

E-SMART TECHNOLOGIES INC

Form 10KSB/A

March 20, 2008

[Table of Contents](#)

SECURITIES AND EXCHANGE COMMISSION

Washington, D.C. 20549

FORM 10-KSB/A

ANNUAL REPORT UNDER SECTION 13 OR 15(d)

OF THE SECURITIES EXCHANGE ACT 1934:

For the Fiscal Year Ended December 31, 2005

Commission File Number: 0-30717

E-SMART TECHNOLOGIES, INC.

(Name of Small Business Issuer in its Charter)

Nevada
(State of Incorporation)

526 West 26th Street, Suite 710, New York, NY 10001

(Address of Principal Executive Office, including Zip Code)

88-0409261
(I.R.S. Employer Identification No.)

Edgar Filing: E-SMART TECHNOLOGIES INC - Form 10KSB/A

(212) 727-3790

(Issuer's Telephone Number)

Securities registered under Section 12(g) of the Exchange Act:

COMMON STOCK, \$.001 PAR VALUE

(Title of Class)

Check whether Issuer: (1) filed all reports required to be filed by Section 13 or 15 (d) of the Securities Exchange Act during the past 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 ☒ No ☐

Check if there is no disclosure of delinquent filers in response to Item 405 of Regulation S-B is not contained in this form, and no disclosure will 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-KSB or any amendment to this Form 10-KSB. ☐

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

Issuer's revenues for the two years ended December 31, 2005: \$ **-0-**

The aggregate market value of Common Stock held by non-affiliates at March 31, 2006 was **\$7,650,000**.

Shares of Common Stock, \$.001 par value per share, outstanding at March 31, 2006: **200,000,000 shares**. The total number of authorized and issued shares will increase, pursuant to the current Plan of Reorganization, to 400,000,000.

DOCUMENTS INCORPORATED BY REFERENCE:

No documents are incorporated by reference into this Annual Report.

Transitional Small Business Disclosure Format (check one): Yes ☐ No ☒

Table of Contents

Table of Contents

PART I

ITEM 1.	<u>Description of Business</u>	1
ITEM 2.	<u>Description of Property</u>	26
ITEM 3.	<u>Legal Proceedings</u>	27
ITEM 4.	<u>Submission of Matters to a Vote of Security Holders</u>	27

PART II

ITEM 5.	<u>Market for the Registrant's Common Equity, Related Stockholder Matters and Small Business Issuer Purchases of Equity Securities</u>	27
ITEM 6.	<u>Management's Discussion and Analysis or Plan of Operations</u>	29
ITEM 7.	<u>Financial Statements</u>	31
ITEM 8.	<u>Changes in and Disagreements with Accountants on Accounting and Financial Disclosure</u>	47
ITEM 8-A.	<u>Controls and Procedures</u>	48

PART III

ITEM 9.	<u>Directors, Executive Officers, Promoters and Control Persons; Compliance With Section 16(a) of the Exchange Act</u>	49
ITEM 10.	<u>Executive Compensation</u>	55
ITEM 11.	<u>Security Ownership of Certain Beneficial Owners and Management and Related Stockholder Matters</u>	58
ITEM 12.	<u>Certain Relationships and Related Transactions</u>	61
ITEM 13.	<u>Exhibits and Reports on Form 8K</u>	63
ITEM 14.	<u>Principal Accountant Fees and Services</u>	65
	<u>SIGNATURES</u>	66
	CERTIFICATIONS	

Table of Contents

Safe Harbor Statement

Certain statements contained herein constitute forward-looking statements within the meaning of the Private Securities Litigation Reform Act of 1995. We desire to avail ourselves of certain safe harbor provisions of the 1995 Reform Act and are therefore including this special note to enable us to do so. Forward-looking statements included in this Report on Form 10-KSB involve known and unknown risks, uncertainties, and other factors which could cause our actual results, performance (financial or operating) or achievements to differ from our best estimate of future results, performance (financial or operating) or achievements expressed or implied by such forward-looking statements. These risks include, but are not limited to, risks related to recently consummated acquisitions as well as future acquisitions, our ability to increase our revenues and generate income from operations, effects of competition and technological changes, risks related to exposure to personal injury and workers compensation claims, risks that our insurers may not provide adequate coverage, risks associated with compliance with government regulations such as ERISA, state and local employment regulations and dependence upon key personnel.

We believe it is important to communicate our expectations to our investors. There may be events in the future, however, that we are not able to accurately predict or over which we have no control. The risk factors listed below, as well as any cautionary language in this report, provide examples of risks, uncertainties and events that may cause our actual results to differ materially from the expectations we described in our forward-looking statements. Before any investment is made in our securities, awareness that the occurrence of any of the events described in the risk factor section and elsewhere in this report, and other events that we have not predicted or assessed could have a material adverse effect on our ability to transition out of the development stage. In such case, the price of our securities could decline and any investor may lose all or part of the investor's investment.

PART I

ITEM 1. DESCRIPTION OF BUSINESS

General

e-Smart Technologies, Inc., a Nevada corporation (the Company or the Registrant), was incorporated on July 15, 1997, under the name Boppers Holdings, Inc. (Boppers). On October 20, 2000, Boppers, Boppers Acquisition Corp., a then newly-formed Nevada corporation and wholly owned subsidiary of Boppers (BAC), and e-Smart Systems, Inc., a Nevada corporation (e-Smart Systems) and wholly owned subsidiary of Intermarket Ventures, Inc., a Utah corporation (IVI), entered into an Agreement and Plan of Merger (the Merger Agreement). Prior to the consummation of the transactions contemplated by the Merger Agreement, Boppers had 200,000,000 authorized shares of Common Stock, par value \$.001 per share (the Boppers Common Stock), 20,000,000 authorized shares of Preferred Stock, par value \$.001 per share and 3,501,000 issued and outstanding shares of Boppers.

Table of Contents

Common Stock. Pursuant to the Merger Agreement, Boppers: (i) issued 58,600,000 shares of Boppers Common Stock to IVI in exchange for 58,600,000 shares of e-Smart System's common stock, par value \$.001 per share, owned of record by IVI; and (ii) converted warrants to purchase an aggregate of 2,900,000 shares of e-Smart System's common stock at \$10.00 per share into warrants to purchase an aggregate of 2,900,000 shares Boppers' Common Stock at \$10.00 per share (the "Warrants"). The foregoing caused a change in the control of Boppers.

Pursuant to the terms of the Merger Agreement: Registrant's present management assumed control of the Company and its name was changed from Boppers Holdings, Inc. to e-Smart Technologies, Inc., effective as of December 22, 2000.

We have limited operations, and, in accordance with SFAS#7, we are considered a development stage company. We have an administrative office located at 526 West 26th Street, Suite 710, New York, NY 10001. Our registered agent in the State of Nevada is The Corporation Service Company and our transfer agent is Holladay Stock Transfer Company of Scottsdale, Arizona. Our common stock trades in the over-the-counter market under the symbol ESMT. Our telephone number is (212) 727-3790.

Pursuant to subsequent grants of rights from IVI Smart (defined hereinafter), we directly own the exclusive license for certain technologies for the U.S.A. and Asia except China. In addition, and through our wholly owned subsidiary e-Smart Systems, Inc., a Nevada corporation, we own the exclusive license for China to the smart card technology and any and all other smart card related assets originally developed or otherwise owned by IVI, one of our major shareholders, and now owned by IVI Smart Technologies, Inc., a Delaware corporation and subsidiary of IVI ("IVI Smart"). This technology is, we believe, the most advanced biometrically protected, multi-application smart card solution, the "Super Smart Card System." We have sublicensed the rights to market the technology to state and federal agencies to our forty-five (45%) percent owned affiliate, Homeland Defense, Inc., a Nevada corporation, which is majority owned (fifty-five (55%) percent) by our Chairman, Chief Executive Officer, President and Chief Financial Officer Mary Grace.

Recent Developments

Letter of Intent and Agreement with MYBi, Inc.

On, July 25, 2005, and as enumerated in Item 5 of our Form 10-QSB Quarterly Report filed on August 15, 2005, e-Smart Korea has been offered a ten year Strategic Alliance Agreement with MYBi. The Agreement contemplates joint activities designed to facilitate the rapid deployment, adoption, and use of a combined IC Card based payment system that incorporates both MYBi's automated fare collection and micro-payment systems and e-Smart's macro-payment systems, all on e-Smart's Super Smart Card. The Agreement also contemplates the joint promotion of our combined systems globally and the creation of a global payment network and processing system to facilitate the growth of Super Smart Card worldwide. The Company is actively seeking to raise the capital necessary to meet the closing conditions of the proposed MYBi arrangement.

Table of Contents

The Agreement requires us: (i) to distribute a designated number of terminals, in stages, throughout South Korea and to provide Super Smart Cards necessary to meet consumer demand but subject to defined limits with overages at our discretion; (ii) to either purchase or cause an affiliate of e-Smart to purchase approximately 15% of MYBI's current issued and outstanding shares at a negotiated price from certain existing shareholders; (iii) to cause the same affiliate of e-Smart to purchase a senior convertible debenture and warrant from MYBI (collectively the "Debt Instruments") with a conversion price on the debenture shares alone that allows the buyer to purchase a minimum of 10.1 percent of a new issuance of MYBI shares (on a fully diluted basis at a designated price); and (iv) to create, operate, and service an Operations Center in Korea necessary to process the Super Smart Cards and any other type of non-cash payments other than Automated Fare Collections and other traditional MYBI e-purse transactions. Upon completion of the MYBI share purchase and debenture transactions as mentioned above, e-Smart's affiliate will obtain the following from MYBI: (i) at least one permanent seat on MYBI's Board of Directors as well as one seat on MYBI's financial control board; and (ii) specified veto rights with respect to major decisions and with respect to any spending outside the usual course of MYBI's business; and (iii) customary assurances with respect to continuation of management and business plans as well as other customary covenants and negative covenants. In addition, MYBI is required to hire a manager designated by us as a full time management employee for harmonious coordination of our joint project.

The Agreement requires MYBI to: (i) utilize the funds received as a result of our purchase of the Debenture to upgrade its existing system and as additional working capital; (ii) jointly with us use commercially reasonable efforts to cause and assist mutually-agreed upon financial institutions to issue Super Smart Cards using our BIIN and our payment processing system in Korea; (iii) use commercially reasonable efforts to provide assistance to our sales force and marketing team and non-technical servicing team in Korea to fulfill designated performance metrics; (iv) use commercially reasonable efforts to refrain from issuing any MYBI accessory cards in real-name card issuance situations (*i.e.*, where payment cards are required to be issued on a real-name basis) such as schools, private educational institutes, corporations, banks, stock markets, insurances, and credit cards, etc; (v) process automated fare collection and other prepaid micro-payments in Korea in a manner consistent with its service level prior to the effective date of the Agreement; and (vi) use commercially reasonable efforts to assist us in securing and maintaining any and all registrations, permits, licenses, approvals, certificates and other governmental actions required to be secured and maintained by us for the activities contemplated by the Agreement. Any such registration, permit, license, approval, certificate or other action will be secured and maintained solely in the name of e-Smart Korea.

In consideration for a designated nominal annual royalty and a royalty based upon generated profits in any such territory, and subject to a prohibition against our decompiling, disassembling, or reverse engineering the licensed technology; the Agreement grants us an exclusive, non-transferable license to use MYBI's proprietary know-how and systems anywhere in the world except Korea (which is granted separately in the Agreement as described above). In addition to the standard representations and warranties, the Agreement provides for mutual non-competition and confidentiality protection.

Table of Contents

The Plan of Reorganization and Recapitalization.

In October 2005, our Board of Directors adopted resolutions ratifying and approving a plan of reorganization and recapitalization (the "Plan"), which plan is intended to enable us to:

Achieve a listing on a national securities exchange;

Transition into the commercialization of our Super Smart Card and Biometric Verification Security System (BVS2) and other technologies;

Enhance our position with our strategic partners;

Position us to more effectively enter the long term capital markets as a means of delivering our growing backlog of contracts for the use of our technologies;

Enable us to respond more effectively to any takeover efforts; and

Maximize shareholder values.

The Plan provided inter alia for a one-for-thirty reverse split of all issued and outstanding (but not authorized) shares of common stock and options; and the exchange of all management, founders and principal stockholder's common stock and options for 5,000,000 shares of Series A Preferred Stock, \$.01 par value per share (the "Preferred Stock") which would vest our management and principal stockholder with ongoing 70% voting control of our company.

In consideration of each of their pro-rata share of the 5,000,000 shares of Preferred Stock, each of our founders agreed to:

Surrender all options and all post reverse split shares held by them to our treasury;

Enter into a five-year written employment agreement with us containing confidentiality and non-compete provisions and agreeing to take all steps necessary to effect licensing to us of all intellectual property which is developed during and within the scope of this employment;

Relinquish conversion and dividend rights per the terms of the Preferred Stock;
Similarly, in consideration for our pro-rata share of the 5,000,000 shares of Preferred Stock IVI Smart Technologies, Inc., agreed to;

Surrender all post reverse split shares held by it to our treasury;

Table of Contents

Forgive our indebtedness of \$2,724,722 together with the interest thereon and waive the return of fifty million common shares also owed to it by us; and

Relinquish conversion and dividend rights per the terms of the Preferred Stock.

On October 14, 2005, the Plan was approved by the written consent of stockholders owning a majority of the 200,000,000 common shares that were outstanding on that date. The stated reasons for the action were to enhance our capital structure, our access to capital markets, our ability to respond to any acquisition efforts and to enhance shareholder value.

Given the nature of the actions taken by the Board, the approval by the Board and the majority of shareholders, and the absence of appraisal rights under Nevada law, no Information Statement was disseminated.

Our Board of Directors authorized management to take all steps necessary to effect the Plan. However, and principally as a result of a capital liquidity opportunity that presented itself, the Plan was not implemented during the fiscal year covered by this report.

Dependent upon the terms and circumstances of the capital liquidity opportunity, the Plan may be implemented in accordance with the approvals received from the Board and Stockholders, to effectuate its terms and stated purposes, but without a reverse split or issuance of Preferred Shares. Accordingly, and in exchange for and in consideration of the terms and conditions set forth above, the principal stockholder and founders will receive, if implemented the equivalent of 5,000,000 shares of post reverse Preferred Shares, i.e., 200,000,000 shares of Common Stock. The principal stockholder and founders have agreed to adhere to and comply with the terms and conditions as set forth above including forgiveness of the Company's indebtedness of \$2,724,722. To the extent that there are material changes in the terms and conditions of the capital liquidity opportunity, the effectuation of the Plan of Reorganization may be altered accordingly.

Products

The Company, IVI Smart and our subsidiaries and affiliates are all principally engaged in the business of creating, marketing, manufacturing, installing, operating and maintaining proprietary systems that are designed to positively authenticate each and every end user of any networked or local access system while protecting all information residing on or transported by the system. These products are designed to provide assurance that the user is the person that he or she claims to be and has the credential to access the premises or information being sought.

We intend to earn income primarily from transaction fees and/or other service based fees connected to the use of our systems once installed. We do not intend to either manufacture or install systems on our own; rather, we intend to outsource manufacturing of our Super Smart Card, Super Smart Readers and proprietary components under OEM agreements; and to outsource installation to

Table of Contents

select partners that are major systems integrators in each country of installation. Prior to the sale of a system, our business activities are strictly limited to marketing, research and development, and customer customization. After a sale is made, we will supervise the manufacture and installation of the system and, once deployed, operate the system on behalf of the purchaser. By outsourcing all other activities, we hope to keep our cost of operations down and minimize the complexity of our business.

One of the key distinctions of our system from all other systems is our proprietary smart card, the Super Smart Card. We believe that we are the world's first and currently still the only provider of a commercially available dual ISO 7816 (contact) and ISO 14443 B (wireless) compatible smart card featuring a fingerprint sensor onboard, a biometric matching engine onboard and a multi-application microprocessor. To our knowledge, as of the date hereof, the Super Smart Card is the only dual-interface biometrically activated, microprocessor-based smart card product available for deployment today. Because our Super Smart Card contains a microprocessor, it can process information and run multiple applications. Because our Super Smart Cards have an on-board digital fingerprint sensor, hold a biometric fingerprint template, and have an onboard biometric matching engine, our Super Smart Cards are able to perform an ID verification without reference to any network (or any other) database. For this reason, we call the Super Smart Card biometrically activated or biometrically powered. Our cards are referred to as dual interface because they work either in conjunction with a reader that requires physical contact with the card to supply power and to transfer data or with a reader that does not require physical contact with a card reader, as power and data are transferred to each card through an electro-magnetic field generated by such a card reader. Our Super Smart Card combines the benefits of microprocessors, biometrics and dual interface cards in an ISO compatible system and form-factor.

All of our products are designed to operate on a common platform which we currently refer to as the Biometric Verification Security System or the BVS2 (the current and improved version of the Super Smart Card System). The BVS2 Platform is based on our licensor's pending patents and other proprietary technologies and consists of our Super Smart Card (our unique smart card with an on-board biometric multi-application micro-processor, a unique on-board biometric sensor (fingerprint) and a unique digital photo ID system among other items), readers, operational software, application development software and a communication technology that ensures that the transmission of data to and from the Super Smart Card and throughout the system is secure and reliable.

The BVS2 can be customized to support a large number of applications in a multitude of markets. Some of the markets for which we have customized solutions for the BVS2 platform include national security, immigration/border crossing, ID-fraud free credit/debit card pre-processing, welfare/food-stamp benefits and medical services. We believe that there is no existing practical limit to the number or types of applications we can customize our system to run.

Table of Contents

Our products offer the following benefits:

The information stored on our card and transferred between the card and the reader is secured behind biometric activation and is protected by both physical and software encryption down to the physical layer (our PrestoChango protection system);

The biometric system being completely on the card with full independent operation capabilities allows for identity and credential verification even during emergency situations where denial of service attacks or other network outages prevent network database access and would cause many other systems to fail;

Our Super Smart Cards support multiple, independent applications secured even from each other on the same card, each protected by the biometric and each protected end-to-end throughout the system by our proprietary information protection system, PrestoChango ;

The system operator of the BVS2 platform (whether we or anyone else) has no access to user or customer information unless granted access by the application owner for some specific reason; and

Our cards are durable and easy to use, our technology can be placed in objects that take a variety of forms, such as key chains, wristwatches and necklaces/pendants among others.

The e-Smart Solution

We believe that our Super Smart Card has a technological advantage over any other existing smart cards in the market. The Super Smart Card is a dual interface card capable of working with existing contact and existing wireless type B readers. The Super Smart Card is a complete biometric system with its own sensor and matching system onboard every card. We believe that the Super Smart Card is an advanced microprocessor type smart card protected by a hardware based firewall enhanced by software that protects data down to the physical layer. We also believe that our Super Smart Card is rendered useless if tampered with and that counterfeiting is not possible. In short, we believe that at this time the Super Smart Card is a one-of-a-kind piece of technology that gives us a competitive advantage over all other suppliers and that makes us a sole source supplier to anyone that needs a reliable, stand-alone, privacy protected, biometrically empowered system of identity verification for public security or private commercial use.

Our technology not only enables a microprocessor-based smart card system to operate in both a contact and a contactless environment, but also enables our biometric fingerprint sensor and biometric engine to work in both a contact and a contactless environment as well. We believe that this ability to operate the biometric system both with a contact reader and wirelessly without any battery is another of the abilities unique to our Super Smart Card . As the Super Smart Card is an ISO compatible smart card, our technology is not only available for new systems, but can be integrated with existing contact and contactless (wireless) systems.

Table of Contents

The Biometric Verification Security System (BVS2)

The BVS2 is an integrated platform designed from the ground up to provide a security blanket of networked services necessary to protect everything from a single system to a nation-wide system. We believe that the BVS2 is a complete platform that can accommodate virtually any existing peripheral deemed appropriate for whatever task is required. We also believe that the BVS2's architecture is totally modular and upgradeable, almost infinitely scalable, fault tolerant, redundant and highly trustworthy. Authorized access both physical and logical is provided via the BVS2's secure, standardized and irrefutable biometric credential as generated by the Super Smart Card (as described below).

All BVS2 transactions (financial, data or otherwise) are routed through, logged, indexed and sorted by the BVS2's Universal Gateway subsystem. This subsystem is empowered by a secure group of networked servers that can access an almost unlimited number of diverse and legacy database systems and protocols via the Universal Gateway's exceptional data translation system, the Automated Protocol Manager (APM). If the BVS2 is tasked to make an inquiry of the normally incompatible database systems of multiple domestic and foreign agencies; the BVS2 can complete the inquiry quickly and efficiently, without human intervention, automatically combining normally irreconcilable data into one single language report. The BVS2's instant data-field manager allows any authorized user to instantly change information requests. With the addition of an optional analysis module, the BVS2's proprietary algorithms can analyze data customized to user requirements. In short, the BVS2 is an easy to use, yet extremely powerful system built to provide security to entire nations. At the same time, and without unnecessarily hampering the work and needs of government officials, we believe that the BVS2 offers the maximum in privacy protection to individuals. Some Key Components and Subsystems Comprising the BVS2 are described below.

The Super Smart Card

The Super Smart Card is the tool required to unlock a BVS2 Transaction. The Super Smart Card is a unique interoperable smart card featuring a non-JAVA based, multi application micro-processor that can perform multiple independent and discrete functions all protected behind hardware firewalls enhanced by software within the chip (the Presto Chango system). In addition, each Super Smart Card contains our own unique fingerprint sensor and biometric processing engine. No biometric data ever leaves the card in the privacy protected version of the Super Smart Card. Biometric data resides only on the Super Smart Card. All biometric processing is done on the card. Only the finger of the owner of each Super Smart Card placed on their own Super Smart Card's fingerprint sensor will activate the card, thereby insuring the personal privacy of each holder. We believe that Identity theft is theoretically made impossible. Lost or stolen cards have no value to anyone. The Super Smart Card, which we believe, but there can yet be no assurance that it will prove to be both tamperproof and counterfeit-proof, supports multiple discrete applications including, among others: ID Card, Debit/Credit Card, Driver's License and Physical and/or Logical Access Card.

Table of Contents

The standard Super Smart Card features an ISO contact operation interface (ISO 7816) and an ISO wireless operation interface (ISO 14443 B) and will operate on most ISO compatible contact 7816 readers or wireless 14443 B readers. The Super Smart Card is an integral part of the BVS2 . Every Super Smart Card contains an on-card biometric fingerprint sensor and digital 3-D photo ID system. Any other biometric can be added to the card and to the system. The Super Smart Card is inherently secure due to our hardware-based architecture. Each application on a Super Smart Card is secured from access by any unauthorized party by virtue of our on-chip hardware firewall system and our high-level encryption system, Presto-Chango . Other card systems, such as those now used for the DOD CAC cards, rely on and run software, primarily JAVA based, to create pseudo multi-applications all with the inherent security problems of JAVA.

The following is a summary of certain of the salient features of the Super Smart Card :

Unique Sensor On-Card. Only the fingerprint of the registered user can activate the card. The sensor performs with equal reliability with wet, dry, hot or cold fingers. The system prevents unauthorized use of any card or card application by requiring the authorized cardholder's fingerprint to activate the micro-processor inside and to initiate any transaction or to access any information (see below for more information about our fingerprint sensor);

Fraud-proof, counterfeit-proof and hack-proof. We believe that the physical characteristics of each Super Smart Card causes tampering to permanently disable it and destroy any information contained therein. We also believe based on technical innovations contained within each Super Smart Card that counterfeit cards will not work on the system thereby rendering any fake cards absolutely useless for all protected purposes but there can be no absolute assurance that this is the case;

Hardware Based, Software Enhanced, Multi-Application System. One card can contain multiple and independent and secure applications. For example, the technology will permit/deny access (physical and/or logical), identify precise location and/or movement of personnel and/or watch list parties while at the same time operating other secure applications, each completely and securely isolated one from the other;

Immediate identification Assurance & Privacy Protection. The system provides immediate and we believe sure authentication for all users and their credentials once they are properly enrolled onto the system. All biometric details are stored only on the Super Smart Card and not in any database (except where required by law, e.g., for INS needs or as required by certain voluntary programs) and the user leaves his or her fingerprint only on his or her own card which never leaves their hand;

Table of Contents

Stolen fingerprints of no use. Unlike other systems where a stolen fingerprint can mean a stolen identity, use of biometric information alone without one's own Super Smart Card is of no use with the BVS2. Each person's biometric information is inextricably entwined with certain other information unique to that user. Unless the biometric presented contains the additional unique information just mentioned (i.e., one's own Super Smart Card), not even the true owner of the biometric information will be granted access without the intervention of at least one, if not two high level, human, operations supervisors /officers' intervention, to establish the identity of the person concerned; and

One Card System Multiple Government Applications Total Security Saves Taxpayer Money. The Super Smart Card allows multiple secure applications to co-exist and operate on the same card. Because of the versatility of the BVS2 and Super Smart Card, one card and one system can be used by every federal agency, as an example, saving each agency the cost of having a multitude of systems and infrastructure to support each. In addition, because of the many services that the Super Smart Card can securely perform, there are many opportunities to defray costs by using one multi-purpose card and one multi-purpose network system and charging separate application fees for each application. In addition, we believe that since there is broad compatibility with many of the readers already in use, our system will, upon installation, save time and money for certain uses.

More information Regarding Our Fingerprint Sensor. A key component of each Super Smart Card is the Fingerprint Sensor. Each Super Smart Card contains one of these tiny (.33 mm thin), low power consumption sensors that is durable enough to be embedded in a smart card and yet not effected by static electricity, the elements or the condition (wet, dry, hot, cold) of the user's skin. Imaging is in 3D and based on micro-pressure variations across the sensor surface caused by the ridges and valleys existing in one's fingerprint. Users of the Super Smart Card with our built in sensor do not have to be concerned about leaving their fingerprint(s) on some reader that is fixed on a wall or sitting on a desk for someone to steal. The cardholder is always in control of his or her own fingerprint(s). The biometric fingerprint sensor incorporated in today's Super Smart Card was developed by BioSensor LLC, a Hawaiian limited liability company (BioSensor) and wholly owned subsidiary of IVI Smart, utilizing base intellectual property developed by IVI Smart but productized by BioSensor. This technology involves the modification and enhancement of certain third party sensors so that they can meet the requirements of a Super Smart Card. The cost of using such sensors is high and therefore the use of same is just an intermediate step in our production.

The Company intends to utilize what we call the BioSensor Fingerprint Sensor, as soon as practicable in its production of Super Smart Cards. When production ready, the BioSensor Fingerprint Sensor will be a fraction of the cost of the sensors currently in use while exhibiting at least the same or better recognition characteristics and physical tolerance than the sensors we use today.

Table of Contents

Use of the sensor is made possible pursuant to a Confidential Technology Assignment and License Agreement dated as of May 1, 2003, with IVI Smart, a principal stockholder of our Company (the "License Agreement"). Pursuant to the License Agreement, IVI Smart granted to BioSensor the exclusive right to develop certain of our intellectual property at BioSensor's sole cost and expense with respect to certain biometric fingerprint sensor technology created by IVI Smart, and BioSensor granted to IVI Smart the exclusive rights to any sensor developed by BioSensor. In consideration for the use of IVI Smart's intellectual property, BioSensor issued 50,000,000 of its Common Units to IVI Smart. No other Common Units were issued by Biosensor. Accordingly, Biosensor became a wholly owned subsidiary of IVI Smart and an affiliate of the Registrant. In consideration for the exclusive rights to use the sensor technology developed by BioSensor, IVI Smart agrees to pay a one-time royalty to BioSensor equal to \$.35 for each Super Smart Card sold or distributed by IVI Smart or any affiliate or licensee.

The Zero/Zero System. Our Zero False Acceptance Zero False Reject system is believed by us to be unique in the field of biometrics. In the normal course, when setting a biometric system, the closer to theoretical zero false acceptances you set your matching system for, the further you get from zero false rejections. In fact, a false rejection rate in the 30% to 40% range is not unheard of when many systems are set to the theoretical zero false acceptance rate. A false acceptance means the system confirms that you are someone else. A false rejection means the system will not confirm that you are who you really are. Based on our internal studies, our Zero/Zero System, using a patent pending technique that combines human factors with mechanical factors, is able to reduce the false reject rate to something less than 0.5% on the first use and to something less than 0.2% after the third to fifth use of the system by each new user. This reduction in the false rejection rate is extremely significant when dealing with high volumes of people in situations such as border crossings and airports. Each false rejection means that valuable time and manpower must be used to conduct a secondary inspection to check someone who is already cleared and increases the risk that an unauthorized individual will get through in the confusion. The Zero/Zero System is built in to of our Super Smart Cards.

Card Readers

The card reader is the tool that supplies power to our Super Smart Cards and the instrument through which each card communicates with the BVS2 platform. We intend to offer a full complement of readers as part of our proposed BVS2 system offering. For clients that need readers, we intend to offer a family of multi-system readers ready to meet almost any need that the market may have. These include a handheld wireless internet appliance and card reader to a dedicated stand alone desktop reader to interface modules that allow the use of most standard, off the shelf PDA's, sub-notebooks and other similar devices. We intend to offer a browser-phone with a contact card reader already incorporated. Our latest reader is a mobile GPRS based internet appliance with constant wireless access to the commercial mobile internet. This reader features a large, full color LCD display, a keyboard and a printer all in a handheld battery operated unit. We believe that there will be a large demand for this reader. All of our readers will be

Table of Contents

manufactured under contract with established card reader manufacturers based on customer orders as received. We intend to distribute these readers on a fully burdened cost basis making little or no profit and generally retaining ownership and maintenance responsibilities. (For the avoidance of confusion, maintenance responsibilities are outsourced to our strategic partners.)

The Universal Gateway with Legacy Preserver Technology

The BVS2 features a special gateway that is designed to take in all types of information from multiple sources and applications, forward it to its correct destinations, and translate the Babel-Speak of over one hundred (100) different legacy systems and technical services (this prevents the need to replace entire systems in use). When any such legacy system is attached to a BVS2 empowered network using our Legacy Preserver hardware, virtually all information passing through the network enters the Universal Gateway and by default is translated by the Universal Gateway's Automated Protocol Manager into a common language such that the information becomes available for use on all connected systems. Translation is in near real-time with the speed of any particular data's delivery basically controlled by the transmission speed of the legacy system that such data resides on. The Universal Gateway is a distributed system with redundant back up at all points. We believe that in the unlikely event that any node went down including the redundant node, such failure would not shut down the entire system.

Presto-Chango

Presto-Chango is designed to protect computer information down to the physical layer from unauthorized access. We believe that any attempt to move information from our storage place without proper authority causes that iteration of the information to morph into gibberish that cannot be deciphered by anyone or any system. Authorized access allows information to move, encrypted for transport, for any authorized and proper use which can be specified by user. Coupled with the BVS2's operating software, Presto-Chango is designed to enable sensitive information to transit the Internet or any public network without risk of information theft. Working together with the Super Smart Card, we believe that our system can provide superior logical protection where truly secure computer access and records are an absolute requirement.

Our Strategy

Our goal is to create a global network featuring the BVS2 platform that allows the full potential of each Super Smart Card to be used anywhere in the world and the maximum potential transaction fees for us. Key elements of our strategy include:

Enhance Technological Position. We intend to continue to invest in research and development in order to enhance our technological position, develop new technologies, extend the functionality of our products and services, and offer innovative products to our customers. For example, at the request of a potential government client, we have just completed the development of a fully wireless biometric passport that can match fingerprints on a stand alone basis or match faces when coupled with our digital video reader or both. We intend to continue with this type of research and development that can lead to immediate potential sales.

Table of Contents

Expand Domestic Market Presence. We are directly and through our Homeland Defense, Inc., affiliate actively engaged in marketing efforts to various agencies of the U.S. federal government. In particular, we have targeted various agencies within the Department of Homeland Security, including but not limited to the Bureau of Immigration and Customs Enforcement and the Transportation Security Administration. We intend to step up our marketing efforts to these and other agencies both on a direct basis and on a partnering basis with major U.S. domestic systems integrators in line with these agencies' current policy of awarding virtually all major contracts to a handful of well known integrators such as Accenture, EDS, SAIC and Titan.

Expand Global Market Presence. Currently, we market our products in Asia from our marketing subsidiary in Seoul, Korea and through strategic partnering agreements with two global IT companies and a Chinese state-owned company for domestic sales in the People's Republic of China. We intend to use these entities to strengthen our presence in existing markets, penetrate new markets, provide local customer service and technical support, and adapt our products to our local customers' specific needs.

Generate Recurring Revenues. We rejected a business model that called for one-time payments for our products and technologies. Other companies that have followed the one-time payment model in the smart card business, such as Gemplus and Oberthur, have not fared well financially during the low end of business cycles. Instead, our business plan is to sell entire systems, including our Super Smart Cards, only on a turn key basis in a manner that permits us to operate the system and collect transaction fees and service fees for an extended period of time. Our business plan is also to focus on large scale governmental clients that will cause wide use of our Super Smart Card and BVS2 system and related technologies and maximize our potential transaction fee base.

Leverage Existing Relationships and Seek New Ones. We have entered into a relationship with Daewoo International, among others, to help us serve the Asian card market. We have entered into this relationship, and others, in order to facilitate and accelerate our penetration into new markets, and to assist us in defining and pursuing new applications for our products. We are continuously seeking additional relationships to complement our marketing strategy and promote our brand worldwide.

Leverage Presence in Existing Industries to Enter into New Industries. We intend to offer our customers the ability to add new applications to their smart cards, thereby expanding the number of industries in which our products are used and the number of transaction fees that we could potentially collect. For example, users of the national ID card will have the option to add a payment application to their card among many others. We plan to generate additional revenues through the sale and installation of the software required to add and operate these applications.

Table of Contents

Marketing and Distribution

We intend to enhance our position in the design and development of Super Smart Card and BVS2 based products and related technologies by developing new applications for our technology. We also intend to enter new markets, either alone or through strategic relationships, to create additional potential sources of revenues from transaction fees and additional potential sources for revenue from customer support.

We intend to market our technologically advanced products directly, through our Homeland Defense, Inc. affiliate, and through e-Smart Korea, Inc., our Korean subsidiary, as well as indirectly through a global network of strategic relationships with major systems integrators and others. Our sales and marketing efforts will be directed from our offices in Seoul, Korea, Beijing, China, New York and Washington, DC.

Proprietary Technologies

We are the owner of three technology licenses. Each license has been granted pursuant to an Exclusive Use and Distribution Agreement (collectively the License Agreements), each of which grants us exclusive rights to the technology in a particular territory. The three territories covered are the People's Republic of China, all of Asia except the People's Republic of China and the United States of America. IVI Smart, the current licensor, is one of our principal shareholders. The rights to technology granted to us includes all smart card and related assets of the licensor including the Super Smart Card, the BVS2 platform and all relevant components thereof. The License Agreements require that all inventions and improvements made by us be assigned to the licensor with a license to use granted back to us on the same terms and conditions as the technology was granted to us in the original license. We are jointly responsible to protect and defend the technology in the event of challenge, or disputes of any kind in a covered territory.

Our success and ability to compete depend in large part upon the protection of the proprietary technology that we license. We and the licensor rely on a combination of patent, trademark, copyright and trade secret law, as well as know-how, confidentiality agreements and other contractual relationships with employees, affiliates, distributors and others. In this regard, our licensor has a number of pending patent applications in various jurisdictions, globally.

Neither we nor the licensor can be certain that patents will be issued with respect to any of the pending or future patent applications. In addition, as with every other company that depends on patents, until the outcome of any future litigation is determined, we can not be certain that any patents if issued will be enforceable against alleged infringers or will be upheld if their validity is challenged.

Competition

Based on our own extensive research, as of the date hereof, we believe that there is no product that can directly compete with the Super Smart Card and the BVS2 platform. On the other hand, there are numerous products and competitors in the smart card and

Table of Contents

smart card operating system arena. We must, therefore, anticipate competition in sales of our products, systems and technologies from other providers of microprocessor-based smart card technologies. We expect competition to intensify as, and if, we become successful in our deployment plans and our competitors commit greater resources to the development of biometrically empowered contactless microprocessor-based smart cards. Some of the larger chip manufacturers that operate in the smart card market, including Atmel, STM, Infineon and Philips Semiconductors, have announced that they are developing contactless microprocessor-based smart cards. However, we know of no card planned or otherwise that has the sophistication and features of the Super Smart Card .

We also compete with contactless ASIC-based technologies developed primarily by Philips Semiconductors, which comply with ISO 14443 and which are used by some of the largest manufacturers of smart cards, including Gemplus, Giesecke & Devrient, and Sony's contactless ASIC based technology. Further, we also compete with contact-based products such as microprocessor-based contact cards, ASIC-based contact cards, memory chip cards and magnetic strip cards.

We believe that all of these cards offer inferior functionality compared to our dual interface, biometrically powered, contactless microprocessor-based smart cards. Nevertheless, some of our potential customers have in the past, and may in the future, consider these inferior alternatives sufficient for their needs.

Employees

As of December 31, 2005 we had two contract administrators at our New York headquarters, two employees in San Jose, California, a staff of eight in our main Asian marketing office in Seoul, Korea, and two consultants in Singapore. Our Chief Executive Officer, President and Chief Financial Officer, Mary A. Grace, lives in Boulder, Colorado but travels more than 95% of the time on our behalf, and our Chief Technical Officer, Tamio Saito, lives in San Jose, California. None of our employees is a party to a collective bargaining agreement.

Risk Factors

The following risks with respect to our proposed business and financial condition should be carefully considered. These risks and uncertainties are not the only ones facing us. Other risks and uncertainties that have not been predicted or assessed by us may also adversely affect us. Some of the information in this report contains forward-looking statements that involve substantial risks and uncertainties. These statements can be identified by forward-looking words such as may, will, expect, anticipate, believe, intend, estimate, and continue or other similar words. Statements that contain these words should be carefully read for the following reasons:

The statements may disclose our future expectations;

The statements may contain projections of our future earnings or our future financial condition; and

The statements may state other forward-looking information.

Table of Contents

Risks Related to Our Business

Until recently, we were delinquent in filing reports with the SEC.

Although we are required to file annual, quarterly and special reports, and other information with the Securities and Exchange Commission (the SEC), until January 10, 2005, we were materially delinquent in our filing of these required reports. Accordingly, and during the period from October 10, 2000 through January 10, 2005, there were periods during which there was limited public information on which to base an informed investment decision concerning our securities.

The SEC commenced an Administrative Proceeding against us.

On February 3, 2005, Administrative Law Judge, Lillian A. McEwen (the ALJ) published her Initial Decision on Remand (the Remand Decision) in an Administrative Proceeding originally commenced by the Securities and Exchange Commission (the SEC) against us on December 12, 2003 (the Proceeding). In the Remand Decision, the ALJ denied the SEC's Division of Enforcement's (the Division) request for the imposition of sanctions against us, and gave both sides 21 days to appeal her decision. The Division's time to appeal expired on February 24, 2005. Accordingly the Remand Decision became final. Details concerning the Proceeding are set forth herein under Item 3, Legal Proceedings.

We have no history of revenue from operations and we have only minimal assets.

As of the date of this report, we have yet to generate any revenue from operations. Our assets are comprised principally of the contracts we have signed and our licenses of the smart card intellectual property from IVI Smart. In all likelihood, we will continue to incur pre-operating expenses without corresponding revenues for some time in the foreseeable future. This may result in continuing increases in our net operating loss until we can generate cash flow from operations. There can be no assurance that we will be successful in developing our proposed operations or that we will ever become profitable.

We are undercapitalized and may be unable to continue our business unless we raise additional money.

We have limited working capital and, until delivery on contracts for our system and smart cards, we will continue to be dependent upon proceeds derived from private securities offerings for funds for the continuation of our proposed transaction business. We will need to obtain additional financing in order to implement all the material aspects of our business plan. There can be no assurance that additional financing will be available to us on acceptable terms, if at all. If we continue to raise funds by issuing additional equity securities, further dilution to existing equity holders will necessarily result. Accordingly, we are subject to all of the risks inherent in starting a new business enterprise including the potential loss of all monies invested.

Table of Contents

We may not be able to operate successfully if we are unable to hire qualified additional personnel.

Our success may largely be dependent on the personal efforts and abilities of our management and our ability to attract and retain qualified key personnel in the future. Except for Tamio Saito, our Chief Technical Officer and member of our Board of Directors, none of our management team has ever operated a smart card business or has any experience with the manufacture and marketing of smart card products. In addition to performing their regular duties, our management must spend a significant amount of time devising strategies to execute our business model.

We are presently highly dependent upon four people.

Our ultimate success or failure will depend to a large extent on the services and efforts of our two executive and operating officers, Mary A. Grace and Tamio Saito, as well as the co-inventor of our BVS2 and Super Smart Card technology, Wayne Drizin, and the Managing Director of e-Smart Korea, Richard In Kun Kim. The loss of the services of any one or more of these key persons, especially during the period prior to the design, complete installation and successful operation of our first biometric card and BVS2 based products and related technologies system will have a material adverse effect on the continued economic viability of our company. Since we believe that Messrs. Saito and Drizin are the individuals best able to continue to refine, to present and to customize the use of our system and oversee its installation, and that Ms. Grace and Mr. Kim are essential managers, the untimely demise, unavailability or disability of one or more of these four persons, would leave us without the ability to pursue, procure and fulfill contracting opportunities or possibly even to continue our business.

We have no Key Man Insurance.

Presently, we do not maintain or carry any key man life insurance. We intend to purchase life insurance on the lives of our key personnel as soon as possible. Upon purchase of this insurance, we will pay the premiums and designate the Company as the sole beneficiary. The lack of key man coverage and the lack of other such insurance may have a material adverse effect upon our business in the event of the untimely loss of any of our key employees.

We have no director's and officer's liability insurance

The employment of other qualified officers and directors may be contingent upon our acquiring a policy of directors and officers liability insurance in an amount reasonably satisfactory to such nominees. Our failure to acquire such a policy may prevent us from attracting the services of other qualified officers and directors.

Table of Contents

We have a history of losses and may not achieve profitability in the foreseeable future.

We have incurred losses in each year since our inception. Our losses resulted primarily from expenses we incurred in research and development, selling and marketing, as well as general and administrative expenses. We have never had any revenue. We expect to continue to incur operating losses in future periods as we invest in the expansion of our global operations and continue to enhance our research and development capabilities and expand our relationship with contract manufacturers.

If the market for smart cards in general, and for biometric, multi-application-based smart cards in particular, does not grow as we expect, we may not succeed in selling our products.

The success of our products depends on commercial enterprises, governmental authorities and other potential card issuers adopting biometric multi-application based smart card technologies. Other card technologies, such as magnetic strips or bar codes, are widely used and could be viewed by potential customers as more cost effective alternatives to our products. Additionally, potential customers in developed countries such as the United States may already have installed systems that are based on technologies different than ours and may therefore be less willing to incur the capital expenditure required to install or upgrade to a biometric multi-application-based smart card system. As a result, we cannot provide any assurance that there will be significant market opportunities for smart card systems. If demand for biometric multi-application-based smart card products such as ours does not develop or develops more slowly than we anticipate, we may have fewer opportunities for growth than we expect.

If we fail to develop new products or adapt our existing products for use in new markets, our revenue growth may be impeded and we may incur significant losses.

To date, we have not implemented any advanced Super Smart Card and BVS2 System. We are currently developing and planning delivery of our technology for use as maximum security ID and payment cards, for use by governmental authorities, banks and commercial enterprises. We have not yet received revenues from sales of these products. We are devoting significant resources to developing and marketing these and other products and adapting our existing products for use in new markets. If we fail to develop markets for our products we will not generate revenues and will continue to incur significant losses.

Our inability to maintain our current, and establish new, strategic relationships could impair our revenue growth.

In accordance with our business model, we plan and have entered into strategic relationships in order to facilitate or accelerate our penetration into new markets. The termination of any of our strategic relationships or our failure to develop additional relationships in the future may limit our ability to develop markets or to sell particular products, and thereby impair our revenue growth.

Table of Contents

We face intense competition. If we are unable to compete successfully, our business prospects will be impaired.

We face intense competition from developers of contact and contactless microprocessor-based technologies and products, developers of contactless products that use other types of technologies that are not microprocessor-based, and non-smart card technologies. We compete on a range of competitive factors including price, compatibility with the products of other manufacturers, and the ability to support new industry standards and introduce new reliable technologies. Many of our competitors, such as Phillips Semiconductors, a division of Phillips Electronics N.V., and Infineon Technologies AG, have greater market recognition, larger customer bases, and substantially greater financial, technical, marketing, distribution, and other resources than we possess. As a result, they may be able to introduce new products, respond to customer requirements and adapt to evolving industry standards more quickly than we can.

While at the moment we believe we offer a unique product that is easy to differentiate from our competitors, in the future, we may not be able to differentiate our products sufficiently from those of our competitors. If we cannot compete successfully with our existing and future competitors, we could fail to develop revenues.

From time to time, we or one or more of our present or future competitors may announce new or enhanced products or technologies that have the potential to replace or shorten the life cycles of our existing products. The announcement of new or enhanced products may cause customers to delay or alter their purchasing decisions in anticipation of such products, and new products developed by our competitors may render our products obsolete or achieve greater market acceptance than our products.

If there is a sustained increase in demand for microprocessors, availability might be limited and prices might increase.

Our products require microprocessors and other silicon based chips. The microprocessor industry periodically experiences increased demand and limited availability due to production capacity constraints. . Increased demand for, or limited availability of, microprocessors could substantially increase the cost of producing our products. In addition, as a result of a shortage, we may be forced to delay shipments of our products, or devote additional resources to maintaining higher levels of microprocessor inventory. Consequently, we may experience substantial period-to-period fluctuations in our cost of revenues and, therefore, in our future results of operations.

Our products have long development cycles and we may expend significant resources in relation to a specific project without realizing any revenues.

The development cycle for our products varies from project to project. Typically, the projects in which we are involved are complex and require that we customize our products to our customers' needs and specifications. We then conduct evaluation, testing, implementation and acceptance procedures of the customized products with the customer. Only after successful completion of these procedures will customers place orders for our products in commercial quantities, if any. We, therefore, cannot provide an assurance that contracts that we enter into will result in commercial sales. As a result, we may expend financial, management and other resources to develop customer relationships before we become capable of recognizing any revenues.

Table of Contents

We are dependent on a small number of suppliers for critical components, delays or discontinuance of the supply of components may hamper our ability to produce our products on a timely basis and cause short-term adverse effects.

The components we use in our products, including microprocessors and cards, are supplied by third party suppliers and manufacturers. Many of these suppliers are our sole suppliers. Although we are now in the process of securing additional sources of supply, in the meantime, we may experience short-term adverse effects due to delayed shipments that will delay the supply of our products to our customers, and that may result in cancellation of orders for our products. In addition, we do not generally have long term supply contracts under which our suppliers are committed to supply us with components at a fixed price. Suppliers could increase component prices significantly without warning or could discontinue the manufacture or supply of components used in our products. We may not be able to develop alternative sources for product components if, and as, required in the future. Even if we are able to identify any alternative source of supply, we may need to modify our products to be compatible with other components, which may cause delays in product shipments, increase manufacturing costs and increase product prices.

Because some of our suppliers are located in Europe and the Far East, we may experience logistical problems in our supply chain, including long lead times for receipt of products or components and shipping delays.

If we fail to hire, train and retain qualified research and development personnel, our ability to enhance our existing products, develop new products and compete successfully may be materially and adversely affected.

Our success depends, in part, on our ability to hire, train and retain qualified research and development personnel. Individuals who have expertise in research and development in our industry are scarce. Competition for such personnel is intense in the electronics industry, particularly in the United States, and therefore hiring, training and retaining such personnel is both time consuming and expensive. If we fail to hire, train and retain employees with skills in research and development, we may not be able to enhance our existing products or develop new products.

Our ability to compete depends on our continuing right to use, and our ability to protect, our intellectual property rights.

Our technology is licensed from a major shareholder, IVI Smart (see *Proprietary Technologies*). Our success and ability to compete depend in large part on using our licensed intellectual property and proprietary rights to protect the technology we use and the products we make. We rely on a combination of patent, trademark, copyright and trade secret law, as well as confidentiality agreements and other contractual relationships with our employees, customers, affiliates, distributors and others.

Table of Contents

Our licensor currently has patents pending in the United States, Europe, Japan and elsewhere that have not yet resulted in granted patents. We cannot be certain that patents will be issued with respect to any of these pending or future patent applications or that the scope of any future patents that are issued to our licensor, will provide us with adequate protection for our technology and products. Others may challenge these patents or registered trademarks. We do not know whether any of them will be upheld as valid or will be enforceable against alleged infringers and thus we do not know whether they will enable us to prevent or hinder the development of competing products or technologies. Moreover, patents provide legal protection only in the countries where they are registered and the extent of the protection granted by patents varies from country to country.

The measures we have taken to protect our technology and products may not be sufficient to prevent their misappropriation by third parties or independent development by others of similar technologies or products. Competitors may also develop competing technology by designing around our patents and will then be able to manufacture and sell products which compete directly with ours. In that case, our business and operating results would be harmed. Substantially all of our employees are subject to non-compete agreements but there is no assurance that employees will not breach such agreements, necessitating costly and protracted litigation.

In order to protect our technology and products and enforce our patents and other proprietary rights, we may need to initiate litigation against third parties or defend opposition proceedings before the European Patent Office or prosecute interference proceedings before the U.S. Patent and Trademark Office. These legal and administrative proceedings could be expensive and occupy significant management time and resources.

Furthermore, a successful opposition to our patent in any jurisdiction could provide a basis for our competitors to claim that our patents in other jurisdictions covering this technology are invalid.

Our products may infringe the intellectual property rights of others.

It is not possible to know with certainty whether the manufacture and sale of our products will infringe patents or other intellectual property rights owned by third parties. There may, for example, be patent applications pending at the moment, which if granted, may cover products that we have just developed or are developing. In certain other jurisdictions there is no publication of the subject matter of patents until the patents are issued. Third parties may from time to time claim that our current or future products infringe their patent or other intellectual property rights. In addition, if third parties claim that our customers are violating their intellectual property rights, our customers may seek indemnification from us, which could be costly, or may terminate their relationships with us. Any intellectual property claim could involve time-consuming and disruptive litigation and, if determined adversely to us, could prevent us from making or selling our products, and subject us to substantial monetary damages or require us to seek licenses.

Table of Contents

Intellectual property rights litigation is complex and costly, and we cannot be sure of the outcome of any such litigation. Even if we prevail, the cost of such litigation could harm our results of operations. In addition, such litigation is time consuming and could divert our management's attention and resources away from our business. If we do not prevail in any litigation, in addition to any damages we might have to pay, we might be required to discontinue the use of certain processes, cease the manufacture, use and sale of infringing products and solutions, expend significant resources to develop non-infringing technology or obtain licenses on unfavorable terms. Licenses may not be available to us on acceptable terms or at all. In addition, some licenses are non-exclusive and, therefore, our competitors may have access to the same technology licensed to us. If we fail to obtain a required license or cannot design around any third party patents or otherwise avoid infringements, we may be unable to sell some of our products.

We are susceptible to changes in international markets and difficulties with international operations could harm our business.

Our ability to penetrate any market, whether domestic or international, is dependent, in part, on political and economic factors that we have no control over. In addition, there are certain inherent risks in international operations which include:

Changes in regulatory requirements and standards;

Required licenses, tariffs and other trade barriers;

Difficulties in enforcing intellectual property rights across, or having to litigate disputes in, various jurisdictions;

Difficulties in staffing and managing international operations;

Potentially adverse tax consequences; and

The burden of complying with a wide variety of complex laws and treaties in various jurisdictions.

General political instability

If we are unable to manage the risks associated with our focus on international sales, our business may be harmed.

We may have to adapt our products in order to integrate them into our customers' systems or if new government regulations or industry standards are adopted or current regulations or standards are changed.

Some of our products are subject to mandatory government regulation in the countries in which they are used. For example, card readers that are used in the United States require certification of compliance with regulations of the Federal Communications Commission and in Europe of compliance with regulations of the European Telecommunications Standards Institute regarding

Table of Contents

emission limits of radio frequency devices. In addition, governmental certification for the systems into which our products are integrated may be required. The International Standards Organization is in the process of approving industry standards regulating the transfer of data between contactless smart cards and readers. If there is a change to government regulations or industry standards, we may have to make significant modifications to our products and, as a result, could incur significant costs and may be unable to deploy our products in a timely manner.

In addition, prior to purchasing our products, some customers may require us to receive certification that our products can be integrated successfully into their systems or comply with applicable regulations. Receipt of these certifications may not occur in a timely manner or at all. In some cases, in order for our products, or for the system into which they are integrated, to be certified, we may have to make significant product modifications. Failure to become so certified could render us unable to deploy our products in a timely manner or at all.

Our products may contain defects that we find only after deployment, which could harm our reputation, result in loss of customers and revenues and subject us to product liability claims.

Our products are highly technical and deployed as part of large and complex projects. Any defects in our products could result in:

Harm to our reputation;