparate networks. The solution validates users and creates an identity ticket enabling web single sign-on for different applications across organizational boundaries. IDENTIKEY Federation Server works as an Identity Provider within the local organization, but can also delegate authentication requests (for unknown users) to other Identity Providers. In a Federated Model, IDENTIKEY Federation Server not only delegates but also receives authentication requests from other Identity Providers, when local users want to access applications from other organizations within the same federated infrastructure.

Cloud Services (DPaaS and MDP)

In October of 2010, we launched our DIGIPASS as a Service security platform. Our initial DPaaS offering was directed at providing strong authentication for B2B and B2E applications. B2B applications are applications between two organizations that have an on-going relationship of some type. An example could be a manufacturer that has a web site through which a customer regularly purchases its products. VASCO s DPaaS platform could be used to strongly authenticate the purchaser to prevent fraudulent activities. B2E applications are applications which have been outsourced by an organization. These could be sales reporting and forecasting applications, payroll and 401(k) plan administration applications, human resource applications, etc. that are operated in the cloud.

We launched MYDIGIPASS (MDP) in April 2012. MDP is directed at the B2B and B2C market. Our goal is to have the user securely access multiple applications with only one DIGIPASS. We believe that with this approach, we can bring two-factor authentication to a large number of online applications.

The combination of our core business line and service offering brings a large number of online applications within VASCO s reach. While revenues generated from DPaaS and MDP to date have been minimal, we believe DPaaS/MDP has potential for future growth as it will make two-factor authentication more affordable and readily available to users and applications markets. We believe that this combination provides VASCO with a viable position in the market, giving us the opportunity to target web application owners and offer their end users convenience and security.

DIGIPASS Hardware Authenticators

We offer a wide variety of DIGIPASS authenticators, each of which has its own distinct characteristics to meet the needs of our customers. All models of the DIGIPASS family are designed to work together so that our customers can switch their users devices without requiring any changes to their existing infrastructure. Our hardware DIGIPASS models range from simple one-button devices to devices that include more secure technologies such as PKI.

With the acquisition of Cronto, VASCO has also added visual cryptography to its product portfolio. Sensitive transaction data are captured in a cryptogram that consists of a matrix of colored dots. By scanning the image with a hardware or software authenticator, the data contained in the cryptogram is decrypted and the transaction details are presented to the user for verification providing a highly secure method of visual transaction signing with maximum user convenience.

During 2014, we launched Bluetooth-enabled authentication and digital signature solutions that bring our high level of security to the increasing number of users of tablets and smart phones that have no USB port. VASCO s Bluetooth Smart devices create an immediate virtual secure connection between the authenticator and the mobile device using a Bluetooth Smart connection,

Many DIGIPASS authenticators also combine the benefits of traditional password authenticators (authentication and digital signatures) with smart card readers. Together, they bring portability to smart cards and allow the use of secure time-based algorithms.

DIGIPASS hardware technology is designed to support authentication and digital signatures for applications running on desktop PCs, laptops, tablets, and smart phones.

DIGIPASS Software Authenticators

Our DIGIPASS Software authenticators are designed to provide our customers with increased security for access to their networks and applications without having to carry a standalone hardware device.

Many of our DIGIPASS Software authenticator models also balance the need for stronger mobile application security with the demands for user convenience by delivering comprehensive, built-in security for mobile applications, combined with a frictionless, hands-free authentication and e-signing experience for mobile users.

DIGIPASS for Apps is a software development kit that contains a library APIs (application programming interface) that allows application developers to add important security features to their mobile applications such as secure storage, secure communication channel, secure provisioning, device binding capabilities, jailbreak detection, rootkit detection, geolocation, IP address detection, and other security features. DIGIPASS for Mobile offers a similar set of security features as a downloadable mobile application.

Table of Contents

Developer Tools:

In additional to serving as a software authenticator, DIGIPASS for Apps is a comprehensive software development kit (SDK) that allows application developers to natively integrate application security such as two-factor authentication and electronic signing into mobile applications. Through a complete library of APIs, application developers can extend and strengthen application security, deliver enhanced convenience to their application users, and streamline application deployment and lifecycle management processes.

Intellectual Property and Proprietary Rights and Licenses

We rely on a combination of patent, copyright, trademark and trade secret laws, as well as employee and third-party non-disclosure agreements to protect our proprietary rights. In particular, we hold several patents in the U.S. and in other countries, which cover multiple aspects of our technology. These patents expire between 2021 and 2033. In addition to the issued patents, we also have several patents pending in the U.S., Europe and other countries. The majority of our issued and pending patents cover our DIGIPASS family and other authentication related technology. We believe these patents to be valuable property rights and we rely on the strength of our patents and on trade secret law to protect our intellectual property rights. To the extent that we believe our patents are being infringed upon, we intend to assert vigorously our patent protection rights, including but not limited to, pursuing all available legal remedies.

Research and Development

Our research and development efforts historically have been, and will continue to be, concentrated on product enhancement, new technology development, and related new product introductions. We employ a team of full-time engineers and, from time to time, also engage independent engineering firms to conduct non-strategic research and development efforts on our behalf. For fiscal years ended December 31, 2014, 2013, and 2012, we incurred expenses of $19.5 million, $21.3 million, and $18.8 million, respectively, for research and development.

Production

Our security hardware DIGIPASS products are manufactured by third party manufacturers pursuant to purchase orders that we issue. Our hardware DIGIPASS products are made primarily from commercially available electronic components purchased globally. Our software products, including software versions of our DIGIPASS products are produced in-house.

Hardware DIGIPASS products utilize commercially available programmable microprocessors purchased from several suppliers. The microprocessors are the only components of our security authenticators that are not commodity items readily available on the open market. Some programmed microprocessors are single sourced. Orders of microprocessors generally require a lead-time of 12-16 weeks. We attempt to maintain a sufficient inventory of all parts to handle short-term increases in orders.

Large orders that would significantly deplete our inventory are typically required to be placed with more than 12 weeks of lead-time, allowing us to make appropriate arrangements with our suppliers. During 2013, we purchased a multi-year supply of certain microprocessors scheduled to be discontinued by a manufacturer. While we can re-engineer our products to use other processors when notified that a processor will no longer be produced, we believe that it is generally more cost effective to carry a multi-year supply than to re-engineer the product.

We purchase the microprocessors and arrange for shipment to third parties for assembly and testing in accordance with our design specifications. The majority of our DIGIPASS products are manufactured by four independent vendors domiciled in Hong Kong and Macau with production facilities in mainland China. Purchases from these companies are made on a volume purchase order basis. Equipment designed to test product at the point of assembly is supplied by us and periodic visits are made by our personnel for purposes of quality assurance, assembly process review and supplier relations.

Table of Contents

Competition

The market for computer and network security solutions is very competitive and, like most technology-driven markets, is subject to rapid change and constantly evolving products and services. Our main competitors are Gemalto and RSA Security, a subsidiary of EMC Corporation. There are many other companies, such as Kobil Systems, SafeNet (acquired by Gemalto in 2014), Symantec, and Entrust that offer competing authentication hardware, software and services that range from simple locking mechanisms to sophisticated encryption technologies. In addition to these companies, we face competition from many small authentication solution providers many of whom offer new technologies and niche solutions such as biometric or behavioral analysis. We believe that competition in this market is likely to intensify as a result of increasing demand for security products. Visibility of global competitors and their planned actions has diminished over the last several years as some of our competitors have been acquired by larger corporations (e.g., EMC s acquisition of RSA in 2006) or private equity firms (e.g., Entrust, acquired by Thoma Bravo in 2009 and subsequently sold to Datacard Group in 2013).

We believe that the principal competitive factors affecting the market for computer and network security products include the strength and effectiveness of the solution, technical features, ease of use, quality/reliability, customer service and support, name recognition, customer base, distribution channels, and the total cost of ownership of the authentication solution. Although we believe that our products currently compete favorably with respect to such factors, other than name recognition in certain markets, there can be no assurance that we can maintain our competitive position against current and potential competitors, especially those with significantly greater financial, marketing, service, support, technical, and other competitive resources.

Some of our present and potential competitors have significantly greater financial, technical, marketing, purchasing, and other resources than we do, and as a result, may be able to respond more quickly to new or emerging technologies and changes in customer requirements, or to devote greater resources to the development, promotion and sale of products, or to deliver competitive products at a lower end-user price. Current and potential competitors have established or may establish cooperative relationships among themselves or with third parties to increase the ability of their products to address the needs of our prospective customers. It is possible that new competitors or alliances may emerge and rapidly acquire significant market share. Accordingly, we have forged, and will continue to forge, our own partnerships to offer a broader range of products and capabilities to the market.

Our products are designed to allow authorized users access to a computing environment or application, in some cases using patented technology, as a replacement for or supplement to a static password. Although certain of our security token technologies are patented, there are other organizations that offer token-type password generators incorporating challenge-response or response-only approaches that employ different technological solutions and compete with us for market share.

Sales and Marketing

Our security solutions are sold worldwide through our direct sales force, as well as through distributors, resellers and systems integrators. Our traditional security solutions are sold through our direct sales force, as well as through approximately 52 distributors, their reseller networks and systems integrators. A sales staff of 102 coordinates our sales activity through both our sales channels and those of our strategic partners making direct sales calls either alone or with the sales personnel of our partners. Our sales staff also provides product education seminars to sales and technical personnel of vendors and distributors with whom we have working relationships and to potential end-users of our products.

VASCO secures and trains its channel. Over 1,200 staff members of our channel partners have become VASCO certified.

Our sales force is able to offer each customer a choice of an on-site implementation using our traditional on-premise model or a cloud implementation using our services platform.

Our DPaaS solution is sold primarily by our direct sales force calling on Enterprise and Application Security customers.

Our MDP solution is also sold primarily by our direct sales force and marketed to application owners. We will work with the application owners to develop marketing programs that will encourage users of the application to access that application through our services platform.

Part of our expanded selling effort includes approaching our existing strategic partners to find additional applications for our security products. In addition, our marketing plan calls for the identification of new business opportunities that may require enhanced security over the transmission of electronic data or transactions where we do not currently market our products. Our efforts also include various activities to increase market awareness of the MDP/DPaaS solutions as well as preparation and dissemination of white papers explaining how our security products can add value or otherwise be beneficial.

Customers and Markets

Customers for our products include some of the world s most recognized names: HSBC, Rabobank, Belfius, Sumitomo Mitsui Banking Corporation, BNP-Paribas Fortis, Swedbank, The Bank of Tokyo-Mitsubishi, Citibank, and Commonwealth Bank of Australia.

Our top 10 customers contributed 46%, 40%, and 37%, in 2014, 2013, and 2012, respectively, of total worldwide revenue. In 2014, 2013, and 2012, HSBC contributed approximately 11%, 18%, and 10%, of our worldwide revenue, respectively. In addition, in 2014, Rabobank contributed 12% of our worldwide revenue.

A significant portion of our sales is denominated in foreign currencies and changes in exchange rates impact results of operations. To mitigate exposure to risks associated with fluctuations in currency exchange rates, we attempt to denominate an amount of billings in a currency such that it would provide a hedge against operating expenses being incurred in that currency. For additional information regarding how currency fluctuations can affect our business, please refer to Management s Discussion and Analysis of Financial Condition and Results of Operations and Quantitative and Qualitative Disclosures about Market Risk.

We experience seasonality in our business. Historically, these seasonal trends are most notable in the summer months, particularly in Europe, when many businesses defer purchase decisions; however, given the relatively small size of our business, the timing of any one or more large orders may temper or offset this seasonality.

We organize our sales group and report our results in two vertical markets:

Banking, which includes Financial Institutions: Traditionally our largest market where we believe that there are substantial opportunities for future growth.

Enterprise and Application Security: A significant market that includes:

- Businesses seeking secure internal and remote network access: We sell to this market primarily through distributors and resellers. Our strategy is to leverage products developed for the Banking market by selling them to businesses. We believe that our strength in this segment is largely related to selling remote access products to both SME (small and medium enterprises) as well as large corporations.

- Other application-specific markets: Our products are being used in a significant number of applications and we believe that we will be able to identify and leverage our knowledge with those applications to increase our penetration in the more promising markets.

- E-commerce: Both business-to-business and business-to-consumer e-commerce are becoming ever more important for us.

- E-government: Our revenue in this market is still small, but we are ready to take advantage of the market s evolution.

Our channel partners are critical to our success in selling to businesses in the Enterprise and Application Security markets. We serve this market exclusively via our two-tier indirect sales channel. We invest in and support our channel with marketing and public relations actions. Distributors and resellers get the tools they need to be successful, such as campaigns, case studies, marketing funds and more. We train employees of our resellers and distributors on-site and in our offices. In addition, we have developed online video training software that allows us to train people worldwide, resulting in cost- and time-saving benefits.

We expect that sales into the application security market, other than businesses, will be on a direct sale basis. We plan to add sales and marketing staff to help increase revenues from each of these targeted areas.

Backlog

Our backlog at December 31, 2014 was approximately $113 million compared to $42 million at December 31, 2013. We anticipate that substantially all of the backlog at the end of 2014 will be shipped in 2015. We do not believe that the specific amount of backlog at any point in time is indicative of the trends in our markets or the expected results of our business. Given the relatively small size of our business and the large size of potential orders, the backlog number can change significantly with the receipt of a new order or modification of an existing order, for example, shipment timing.

Financial Information Relating to Foreign and Domestic Operations

For financial information regarding VASCO, see our Consolidated Financial Statements and the related Notes, which are included in this Annual Report on Form 10-K. We have a single reportable segment for all our products and operations. See Note 12 in the Notes to Consolidated Financial Statements for a breakdown of revenue and long-lived assets between U.S. and foreign operations.

Employees

As of December 31, 2014, we had 371 total employees, which included 350 full-time employees. Of the total employees, 38 were located in the U.S., 305 in EMEA (Europe, the Middle East and Africa), 19 in the Asia Pacific Rim countries and 9 in other countries, including Australia, Latin America, India and Central Asia. Of the total employees, 179 were involved in sales, marketing, operations and customer support, 136 in research and development and 56 in general and administration.

Item 1A - ***Risk Factors***

RISK FACTORS

You should carefully consider the following risk factors, which we consider the most significant, as well as other information contained in this Annual Report on Form 10-K. In addition, there are a number of less significant and other general risk factors that could affect our future results. If any of the events described in the risk factors were to occur, our business, financial condition or operating results could be materially and adversely affected. We have grouped our Risk Factors under captions that we believe describe various categories of potential risk. For the reader s convenience, we have not duplicated risk factors that could be considered to be included in more than one category.

Table of Contents

Risks Related to Our Business

A significant portion of our sales are to a limited number of customers. The loss of substantial sales to any one of them could have an adverse effect on revenues and profits.

We derive a substantial portion of our revenue from a limited number of customers, most of which are European or Asian headquartered banks. The loss of substantial sales to any one of them could adversely affect our operations and results. In fiscal 2014, 2013, and 2012, our top 10 largest customers contributed 46%, 40%, and 37%, respectively, of total worldwide revenue. In fiscal 2014, 2013, and 2012, HSBC contributed approximately 11%, 18%, and 10%, respectively, of total worldwide revenue. In addition, in 2014, Rabobank contributed 12% of total revenue principally due to an order for card readers incorporating our CrontoSign technology which began shipping in the third quarter of 2014 and scheduled to be completed by the third quarter of 2015.

HSBC has no long term contractual commitment to purchase products or services from us. HSBC and its affiliates only make purchase commitments pursuant to individual purchase orders placed with us from time to time, which are subject to our acceptance. The general commercial framework that applies to such purchases by HSBC may be terminated by HSBC at any time, without cause, on 90 days notice to us without payment of any termination charge by HSBC.

The return of a worldwide recession and/or an increase in the concern over the European sovereign debt crisis may further impact our business.

Our business is subject to economic conditions that may fluctuate in the major markets in which we operate. Factors that could cause economic conditions to fluctuate include, without limitation, recession, inflation, deflation, higher interest borrowing rates, higher levels of unemployment, higher consumer debt levels, general weakness in retail or commercial markets and changes in consumer or business purchasing power or preferences.

While it appears that circumstances that led to the sovereign debt crisis have abated, many significant economic issues have not been addressed fully. As a result, we expect that Europe will continue to face difficult economic conditions in 2015. If global economic and financial market conditions remain uncertain and/or weak for an extended period of time, any of the following factors, among others, could have a material adverse effect on our financial condition and results of operations:

slower consumer or business spending may result in reduced demand for our products, reduced orders from customers for our products, order cancellations, lower revenues, increased inventories, and lower gross margins;

continued volatility in the global markets and fluctuations in exchange rates for foreign currencies and contracts or purchase orders in foreign currencies could negatively impact our reported financial results and condition;