SCM MICROSYSTEMS INC
Form 10-K
March 18, 2008

Table of Contents

UNITED STATES SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

Form 10-K

þ **ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**
For the fiscal year ended December 31, 2007

or

o **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 0-29440

SCM MICROSYSTEMS, INC.
(Exact Name of Registrant as Specified in its Charter)

DELAWARE	**77-0444317**
(State or other jurisdiction of Incorporation or organization)	*(I.R.S. Employer Identification Number)*
Oskar-Messter-Strasse 13, Ismaning, Germany	**85737**
(Address of Principal Executive Offices)	*(Zip Code)*

Registrant s telephone number, including area code:
+49 89 95 95 5000

Securities Registered Pursuant to Section 12(b) of the Act:
None

Securities Registered Pursuant to Section 12(g) of the Act:
Common Stock, $0.001 par value, and associated Preferred Share Purchase Rights
(Title of Class)

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

Indicated by check mark if the registrant is not required to file reports pursuant to Section 13 or Section 15(d) of the Act. Yes o No þ

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 þ No o

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 or any amendment to this Form 10-K. þ

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

Large accelerated filer o	Accelerated filer o	Non-accelerated filer o (Do not check if a smaller reporting company)	Smaller reporting Company þ

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

Based on the closing sale price of the Registrant s Common Stock on the NASDAQ National Market System on June 30, 2007, the last business day of the Registrant s most recently completed second fiscal quarter, the aggregate market value of Common Stock held by non-affiliates of the Registrant was $37,531,932.

At March 6, 2008, the registrant had outstanding 15,743,515 shares of Common Stock.

DOCUMENTS INCORPORATED BY REFERENCE

Designated portions of the Company s Proxy Statement and Notice of Annual Meeting to be filed within 120 days after the Registrant s fiscal year end of December 31, 2007 are incorporated by reference into Part II, Item 5 and Part III of this Report.

SCM Microsystems, Inc.

Form 10-K
For the Fiscal Year Ended December 31, 2007

TABLE OF CONTENTS

Table of Contents

PART I

This Annual Report on Form 10-K, including the documents incorporated by reference in this Annual Report, contains forward-looking statements within the meaning of Section 27A of the Securities Act of 1933, as amended, and Section 21E on Form 10-K of the Securities Exchange Act of 1934, as amended. For example, statements, other than statements of historical facts regarding our strategy, future operations, financial position, projected results, estimated revenues or losses, projected costs, prospects, plans, market trends, competition and objectives of management constitute forward-looking statements. In some cases, you can identify forward-looking statements by terms such as believe, could, should, would, may, anticipate, intend, plan, estimate, expect, project or the ne other similar expressions. Although we believe that our expectations reflected in or suggested by the forward-looking statements that we make in this Annual Report on Form 10-K are reasonable, we cannot guarantee future results, performance or achievements. You should not place undue reliance on these forward-looking statements. All forward-looking statements speak only as of the date of this Annual Report on Form 10-K. While we may elect to update forward-looking statements at some point in the future, we specifically disclaim any obligation to do so, even if our expectations change, whether as a result of new information, future events or otherwise. We also caution you that such forward-looking statements are subject to risks, uncertainties and other factors, not all of which are known to us or within our control, and that actual events or results may differ materially from those indicated by these forward-looking statements. We disclose some of the factors that could cause our actual results to differ materially from our expectations in the Customers, Research and Development, Competition, Proprietary Information and Technology and Risk Factors sections and elsewhere in this Annual Report on Form 10-K. These cautionary statements qualify all of the forward-looking statements included in this Annual Report on Form 10-K that are attributable to us or persons acting on our behalf.

ITEM 1. *BUSINESS*

Description of Business

SCM Microsystems, Inc. (SCM, the Company, we and us) was incorporated in 1996 under the laws of the state of Delaware. We design, develop and sell hardware, software and silicon solutions that enable people to conveniently and securely access digital content and services. We sell our secure digital access products in two market segments: PC Security and Digital Media Readers.

For the PC Security market, we offer smart card reader technology that enables authentication of individuals for applications such as electronic identification and driver s licenses, electronic healthcare cards, secure logical access to PCs and networks, and physical access to facilities. Within the PC Security segment, we also offer a line of smart card solutions under the CHIPDRIVE® brand that include productivity applications such as time recording and attendance, physical access and password management for small and medium sized enterprises.

For the Digital Media Reader market, we offer digital media readers that are used to transfer digital content to and from various digital flash media. These readers are primarily used in digital photo kiosks.

We sell our products primarily to original equipment manufacturers, or OEMs, who typically either bundle our products with their own solutions, or repackage our products for resale to their customers. Our OEM customers include: government contractors, systems integrators, large enterprises and computer manufacturers, as well as banks and other financial institutions for our smart card readers; and computer electronics and photoprocessing equipment manufacturers for our digital media readers. We sell and license our products through a direct sales and marketing organization, as well as through distributors, value added resellers and systems integrators worldwide. We sell our

CHIPDRIVE products primarily through retail channels and the Internet.

In May 2006, we completed the sale of our Digital Television solutions (DTV solutions) business to Kudelski S.A. As a result, we have accounted for the DTV solutions business as a discontinued operation, and the statements of operations and cash flows for all periods presented reflect the discontinuance of this business. In addition, our operations previously included a retail Digital Media and Video business, which we sold in the third quarter of 2003. As a result of this sale and divestiture, beginning in the second quarter of fiscal 2003, we have accounted for the retail Digital Media and Video business as a discontinued operation, and statements of operations

Table of Contents

for all periods presented reflect the discontinuance of this business. (See Note 3 to our consolidated financial statements that are included in this Annual Report on Form 10-K.)

Overview of the Market for Secure Digital Access Products

Individuals, businesses, governments and educational institutions increasingly rely upon computer networks, the Internet and intranets for information, entertainment and services. The proliferation of and reliance upon electronic data and electronic transactions has created an increasing need to protect the integrity of digital data, as well as to control access to electronic networks and the devices that connect to them. For government entities and large corporate enterprises, there is a need to restrict and manage access to shared networks and intranets to prevent loss of proprietary data. In addition, there is a need to manage and monitor access to information stored on identification cards used in new government-driven programs around the world, such as electronic passports, driver s licenses, citizen ID and electronic healthcare cards. In some cases, there may also be a need to expand the capability of electronic networks to protect or restrict access to physical facilities for corporate employees or government personnel. Finally, for consumers and online merchants or banks, there is a need to authenticate credit cardholders or bank clients for Internet-based or other electronic transactions without jeopardizing sensitive personal account information. In all of these areas, we believe standards-based devices that easily interface to a PC or network to provide secure, controlled access to digital content or services are an easily deployed and effective solution.

PC and Network Security Market

The proliferation of personal computers in both the home and office, combined with widespread access to computer networks and the Internet, have created significant opportunities for electronic transactions of all sorts, including business-to-business, e-government, e-commerce and home banking. In government agencies and corporate enterprises, the desire to link disparate divisions or offices, reduce paperwork and streamline operations is also leading to the adoption of more computer- and network-based programs and processes. Network-based programs are also used to track and manage data about large groups of people, for example, citizens of a particular country. While the benefits of computer networks may be significant, network and Internet-based transactions also pose a significant threat of fraud, eavesdropping and data theft for both groups and individuals. To combat this threat, parties at both ends of the transaction must be assured of the integrity of the transaction. Online merchants and consumers need assurance that customers are correctly identified and that the authenticity and confidentiality of information such as credit card numbers is established and maintained. Corporate, government and other networks need security systems that safeguard the data of individuals and protect the network from manipulation or abuse, both from within and without the system.

Increasingly, large organizations such as corporations, government agencies and banks are adopting systems that protect the network, the information in it and the people using it by authenticating each user as the user logs on and off the network. Authentication of a user s identity is typically accomplished by one of two approaches: passwords, which are codes known only by specific users; and tokens, which are user-specific physical devices that only authorized users possess. Passwords, while easier to use, are also less secure because they tend to be short and static, and are often transmitted without encryption. As a result, passwords are vulnerable to decoding or observation and subsequent use by unauthorized persons. Tokens range from simple credit card-size objects to more complex devices capable of generating time-synchronized or challenge-response access codes. Certain token-based systems require both possession of the token itself and a personal identifier, such as a fingerprint or personal identification number, or PIN, to indicate that the token is being used by an authorized user. Such an approach, referred to as two-factor authentication, provides much greater security than single factor systems such as passwords or the simple possession of a token.

One example of a token used in two-factor authentication is the smart card, which contains an embedded microprocessor, memory and a secure operating system. In addition to their security capabilities, smart cards are able to store data such as account information, healthcare records, merchant coupons, still or video images and, in some cases, cash. Smart cards are typically about the size of a credit card and can easily be carried in a wallet or attached to a badge. Smaller cards designed for use with small devices such as mobile phones are also increasingly being utilized. Depending on the application for which they are being used, smart cards can be designed to insert

Table of Contents

into a reader attached to a PC or other device, or can include wireless capabilities for contactless interface. Worldwide shipments of smart cards topped 3.3 billion in 2007 and are estimated to grow to nearly 3.9 billion in 2008 for applications ranging from mobile communications to corporate security to online banking, according to the European smart card industry organization, Eurosmart. Demand for readers used in conjunction with those cards is also expected to grow. In a March 2006 report, research firm Frost & Sullivan predicts that reader shipments will grow from 6.9 million in 2004 to 33 million in 2010. We believe that the combination of smart cards and readers provides a secure solution for network access, personal identification, electronic commerce and other transactions where authentication of the user is critical.

To date, the largest and one of the most advanced deployments of smart cards for digital security purposes has been the U.S. Department of Defense s Common Access Card (CAC) program. Beginning in October 2000, the U.S. Department of Defense has distributed more than 10 million smart cards to military personnel and contractors. These cards are being used as the standard identification credential for military personnel, and are also being used for secure authentication and network access. In compliance with Homeland Security Presidential Directive (HSPD)-12, since late 2006, the CAC card also has served as a standard identity credential that is both secure and interoperable across all federal agencies, regardless of which agency issued the card. To satisfy the technical requirements of HSPD-12, the National Institute for Standards and Technology (NIST) developed Federal Information Processing Standards Publication 201 (FIPS 201) a U.S. federal government standard specifying Personal Identity Verification (PIV) requirements for federal employees and contractors. Under FIPS 201 specifications, PIV cards must also include capabilities for contactless interface with security terminals at doorways and other entrances to provide secure physical access at government facilities.

In order to comply with HSPD-12, government facilities are replacing their existing access control credentials with PIV cards and are replacing their CAC card readers with FIPS 201 compliant smart card readers. The U.S. government s decision to deploy an integrated, agency-wide, common smart card platform will continue to raise the awareness of smart card technology and hence increase the demand for contactless smart card proximity readers in both public and private sectors, according to IMS Research Group. A July 2007 market study from IMS Research forecasts that the American market for electronic physical access control equipment will reach $925 million in 2011, with a forecast compound annual growth rate (CAGR) of 8.3%. One of the key trends driving this growth is the replacement of 125 kHz proximity readers with 13.56MHz smart card readers. This trend is set to accelerate over the next two years following the introduction of the government mandate HSPD-12.

The U.S. government is actively driving the use of smart cards outside the boundaries of the U.S. as well, with the request in 2002 to 27 visa waiver countries to develop electronic passports that will include biometric data to authenticate the holder. Under the auspices of the International Civil Aviation Organization (ICAO), several countries have been working together to define and develop standards for e-passports based on contactless smart card technology. The goal of the program is to ensure that these e-passports cannot be copied or altered, and that the biometric facial image stored on the card could be used to positively identify the holder. All of the 27 visa waiver countries now issue electronic passports and many countries worldwide have introduced the new documents, including Australia, Belgium, Canada, China, Denmark, Hong Kong, Japan, Korea, Macao, Malaysia, the Netherlands, Singapore, Sweden, the United Kingdom and the U.S.

In many countries, both local and federal governments are beginning to use smart card technology for internal programs, such as new or enhanced national ID cards, storing digital certificates for online transactions, residency permits and visas, and driver s licenses. Some examples of programs include national ID rollouts in Thailand and China and deployment of electronic driver s licenses in Japan. According to IMS Research Group, more than one billion smart cards will be used in identity programs by governments and other public bodies worldwide by 2010.

In addition, many governments are also evaluating or making plans to develop electronic healthcare record systems, which would include smart card-based healthcare cards for participants. Mexico, China, Taiwan and Russia, as well as several European countries, including Austria, Belgium, France, Germany, Italy, Poland and Turkey, are among the countries and regions that have already deployed or are deploying electronic healthcare cards to millions of healthcare users. These cards identify the user and store insurance and medical information that can be accessed by doctors and hospitals, for example. To date, one of the largest programs actively underway is in Germany, where pilot tests were set up in 2007. The German government plans to distribute 82 million new eHealth

Table of Contents

cards to citizens beginning in late 2008 and to have in place a corresponding network and card reader infrastructure for doctors, hospitals, pharmacies and other healthcare providers by 2009.

Outside the government sector, many corporate enterprises are adopting smart card technology to protect access to buildings and computer networks. Several smart card-based employee identification programs have already been put in place by companies such as Boeing, Chevron, Hitachi, Microsoft, Nissan, NTT Corporation, Pfizer, Royal Dutch/Shell Group and Sun Microsystems.

In the financial industry, major credit card companies in many parts of the world have embraced smart card technology as a more secure way to safeguard transactions and eliminate fraud, the cost of which can be significant. The majority of credit cards issued worldwide now comply with the Europay Mastercard Visa (EMV) standard for securing financial transactions using a smart card. Over the last two years, electronic payment programs featuring cards equipped with contactless technology, such as such as Visa® payWave™ and MasterCard® PayPass™, have become widespread in Europe and Asia and are expected to generate significant demand worldwide for smart cards and related technology going forward. Integration of contactless payment technology into mobile phones is expected to further spur demand for contactless technology over the next several years.

Our PC Security Products

We offer a full range of smart card reader technology solutions to address the need for smart card-based security for a range of applications and environments, including PCs, networks, physical facilities and authentication programs. Our products include smart card readers, application specific integrated circuits, or ASICs, and small office productivity packages based on smart cards. We sell our readers and ASICs primarily to PC original equipment manufacturers, or OEMs, smart card solutions providers and government systems integrators to support specific security programs, such as secure logon for employees, secure home banking or U.S. government PIVs program; as well as to OEMs that incorporate our products into their devices, such as PCs or keyboards. We sell our CHIPDRIVE small office productivity packages primarily to end users via retail channels and the Internet.

Smart Card Readers. We are one of the world s leading suppliers of smart card readers for security-oriented applications. Our smart card readers are hardware devices that connect either externally or internally with a computer or other processing platform to verify the identity of, or authenticate, the user, and thus control access. Much like a lock works with a key, our readers work with a smart card to admit or deny access to a computer or network, or to authenticate the card holder for identification and access to facilities, programs or services. Our readers are used to authenticate users in order to support security programs and applications for corporations, financial institutions, governments and individuals. These security programs and applications include secure network logon; personnel identification for programs such as healthcare delivery, driver s licenses and electronic passports; secure home banking; digital signatures; and secure e-commerce.

Our products employ an open-systems architecture that provides compatibility across a range of hardware platforms and software environments and accommodates remote upgrades so that compatibility can be maintained as the security infrastructure evolves. We have made significant investments in software embedded in our products that enable our smart card readers and components to read the majority of smart cards in the world, regardless of manufacturer or application. Our smart card readers are also available with a variety of interfaces, including biometric (fingerprint), wireless/contactless, keypad, USB, PCMCIA, ExpressCard® and serial port, and offer various combinations of interfaces integrated into one device in order to further increase the level of security.

To address the varied needs of our customers, we offer an array of smart card readers. These include readers designed for various platforms, such as desktop and notebook computers; readers for contactless interface; as well as readers offering incremental levels of protection against unauthorized use, from simple PC Card reader devices to more

complex PIN entry systems, which require both a smart card and a user s personal identification number to authenticate the user. Our smart card reader product line includes:

Secure Card Readers internal or external card readers requiring only a smart card to provide secure authentication;

Secure PINpad Readers external readers with a numeric PINpad that utilize a smart card in conjunction with a personal identification code to ensure two factor authentication of the user;

Table of Contents

Contactless Readers and Dual Interface Readers internal and external readers that address the demand for contactless interface used in many security programs based on smart cards, for example public transport, e-banking and e-passport personalization and verification;

Physical Access Control Terminal (PACT) designed to address the requirements of the U.S. government for secure access to facilities. The PACT terminal combines new technologies such as contactless and biometric interface with existing control systems as well as CAC and newer PIV credential cards, to provide support for new connectivity options going forward;

eHealth terminal specifically designed to meet the requirements of the German Health Card, to support Germany s intended rollout of healthcare cards to 82 million citizens. The eHealth100 terminal reads and operates both with Germany s current memory card-based health card as well as the new chip-based card, and is compliant for use with three different card types: the electronic health card (eGK), the health professional card (HPC), and the Secure Module Cards (SMC) used for secure data communication;

ePassport readers designed to read all electronic passports currently in use or planned for distribution. Ranked among the highest in interoperability and versatility in international interoperability tests. We offer both complete ePassport readers and ePassport modules that can be incorporated into customer terminals and designs;

Mobile Readers unconnected devices that enable secure network access and user authentication by generating one-time passwords; and

Keyboard Readers reader interfaces that are designed to be embedded into a computer keyboard at the manufacturer.

Our smart card readers are developed in compliance with relevant industry standards related to the applications for which they will be used, including PC/SC, EMV, FINREAD and Common Criteria. For example, many of our readers, including the SCRx31 Secure Card Reader line, conform to EMV international standards for financial transactions. We typically customize our smart card readers with unique casing designs and configurations to address the specific requirements of each customer.

In addition, we also offer *ASICs/Chip Sets,* which provide smart card interface capabilities for embedded platforms, such as desktop computers or keyboards. We offer two levels of ASICs to provide both basic smart card interface capability and support for multiple interfaces and reader devices. All of our ASICs comply with all relevant security standards for applications in the smart card industry. In addition, our advanced chip allows on-board flash upgrades for future firmware and application enhancements.

CHIPDRIVE Productivity Solutions. We offer several CHIPDRIVE packages, consisting of smart cards, readers and software applications, for small and medium sized businesses. These products support applications such as smart card-enabled logon to Microsoft® Windows® and smart card-based, secure electronic time recording.

Digital Media Reader Market

Digital cameras have rapidly saturated the consumer market over the last few years, with 80% of U.S. households predicted to own a digital camera by 2010, according to Gartner Group. Camera phones have also gained rapid popularity, with the result that 15% of consumers declare their phones to be their primary picture taking device, according to an October 2007 survey from InfoTrends. InfoTrends estimates that U.S. output of digital photo prints

will grow from 13.2 billion prints in 2005 to 16 billion by 2009. Digital flash media cards, which store digital images on the majority of digital cameras and some camera phones, are the key driver behind digital print growth. Higher capacity memory cards allow digital camera users to take more pictures before having to download images or swap out the card. As card capacities increase, more time is needed to download images. This uses more of the camera s battery life, which already may be insufficient for many camera owners. To print without draining the camera battery, the digital flash media card can be removed and inserted into a card reader on a PC, printer or kiosk to download and print images.

Retail photo kiosks and minilabs, which give instant, high-quality printouts of digital images, make printing photos more convenient for the consumer and typically provide higher quality prints than home printers. According

Table of Contents

to a December 2007 survey conducted by InfoTrends, 49% of digital camera owners who print photos had obtained prints at a retail location in 2007, and the number is expected to grow. As flash memory card capacities increase and digital cameras continue to proliferate, we believe consumers will increasingly use photo kiosks and minilabs to download and print their digital pictures. Each photo kiosk or minilab requires a variety of media card readers to download images from the various media cards in use in digital cameras on the market.

Our Digital Media Reader Products

We offer digital media readers that provide an interface to the various formats of digital media cards to download digital images and other content. We sell our digital media readers primarily to photo kiosk manufacturers. Our digital media readers allow photo kiosk makers and others to build digital flash media interface capabilities into their products and provide interface capabilities for all major memory card formats, including PCMCIA I and II, CompactFlash® I and II, MultiMediaCard™, Secure Digital Card®, SmartMedia™, Sony Memory Stick® and xD-Picture Card™. Our digital media readers leverage our interface chips to enable each reader slot to read multiple types of cards. Our digital media reader product line includes:

Preconfigured Drives our 3.5 inch 5- and 6-bay drives provide plug-and-play interface for photo kiosks and mini labs. Marketed as Professional Card Drive (PCD) or Modular (gMOD and PCD-zMOD) readers, these drives are designed to support heavy commercial usage and support multiple media card formats in either an integrated or a modular form factor.

Single Board Drives our single board drives provide flexible interface solutions for print kiosks, photo labs and other applications requiring digital flash media interface. Single board drives can be configured using any combination of media interface and drive placement to address the specific requirements of each kiosk or other product environment.

Business Segment Financial Information

See Note 11 to our consolidated financial statements that are included in this Annual Report on Form 10-K for financial information regarding revenue and gross margin for our reported business segments through 2007. See Management s Discussion and Analysis of Financial Conditions and Results of Operations for historical financial information, including revenue and gross margin.

Technology

Most of the markets in which we participate are in their early stages of development and we expect they will continue to evolve. For example, early markets such as ours typically require complete hardware solutions, but over time requirements shift to critical components such as silicon or software as OEM customers increase their knowledge and sales volumes of the technologies being provided. We are committed to developing products using standards compliant technologies. Our core technologies, listed below, leverage our development efforts to benefit customers across our product lines and markets.

Silicon Strategy. We have implemented a number of our core interface and processing technologies into our own silicon chips. We have also selected what we believe are the best available silicon from outside suppliers based on desired functionality and have embedded our core interface and processing technologies in order to meet time-to-market requirements. We expect to continue to maintain a balance between our own silicon and using third party devices.

Firmware and Drivers. For our PC Security products, including contact and contactless readers, we have developed interface technology that provides interoperability between PCs and smart cards from many different smart card manufacturers and with many different operating systems. Our interoperable architecture includes an International Standards Organization, or ISO, compliant layer as well as an additional layer for supporting non-ISO compliant smart cards. Through our proprietary integrated circuits and firmware, our smart card readers can be updated electronically to accommodate new types of smart cards without the need to change the reader s hardware. For our Digital Media Reader products, we have developed interface technology that provides interoperability and compatibility between various digital appliances, computer platforms and flash memory cards. For complex

Table of Contents

terminals for electronic healthcare and other markets, we have chosen to use Linux®-based embedded firmware, which helps to provide us the base layers for writing higher levels of application software. All SCM s products are offered with the necessary device drivers for major operating systems, including Microsoft Windows, Windows Vista™, Linux and MAC OS®.

Complete Hardware Solutions. We provide complete hardware solutions for a range of secure digital access applications, and we can customize these solutions in terms of physical design and product feature set to accommodate the specific requirements of each customer. For example, we have designed and manufactured smart card readers that incorporate specific features, such as a transparent case and removable USB cable, to address the needs of specific OEM customers.

Customers

Our products are targeted at government contractors and systems integrators, as well as manufacturers of computers, computer components, consumer electronics and photo processing equipment. Sales to a relatively small number of customers historically have accounted for a significant percentage of our total sales. Sales to our top ten customers accounted for approximately 61% of revenue in 2007, 53% of revenue in 2006 and 54% of revenue in 2005. In 2007, Envoy Data Corporation accounted for more than 10% of our revenue. In 2006, Solectron accounted for more than 10% of our revenue. In 2005, IBM and Shin Shin Co. Ltd. each accounted for more than 10% of our revenue. We expect that sales of our products to a limited number of customers will continue to account for a high percentage of our total sales for the foreseeable future. The loss or reduction of orders from a significant customer, including losses or reductions due to manufacturing, reliability or other difficulties associated with our products, changes in customer buying patterns, or market, economic or competitive conditions in the digital information security business, could harm our business and operating results.

Sales and Marketing

We utilize a direct sales and marketing organization, supplemented by distributors, value added resellers, systems integrators, resellers and Internet sales. As of December 31, 2007, we had 28 full-time employees engaged in sales and marketing activities. Our direct sales staff solicits prospective customers, provides technical advice and support with respect to our products and works closely with customers, distributors and OEMs. In support of our sales efforts, we conduct sales training courses, targeted marketing programs and advertising, and ongoing customer and third-party communications programs, and we participate in trade shows.

Backlog

A significant portion of our sales are made from inventory on a current basis. Sales are made primarily pursuant to purchase orders for current delivery or agreements covering purchases over a period of time. Our customer contracts generally do not require fixed long-term purchase commitments. In view of our order and shipment patterns and because of the possibility of customer changes in delivery schedules or cancellation of orders, we do not believe that such agreements provide meaningful backlog figures or are necessarily indicative of actual sales for any succeeding period.

Collaborative Industry Relationships

We are party to collaborative arrangements with a number of third parties and are a member of several industry consortia. We evaluate, on an ongoing basis, potential strategic alliances and intend to continue to pursue such relationships. Our future success will depend significantly on the success of our current arrangements and our ability to establish additional arrangements. These arrangements may not result in commercially successful products.

NETC@RDS. We are a member of the NETC@RDS initiative, which is devoted to establishing improved health care access and administration procedures for mobile citizens across the European Union (EU), using the electronic European Health Insurance Card. We are a technology provider to the NETC@RDS project and have participated in market validation tests which included 85 pilot sites in 10 EU member states.

Table of Contents

NFC Forum. We are a principal member of the NFC Forum, a non-profit industry association whose mission is to advance the use of Near Field Communication (NFC) technology by developing specifications, ensuring interoperability among devices and services, and educating the market about NFC technology. NFC is a type of radio frequency technology that allows for secure transference of data between a card and reader over distances of not more than a few inches, and is an important technology for contactless payment applications. The NFC Forum consists of 135+ global member companies, including leading mobile communications, semiconductor and consumer electronics firms. NFC Forum members are currently developing specifications for a modular NFC device architecture, protocols for interoperable data exchange and device-independent service delivery, device discovery, and device capability.

PCMCIA. We are a member of the Personal Computer Memory Card International Association, or PCMCIA, an international standards body and trade association with more than 100 member companies. We have been a member of PCMCIA since 1990. PCMCIA was founded in 1989 to establish standards for integrated circuit cards and to promote interchangeability among mobile PCs.

PC/SC Workgroup. We are an associate member of the PC/SC workgroup, a consortium of technology companies that seeks to set the standard for integrating smart cards and smart card readers into the mainstream computing environment.

Silicon Trust. We are a member of Silicon Trust, an industry forum sponsored by Infineon Technologies that focuses on silicon based security solutions, including smart cards, biometrics, and trusted platforms.

Smart Card Alliance. We are a member of the Smart Card Alliance, a U.S.-based, multi-industry association of member firms working to accelerate the widespread acceptance of multiple applications for smart card technology. We are also a member of Smart Card Alliance s Leadership Council.

Teletrust. We are a member of Teletrust, a German organization whose goal is to provide a legally accepted means to adopt digital signatures. Digital signatures are encrypted personal identifiers, typically stored on a secure smart card, which allow for a high level of security through internationally accepted authentication methods. We are also a member of the smart card terminal committee of Teletrust, which defines the standards for connecting smart cards to computers for applications such as secure electronic commerce over the Internet.

We are also members of several digital flash media card organizations, including CompactFlash Association, Memory Stick Developers Forum, MultiMediaCard Association, SD Card Association, SSFDC SmartMedia Forum, xD-Picture Card Forum, Photo Marketing Association International and USB Implementers Forum.

Research and Development

To date, we have made substantial investments in research and development, particularly in the areas of smart card-based physical and network access devices and digital connectivity and interface devices. Our engineering design teams work cross-functionally with marketing managers, applications engineers and customers to develop products and product enhancements to meet customer and market requirements. We also strive to develop and maintain close relationships with key suppliers of components and technologies in order to be able to quickly introduce new products that incorporate the latest technological advances. Our future success will depend upon our ability to develop and to introduce new products that keep pace with technological developments and emerging industry standards while addressing the increasingly sophisticated needs of our customers.

Our research and development expenses were approximately $3.1 million, $3.8 million and $4.1 million for the three years ended December 31, 2007, respectively. As of December 31, 2007, we had 83 full-time employees engaged in research and development activities, including software and hardware engineering, testing and quality assurance and

technical documentation. The majority of our research and development activities occur in India. We expect our research and development expenses to vary based on future project demands and on the markets we target. We expect to add research and development resources in 2008 to enhance our product offerings.

Table of Contents

Manufacturing and Sources of Supply

We utilize the services of contract manufacturers primarily in Singapore to manufacture our products and components. We have implemented a global sourcing strategy that we believe enables us to achieve economies of scale and uniform quality standards for our products, and to support gross margins. In the event any of our contract manufacturers are unable or unwilling to continue to manufacture our products, we may have to rely on other current manufacturing sources or identify and qualify new contract manufacturers. Any significant delay in our ability to obtain adequate supplies of our products from current or alternative sources would harm our business and operating results.

We believe that our success will depend in large part on our ability to provide quality products and services while ensuring the highest level of security for our products during the manufacturing process. We have a formal quality control program to satisfy our customers requirements for high quality and reliable products. To ensure that products manufactured by others are consistent with our standards, we manage all key aspects of the production process, including establishing product specifications, selecting the components to be used to produce our products, selecting the suppliers of these components and negotiating the prices for these components. In addition, we work with our suppliers to improve process control and product design. As of December 31, 2007, we had nine full-time employees engaged in manufacturing and logistics activities, focused on coordinating product management and supply chain activities between SCM and our contract manufacturers.

Over the past several months, we have added alternative sources for both our products and components. Even so, we rely upon a limited number of suppliers for some key components of our products. For example, we currently utilize the foundry services of two suppliers to produce our ASICs for smart cards readers, and we use chips and antenna components from one supplier in our contactless smart card readers. Wherever possible, we have added additional sources of supply for mechanical components such as printed circuit boards or casing. However, a risk remains that we may be adversely impacted by an inadequate supply of components, price increases, late deliveries or poor component quality. In addition, some of the basic components we use in our products, such as digital flash media, may at any time be in great demand. This can result in the components not being available to us timely or at all, particularly if larger companies have ordered more significant volumes of the components; or in higher prices being charged for the components. Disruption or termination of the supply of components or software used in our products could delay shipments of our products, which could have a material adverse effect on our business and operating results. These delays could also damage relationships with current and prospective customers.

Competition

The PC Security and Digital Media Reader markets are competitive and characterized by rapidly changing technology. We believe that competition in these markets is likely to intensify as a result of anticipated increased demand for digital access products. We currently experience competition from a number of sources, including:

Advanced Card Systems, Gemalto (formerly Gemplus and Axalto), O2Micro and OmniKey in smart card readers, ASICs and universal smart card reader interfaces for PC and network access;

AMAG Technology, Bioscrypt, BridgePoint Systems, HID, Integrated Engineering, Precise Biometrics, XceedID and XTec in physical access control terminals; and

Atech, Datafab, OnSpec and YE Data for digital media readers.

We also experience indirect competition from certain of our customers who currently offer alternative products or are expected to introduce competitive products in the future. We may in the future face competition from these and other

parties that develop digital data security products based upon approaches similar to or different from those employed by us. In addition, the market for digital data security and access control products may ultimately be dominated by approaches other than the approach marketed by us.

We believe that the principal competitive factors affecting the market for our products include:

- the extent to which products must support industry standards and provide interoperability;

Table of Contents

the extent to which standards are widely adopted and product interoperability is required within industry segments;

technical features;

quality and reliability;

the ability of suppliers to develop new products quickly to satisfy new market and customer requirements;

ease of use;

strength of distribution channels; and

price.

While we believe that we compete favorably with respect to these factors, we may not be able to continue to successfully compete due to these or other factors and competitive pressures we face could materially and adversely affect our business and operating results.

Proprietary Technology and Intellectual Property

Our success depends significantly upon our proprietary technology. We currently rely on a combination of patent, copyright and trademark laws, trade secrets, confidentiality agreements and contractual provisions to protect our proprietary rights, which afford only limited protection. Although we often seek to protect our proprietary technology through patents, it is possible that no new patents will be issued, that our proprietary products or technologies are not patentable, and that any issued patent will fail to provide us with any competitive advantages.

There has been a great deal of litigation in the technology industry regarding intellectual property rights and from time to time we may be required to use litigation to protect our proprietary technology. This may result in our incurring substantial costs and there is no assurance that we would be successful in any such litigation. Despite our efforts to protect our proprietary rights, unauthorized parties may attempt to copy aspects of our products or to use our proprietary information and software without authorization. In addition, the laws of some foreign countries do not protect proprietary and intellectual property rights to the same extent as do the laws of the United States. Because many of our products are sold and a substantial portion of our business is conducted outside the United States, our exposure to intellectual property risks may be higher. Our means of protecting our proprietary and intellectual property rights may not be adequate. There is a risk that our competitors will independently develop similar technology, duplicate our products or design around patents or other intellectual property rights. If we are unsuccessful in protecting our intellectual property or our products or technologies are duplicated by others, our business could be harmed.

In addition, we have from time to time received claims that we are infringing upon third parties intellectual property rights. Future disputes with third parties may arise and these disputes may not be resolved on terms acceptable to us. As the number of products and competitors in our target markets grow, the likelihood of infringement claims also increases. Any claims or litigation may be time-consuming and costly, divert management resources, cause product shipment delays, or require us to redesign our products, accept product returns or to write off inventory. Any of these events could have a material adverse effect on our business and operating results.

Employees

As of December 31, 2007, we had 153 full-time employees, of which 83 were engaged in engineering, research and development; 28 were engaged in sales and marketing; nine were engaged in manufacturing and logistics; and 33 were engaged in general management and administration. We are not subject to any collective bargaining agreements and, to our knowledge, none of our employees are currently represented by a labor union. To date, we have experienced no work stoppages and believe that our employee relations are generally good.

Foreign Operations

Our corporate headquarters are in Ismaning, Germany and we lease small sales and marketing facilities in California and in Japan. We conduct our research and development activities from our facility in Chennai, India.

Table of Contents

Please see Note 11 to our consolidated financial statements included in this Annual Report on Form 10-K which are included in response to Item 8, for financial information about geographic areas in which we have operations.

Availability of SEC Filings

We make available through our website our annual reports on Form 10-K, quarterly reports on Form 10-Q, current reports on Form 8-K, and amendments to those reports free of charge as soon as reasonably practicable after we electronically file such material with the Securities and Exchange Commission (SEC). Our Internet address is www.scmmicro.com. The content on our website is not, nor should be deemed to be, incorporated by reference into this Annual Report on Form 10-K.

ITEM 1A. *RISK FACTORS*

Our business and results of operations are subject to numerous risks, uncertainties and other factors that you should be aware of, some of which are described below. The risks, uncertainties and other factors described in the following risk factors described below are not the only ones facing our company. Additional risks, uncertainties and other factors not presently known to us or that we currently deem immaterial may also impair our business operations. Any of the risks, uncertainties and other factors could have a materially adverse effect on our business, financial condition, results of operations, cash flows or product market share and could cause the trading price of our common stock to decline substantially.

We have incurred operating losses and may not achieve profitability.

We have a history of losses with an accumulated deficit of $192.1 million as of December 31, 2007. In the future, we may not be able to achieve expected results, we may continue to incur losses and we may be unable to achieve or maintain profitability.

Our quarterly and annual operating results will likely fluctuate.

Our quarterly and annual operating results have varied greatly in the past and will likely vary greatly in the future depending upon a number of factors. Many of these factors are beyond our control. Our revenues, gross profit and operating results may fluctuate significantly from quarter to quarter due to, among other things:

- business and economic conditions overall and in our markets;
- the timing and amount of orders we receive from our customers that may be tied to budgetary cycles, seasonal demand, product plans or program roll-out schedules;
- cancellations or delays of customer product orders, or the loss of a significant customer;
- our ability to obtain an adequate supply of components on a timely basis;
- poor quality in the supply of our components;
- delays in the manufacture of our products;
- the absence of significant backlog in our business;
- our inventory levels;

our customer and distributor inventory levels and product returns;

competition;

new product announcements or introductions;

our ability to develop, introduce and market new products and product enhancements on a timely basis, if at all;

our ability to successfully market and sell products into new geographic or market segments;

Table of Contents

- the sales volume, product configuration and mix of products that we sell;
- technological changes in the markets for our products;
- the rate of adoption of industry-wide standards;
- reductions in the average selling prices that we are able to charge due to competition or other factors;
- strategic acquisitions, sales and dispositions;
- fluctuations in the value of foreign currencies against the U.S. dollar;
- the timing and amount of marketing and research and development expenditures;
- loss of key personnel; and
- costs related to events such as dispositions, organizational restructuring, headcount reductions, litigation or write-off of investments.

Due to these and other factors, our revenues may not increase or even remain at their current levels. Because a majority of our operating expenses are fixed, a small variation in our revenues can cause significant variations in our operational results from quarter to quarter and our operating results may vary significantly in future periods. Therefore, our historical results may not be a reliable indicator of our future performance.

It is difficult to estimate operating results prior to the end of a quarter.

We do not typically maintain a significant level of backlog. As a result, rev