ZIX CORP
Form 10-K
March 15, 2010

**United States**
**SECURITIES AND EXCHANGE COMMISSION**
**Washington, D.C. 20549**

**Form 10-K**

(Mark One)

þ **ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**
**For the fiscal year ended December 31, 2009**

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: 0-17995**

**Zix Corporation**
*(Exact Name of Registrant as Specified in its Charter)*

| **Texas** | **75-2216818** |
|---|---|
| *(State or Other Jurisdiction of Incorporation or Organization)* | *(I.R.S. Employer Identification Number)* |

**2711 N. Haskell Avenue, Suite 2200, LB 36, Dallas, Texas 75204-2960**
*(Address of Principal Executive Offices)*
**(214) 370-2000**
*(Registrant s Telephone Number, Including Area Code)*
**Securities Registered Pursuant to Section 12(b) of the Act:**

| *Common Stock $0.01 Par Value* | *NASDAQ* |
|---|---|

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

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

Indicate by check mark if disclosure of delinquent filers pursuant to Item 405 of Regulation S-K (§229.405 of this chapter) is not contained herein, and will not be contained, to the best of Registrant s knowledge, in definitive proxy or information statements incorporated by reference in Part III of this Form 10-K or any amendment to this Form 10-K. o

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 definitions of large accelerated filer , accelerated filer and smaller reporting

company in Rule 12b-2 of the Exchange Act. (Check one):

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

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

As of March 5, 2010, there were 63,887,125 shares of Zix Corporation $0.01 par value common stock outstanding. As of June 30, 2009, the aggregate market value of the shares of Zix Corporation common stock held by non-affiliates was $93,883,611.

DOCUMENTS INCORPORATED BY REFERENCE

Portions of the Registrant s 2010 Proxy Statement are incorporated by reference into Part III of this Form 10-K.

**TABLE OF CONTENTS**

**PART I**
Item 1. Business 3
Item 1A. Risk Factors 9
Item 1B. Unresolved Staff Comments 16
Item 2. Properties 16
Item 3. Legal Proceedings 16
Item 4. (Removed and Reserved) 16
**PART II**
Item 5. Market for Registrant s Common Equity, Related Stockholder Matters and Issuer Purchases of Equity Securities 17
Item 6. Selected Financial Data 18
Item 7. Management s Discussion and Analysis of Financial Condition and Results of Operations 19
Item 7A. Quantitative and Qualitative Disclosures About Market Risk 31
Item 8. Financial Statements and Supplementary Data 31
Item 9. Changes in and Disagreements with Accountants on Accounting and Financial Disclosure 31
Item 9A. Controls and Procedures 31
Item 9B. Other Information 34
**PART III**
Item 10. Directors, Executive Officers and Corporate Governance 35
Item 11. Executive Compensation 35
Item 12. Security Ownership of Certain Beneficial Owners and Management and Related Stockholder Matters 35
Item 13. Certain Relationships and Related Transactions, and Director Independence 35
Item 14. Principal Accountant Fees and Services 35
**PART IV**
Item 15. Exhibits and Financial Statement Schedules 35

## PART I

**Item 1.** ***Business***

Zix Corporation s ( ZixCorp® the Company, we, our, or us ) focus is the operation of an Email Encryption Servi ZixCorp s Email Encryption Service enables the use of secure email for sensitive information exchange primarily in the healthcare, financial services, insurance, and government sectors. For 2009 we operated two reporting segments, Email Encryption and e-Prescribing (see Note 3 to the consolidated financial statements). Specific to our e-Prescribing business, we announced on June 11, 2009, that we had retained Allen & Company LLC to assist our Board of Directors in investigating strategic alternatives ( Strategic Review ) for maximizing value of this business segment. Based on the Strategic Review we announced on December 8, 2009, our intention to exit the e-prescribing business. After fulfilling our customer and partner obligations, we are targeting December 31, 2010, as the official termination date for this business.

The business operations and service offerings are supported by the ZixData Center , a network operations center dedicated to secure electronic transaction processing. The operations of the ZixData Center are independently audited annually to maintain AICPA SysTrust certification in the areas of security, confidentiality, integrity and availability. Auditors also produce a SAS70 Type II report on the effectiveness of operational controls used over the audit period. The center is staffed 24 hours a day with a proven 99.99% reliability. Whether it is delivery of email, prescriptions or other sensitive information, we enable communications to be sent in a trusted, safe, and secure manner. This is ZixCorp s core competency and we believe it is a competitive advantage.

Our Email Encryption Service is a comprehensive secure messaging service, which allows an enterprise to use policy-driven rules to determine which emails should be sent securely to comply with regulations or corporate policy. It is primarily offered as a Software-as-a-Service ( SaaS ) solution, for which customers pay an annual service subscription fee. ZixCorp s main differentiation in the marketplace is our focus on the transparent delivery of secure, encrypted email. Most email encryption solutions are focused on the sender. They typically introduce an added burden on receivers, often requiring additional user authentication with creation of a new user identity and password. We designed our solution to alleviate the receiver s burden by enabling the delivery of encrypted email automatically and transparently. ZixCorp offers transparent delivery as a result of (1) our ZixDirectory®, which is designed to share identities, (2) Zix s Best Method of Delivery, which is designed to deliver email according to the sender s encryption policy and (3) ZixGateway (formerly ZixVPM®), which is an enterprise gateway that automatically decrypts the message. The result is secure encrypted email exchange that s transparent for both sender and receiver.

e-Prescribing consists of a single product line named PocketScript®, which is an electronic prescribing service that allows physicians to use a handheld device to prescribe drugs and transmit the prescription electronically to virtually any pharmacy. Our Email business is profitable; however, the e-Prescribing business has continued to consume cash, and we plan to exit this business at the end of 2010.

**Business Segments**

***Email Encryption***

*Segment Overview:* Email is a mission-critical means of communication for enterprises. However, if email leaves a secure network environment in clear text, it can be intercepted along the path between a sender and a recipient, which permits theft, redirection, manipulation, or exposure to unauthorized parties. Failure to control and manage such risks can result in enforcement penalties for noncompliance under numerous different regulations. Healthcare organizations are primarily concerned with the recent changes to the Health Information Portability Accountability Act (HIPAA) introduced via the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009. Financial institutions are concerned with Gramm-Leach-Bliley Act ( GLBA ). In addition, individual states such as Massachusetts and Nevada have recently introduced state laws regulating email encryption. Failure to manage the risks associated with email can also lead to decreased productivity, damaged reputation, competitive disadvantage, a loss of intellectual property or other corporate assets, exposure to negligence or liability claims, and diversion of resources to repair such damage.

Corporations require email protection that can be used on an enterprise-wide basis, is cost-effective, quickly deployed, regularly updated to guard against obsolescence and ineffectiveness, and is easy to use. To satisfy these

needs, our Email Encryption Service provides a comprehensive solution that analyzes and encrypts email communications.

Our Email Encryption Service provides a user the ability to deliver encrypted email to any email user at any email address by using the ZixCorp Best Method of Delivery protocol that automatically determines the most direct and appropriate means of delivery, based on the sender s and recipient s communications environment and preferences. The service supports a number of encrypted email delivery mechanisms, including S/MIME, TLS, OpenPGP, push delivery and secure portal pull delivery. These last two mechanisms enable users to send messages instantly and securely to anyone with an email address, including those who do not have an encryption tool. Our Best Method of Delivery makes the technology simple for end users and provides flexibility and ease of implementation for information technology professionals. We believe the ability to send messages through different modes of delivery makes our Email Encryption Service superior to competitive offerings.

The deployment of our Email Encryption Service at the periphery of the customer s network means our Email Encryption Service encrypts email for an enterprise s customers and business partners without the need to create, deploy or manage end user encryption keys or deploy desktop software. Our technology solutions are user friendly, easy to deploy, and can be made operational quickly.

Our service has an integrated policy management capability. This policy engine can inspect the contents of outbound emails and apply policies that match specific industry criteria such as HIPAA and GLBA. Customers can also build their own specific policies. This policy driven email for regulatory compliance means customers can reduce the training required of their staff.

Our Email Encryption Service employs a centralized directory of users called the ZixDirectory, which we consider a key differentiator of our offering. The ZixDirectory operates as a global community for email encryption, and today contains over 20 million user email addresses. The ZixDirectory has recently grown at a rate of over 100,000 new members per week. Access to these email addresses and encryption codes in the ZixDirectory greatly improves ease of use for both senders and receivers of secure email, while affording them the option of strong encryption methods, extended feature sets and the flexibility of a variety of fully integrated and fully interoperable solutions.

Today in healthcare, our Email Encryption Service is used by over thirty Blue Cross Blue Shield organizations and over 1,000 hospitals. In the financial services sector, we serve over 1,200 banks, credit unions and farm credit associations, as well as all of the Federal Financial Institutions Examination Council ( FFIEC ) regulators. We also provide service to more than twenty-five state governments covering various state agencies in those states.

*Competition:* Our service differs from the products and services of our competitors since we offer a SaaS offering, while most of our competitors offer primarily a product-based approach that the customer builds and runs themselves. Some of these competing companies have substantial information technology security and email protection products; however, we believe that the ZixDirectory provided through our subscription SaaS architecture offers many advantages in the marketplace. Specifically, the ZixDirectory allows the sharing of user identities for encryption and interoperability between users in a community of interest within healthcare, finance or government. Our competitors customers tend to build and operate their own systems, and the directory of user identities each competitor creates is not shared. This practice has become less desirable as different companies encrypted email systems are not interoperable.

Our capability to offer interoperability is particularly important when it is necessary to communicate with external networks, as is the case with the healthcare and financial services markets. Our customers become part of the ZixDirectory, a global white pages that enables transparent secure communications with other ZixGateway customers using our centralized key management system and overall unique approach to implementing secure e-messaging technology. We enable secure communications with other users via our push and secure portal delivery mechanisms. However, we believe our unique transparent delivery is the more preferred delivery model.

Our Email Encryption Service focuses on the secure (encryption) delivery portion of the secure email market, a sub-segment of the e-messaging market. We have been listed as an industry leader in a prominent study that compared eight qualified email encryption vendors. Companies operating in this portion of the market include

IronPort (acquired by Cisco Systems Inc.), PGP Corporation, Proofpoint, Trend Micro, Voltage Security, Secure Computing (acquired by McAfee, Inc.), Echoworx, Sigaba Corporation (acquired by Proofpoint), Certified Mail, Authentica (acquired by EMC Corporation, and Tumbleweed Communications Corp. (acquired by Axway). Technically, while these companies offer send-to-anyone encrypted email, we believe they are unable to offer the benefits that come from access to the ZixDirectory and from using our Best Method of Delivery protocol. Nevertheless, some of these competitors are large enterprises with substantial financial and technical resources that exceed those we possess.

***e-Prescribing***

*Segment Overview:* On December 8, 2009, the Company filed a Current Report on Form 8-K disclosing the decision by the Company s Board of Directors to exit the e-Prescribing business by winding down its operations while servicing existing contractual obligations to current customers. The Company has targeted December 31, 2010, as the official termination date for this business, due in large measure to the expiration of ongoing contractual commitments by that date.

We continue to believe e-Prescribing delivers many benefits, including improved patient safety through alerts to potential adverse drug or allergy interactions, reduced calls from the pharmacy to the physician, reduced costs for patients and their insurers through increased prescribing within drug formulary guidelines, increased delivery of prescribed drugs via mail order and reduced prescribing errors. Our e-Prescribing application not only delivered the foregoing benefits, but it could also be used as a technology platform to deliver related products and additional point-of-care services to improve the efficiency and effectiveness of physicians by providing greater access to information and other decision making support tools. However, after investing in the development of this business for six years, we decided that the rate of growth, the need for continued investment of time and resources, and the uncertainty surrounding the overall evolution of the e-Prescribing market did not warrant the risk associated with continued investment in this business and that focusing more resources on our Email Encryption business was likely to deliver greater returns to our shareholders.

We design and develop our e-Prescribing solution and have historically distributed it directly to physicians and healthcare institutions through payor relationships. We have entered into sponsorship programs whereby large health insurance companies (payors), have agreed to provide the e-Prescribing devices for various periods of time to associated physicians. In the past, ZixCorp generally sold this as an annual service with an initial set-up and hardware charge. Typically, the third-party sponsors agreed to pay for at least most of the initial set-up costs and first year of service, because they have a vested benefit in the cost savings associated with use of this technology.

Because we have committed to fulfill our contractual commitments through the end of 2010, we have retained sufficient personnel to operate our e-Prescribing service. We are also renewing end-users for various time periods, but in no case ending later than the end of 2010, to allow them to continue using the service while they determine what action to take in light of our announced exit from this business. Except in special circumstances, such as a new physician joining a practice that is an existing user of our service, we are not deploying new prescribers in 2010. In some instances, our payor sponsors are continuing to fund prescriber renewal, but generally prescribers pay for their renewal themselves.

***PocketScript®*** PocketScript is our e-Prescribing service. The service works with a handheld wireless Personal Data Assistant or a browser to provide physicians with the ability to write and transmit prescriptions directly to any pharmacy. In addition, providers can view available patient drug histories obtained from third parties for the purpose of confirming that prescriptions are being filled and safeguarding against duplication of therapies. The system also identifies generics and preferred drugs for multiple formularies enabling providers to choose the most appropriate option. The comprehensive prescription drug database, which PocketScript provides under license from a third party, provides information on virtually every drug available, including drug-to-drug interactions, drug-allergy interactions and a drug reference guide. In association with various PocketScript abilities, we sell and market certain transaction-based offerings to various customers.

*Competition:* In general, our e-Prescribing Service competes in a less developed market than our Email Encryption Service. However, because of recent advances in healthcare technology, advances in handheld

computing, and the civic and legislative mandates to reduce healthcare costs and increase patient safety, this market is seeing increases in competitive activity.

We have several competitors. These include AllScripts-Misys Healthcare Solutions, Dr. First, Inc., iScribe, Prematics, and RxNT. Many of the competitors in this market also focus on other technologies such as electronic health records and practice management solutions, or they act as application service providers in the healthcare market.

Companies that do not currently compete in the e-Prescribing market or only compete with selected products or in selected markets could become competitors to the current industry participants in the future on a larger scale. Companies such as GE Healthcare or McKesson Corporation would likely offer a broad portfolio of health information technologies for all or some of the pharmaceutical, pharmacy, healthcare provider and managed care markets. With considerable size and access to capital, they could become significant competitors. Favorable legislative developments (see **Regulatory Drivers** below) may make their entry into the market more likely.

**Regulatory Drivers**

*Email Encryption Service:* We have been successful in securing additional market penetration for our Email Encryption Service in our target vertical markets of healthcare, finance services and government markets. There was a significant increase in demand in the healthcare sector leading up to the April 2005 HIPAA Security Rule deadline and sales in this sector have remained generally strong since that time. The HITECH Act within the American Recovery and Reinvestment Act of 2009, also known as the stimulus package, contains an expansion of the HIPAA laws that went into effect following the February 17, 2009, passage of the law. Key elements of the HITECH Act relating to HIPAA include increased penalties for violations, stricter and more onerous breach notification requirements, broadening the reach of the law to include previously uncovered business associates, and the ability for states to pursue HIPAA violations in addition to the U.S Department of Health and Human Services ( HHS ). The Company believes these changes will increase demand for email encryption by broadening the potential market and providing further incentive for potential customers to adopt email encryption technology.

Additional federal regulations, such as GLBA, and state regulations across the country have enhanced security awareness in vertical markets outside of healthcare, and have prompted affected organizations to consider adopting systems that ensure data security and privacy.

Recently state governments have begun to focus increasingly on encryption. The first of the email encryption state laws was passed by Nevada on October 1, 2008. On March 1, 2010, the state of Massachusetts began enforcing its new regulations as well (201 CMR 17.00). The Massachusetts regulations will be the most comprehensive encryption requirements imposed on businesses by any state and, because it covers any business with a customer or business dealing in the state of Massachusetts, it reaches far beyond its own state borders.

Even where there are no specific regulations, corporations may demand email protection to adhere to evolving industry best practices for protecting sensitive information. In 2003 we responded to these trends by expanding our focus beyond healthcare into other vertical markets including financial services, insurance and government. As part of the strategy to penetrate the financial services sector, we targeted the relevant regulators who themselves were placing an increased emphasis on the secure transmission of sensitive information. We currently have all of the federal regulators who comprise the FFIEC as customers and our service is a recommended solution of the Conference of State Bank Supervisors, whose members regulate the more than 6,000 state-chartered banks in the U.S. We also currently have the state banking regulators in more than twenty states as customers.

*e-Prescribing Service:* In the Medicare Prescription Drug and Modernization Act of 2004, e-prescribing is specifically addressed in Section 1860D-4 and also in the subsequent final rule on the Medicare Prescription Drug Benefit, which states that Part D sponsors that participate in the Part D program are required to support and comply with electronic prescribing standards. In January 2006 the initial Foundation Standards for e-prescribing went into effect, with Final Standards to be issued after additional standards are tested.

In 2008 the U.S. Congress passed the Medicare Improvements for Patients and Providers Act of 2008 ( MIPPA ). MIPPA authorized a new and separate incentive program for eligible professionals who are successful

electronic prescribers ( e-Prescribers ), as defined by MIPPA. During the beginning years of the program, physicians who are e-Prescribers will be paid bonuses (which could be earned beginning in 2009). In the later years of the program, penalties will be assessed on physicians for non-use of e-prescribing.

The HITECH Act also contains economic incentives for the adoption of health information technologies, including certified electronic health record systems ( EHRs ) that contain an e-prescribing component. Similar to MIPPA, the incentives take the form of bonuses starting in 2011, followed by penalties for non-use beginning in 2015. Throughout the course of 2009, the terms of these bonuses and penalties were analyzed by statutory committees set up for this purpose, who submitted recommendations to HHS for their definition. The terms were defined in interim rulings by HHS published in December 2009, although the process for certification itself remains undefined. While e-prescribing ultimately remained a core requirement of a certified EHR system, the ongoing uncertainties occurring in the regulatory environment factored into the strategic review of our e-Prescribing segment, and by the time these definitions were published, the Company had already announced its intentions to exit the e-Prescribing business.

**Sales and Marketing**

We primarily sell our Email Encryption Service through a direct sales force that focuses on larger businesses and a telesales force that focuses on small to medium-sized accounts. We also use a network of resellers and other distribution partners, particularly other service providers seeking an encryption offering in an Original Equipment Manufacturing ( OEM )-like relationship. In 2005 we began a program to place greater emphasis on these distribution channels, with the expectation that they will become a more significant source of revenues in the future. In 2009, 12% of our new first-year Email Encryption sales came from these OEM partners. Our partners include Google Inc., MessageLabs, Inc. (acquired by Symantec), SecureWorks, Inc., Webroot, M86 Security, and Code Green Networks.

Prior to 2003, the healthcare market had been our highest selling and marketing priority, given the legislative requirements of HIPAA. In 2009, nearly one half of our new first-year orders still came from healthcare. Since late 2003 we have expanded our Email Encryption Service sales and marketing efforts to include the financial services, insurance and government sectors, with the financial services sector becoming a second core customer segment for us. In 2009 about one-third of the new first year orders came from the financial services sector.

For e-Prescribing, we have not emphasized sales directly to physicians but rather have focused on other stakeholders that benefit from healthcare technology. Because of the potential savings resulting from lower drug spend and improved patient safety, we have historically partnered with health insurance companies who have underwritten the deployment and initial subscription costs of the service for the physicians. Following our December 2009 announcement of our intent to exit the e-prescribing business, we are no longer attempting to secure sales to new customers. However, we are committed to fulfilling our contractual commitments through the end of 2010 and are also renewing end-users for service during this period. In some instances, our payor sponsors are continuing to fund these prescriber renewals, but generally we contract with the physicians to pay for their renewal themselves.

**Employees**

We had 136 employees as of December 31, 2009, with 83 employees categorized under the Email Encryption segment, 27 employees categorized under the e-Prescribing segment, and 26 employees categorized as Corporate. Five full-time equivalent resources were shared resources across both categories. Thirteen employees categorized under the e-Prescribing segment departed the Company in January 2010. The majority of our employees are located in Dallas, Texas; Burlington, Massachusetts; and Ottawa, Ontario, Canada.

**Research and Development Patents and Trademarks**

We incurred research and development expenses of $6,948,000, $6,158,000, and $5,322,000 for the twelve-month periods ended December 31, 2009, 2008 and 2007, respectively.

In 2009 Email Encryption technology developments included foundation work to enable foreign language content transparency and multi-language command flexibility across several of our core systems. We designed a

number of service environments for new partners and product features; some of which are intended to enable new business by building on the 2008 introduction of our data center in the United Kingdom. We implemented design improvements to reduce special customer network configurations related to our ZixGateway deployments; to improve alignment with our customers network and application security designs and to increase the rate and capacity of deployments for hosted ZixGateway, ZixPort® and ZixDirect services. We also continued to make investments to strengthen our feature and service suite, including delivery of a new customer-facing reporting capability and an upgrade of our Email Encryption audit software aimed at significantly increasing both efficiency and integrity.

In the e-Prescribing technology area, we implemented major enhancements to formulary and benefits presentation and general prescriber workflows including improvements related to the prescription renewal function, additional functional flexibilities within the controlled substance prescribing process and new features to strengthen the protection of patient privacy. With our decision to make 2010 our final year of PocketScript operation, the above changes have positioned us to place the service into a steady operating state with relative containment of the risk that compliance gaps or requirements might mandate new core feature development.

We have patents that protect certain elements of our core technology underlying the Email Encryption business. We have not realized any revenues from licensing any of our patents to third parties. We received four new U.S. patents in 2009, all pertaining to our Email Encryption business.

The following are registered trademarks of ours and certain of our subsidiaries: ZixCorp, ZixVPM, ZixGateway, ZixDirectory, ZixIt, ZixPort, and PocketScript.

**Compliance with Environmental Regulations**

We have not incurred, and do not expect to incur, any material expenditures or obligations related to environmental compliance issues.

**Governmental Contracts**

While we do have many contracts with state and federal regulators, we do not have a material portion of our revenue related to contracts with governmental agencies. However, we believe that sales to certain of these high profile regulators lends additional credibility to our brand, and the loss of this business could influence some of our existing and potential Email customers to consider purchasing other encryption solutions besides our own.

**Significant Customers**

In 2009, 2008 and in 2007 no single customer accounted for 10% or more of our total revenues.

**Backlog**

Our end user order backlog is comprised of contractual commitments that we expect to amortize into revenue in the future. Backlog consists of the following at December 31, 2009 and 2008:

| | December 31, 2009 | December 31, 2008 |
|---|---|---|
| Email Encryption | $ 42,901,000 | $ 34,728,000 |
| e-Prescribing | 1,399,000 | 2,661,000 |
| Total backlog | $ 44,300,000 | $ 37,389,000 |

As of December 31, 2009, our backlog is comprised of the following elements: $17,299,000 of deferred revenue that has been billed and paid, $4,746,000 billed but unpaid net, and approximately $22,255,000 of unbilled contracts. The backlog is recognized into revenue as the services are performed. Approximately 60% of the total backlog is expected to be recognized as revenue during 2010. The timing of revenue is affected by both the length of time required to deploy a service and the length of the service contract.

**Seasonality**

Our experience has shown the third quarter can be a slow time for Email Encryption bookings. We believe this trend is the result of typical vacation schedules. Historically we have seen minimal seasonality in e-Prescribing relative to our bookings; however, we expect volume to decrease throughout 2010 as the PocketScript business winds down.

**Geographic Information**

Our operations are primarily based in the U.S., with approximately 8% of employees located in Canada. Except for a United Kingdom based data center to support customers of our OEM resellers, we do not operate in, or have dependencies on, any other foreign countries. Our revenues and orders to-date are almost entirely sourced in the U.S. and all significant corporate assets at December 31, 2009, were located in the U.S.

**Available Information**

Our business involves risks and uncertainties, and there are no assurances that we will be successful in our efforts. See Item 1A. Risk Factors and Item 7. Management s Discussion and Analysis of Financial Condition and Results of Operations below for a description of certain management assumptions, risks and uncertainties relating to our operations.

We were incorporated in Texas in 1988. Originally named Amtech Corporation, in 1999 we changed our name to ZixIt Corporation at the time we entered the encrypted email market. In 2002 we became Zix Corporation, our current name. We entered the e-prescribing market in 2003, and on December 8, 2009, announced our plan to exit from this market. We are currently targeting December 31, 2010, as the termination date for our e-Prescribing business. Our executive offices are located at 2711 North Haskell Avenue, Suite 2200, LB 36, Dallas, Texas 75204-2960, (214) 370-2000.

We file annual, quarterly, current and other reports, proxy statements and other information with the Securities and Exchange Commission (the SEC ), pursuant to the Securities Exchange Act of 1934, as amended (the Exchange Act ). You may read and copy any materials we file with the SEC at the SEC s Public Reference Room at 450 Fifth Street, N.W., Washington, D.C. 20549. You may obtain information on the operation of the SEC s Public Reference Room by calling the SEC at 1-800-SEC-0330. The SEC maintains a Web site that contains reports, proxy and other information statements, and other information regarding issuers, including us, that file electronically with the SEC. The address of the Web site is *www.sec.gov*.

Our Internet address is *www.zixcorp.com.* Information contained on our Web site is not part of this report. We make available free of charge through this site, under the heading Financial Reports, our Annual Report on Form 10-K, Quarterly Reports on Form 10-Q, Current Reports on Form 8-K, and amendments to those reports filed or furnished pursuant to Section 13(a) or 15(d) of the Exchange Act as soon as reasonably practicable after we electronically file such material with, or furnish it to, the SEC.

**Item 1A.** ***Risk Factors***

Statements in this report, or in our news releases, websites, public filings, investor and analyst conferences or elsewhere, which are not purely historical facts or which necessarily depend upon future events, including statements about trends, uncertainties, hopes, beliefs, anticipations, expectations, plans, intentions or strategies for the future, may be forward-looking statements within the meaning of Section 21E of the Securities Exchange Act of 1934. Forward-looking statements involve risks and uncertainties that could cause actual events or results to differ materially from the events or results described in the forward-looking statements, including risks and uncertainties described below in Item 1A. *Risk Factors*. Readers are cautioned not to place undue reliance on forward-looking statements. All forward-looking statements are based upon information available to us on the date the statements are made. We undertake no obligation to publicly update or revise any forward-looking statements, whether as a result of new information, future events or otherwise.

Risks associated with an investment in our securities, with our business and with our achieving any forward-looking statements, include the risk factors described below. Any of these risk factors could have a material adverse effect on our business, financial condition or financial results and reduce the value of an investment in our securities. We may not succeed in addressing these and other risks.

**Our Email Encryption business depends upon customers using email to exchange confidential information, and a significant shift of those messages to other communication channels could impair our growth prospects and negatively affect our business, financial condition and financial results.**

Our Email Encryption customers deploy and use our products and services to easily, securely and confidentially send and receive encrypted email messages. Our Email Encryption business and revenue substantially depend on our current and potential customers using email to exchange sensitive information electronically. New technologies or products, or new business models that could support secure communications, could be disruptive to our business. If prospective or current customers were to send and receive sensitive information using technology or communication channels other than ours, our growth prospects and our business, financial condition and financial results could be materially adversely affected.

**Public key cryptography technology used in our businesses is subject to technology integrity risks that could reduce demand for our products and services and could negatively affect our business, financial condition and financial results.**

Our Email Encryption and e-Prescribing businesses employ public key cryptography technology and other encryption technologies to encrypt and decrypt messages. The security afforded by encryption depends on the integrity of the private key, which is predicated on the assumption that it is very difficult to mathematically derive the private key from the related public key. Public reports of the successful decryption of encrypted messages or encrypted information could reduce demand for our products and services. If new methods or technologies make it easier to derive the private key from the related public key, the security of encryption services using public key cryptography technology could be impaired and our products and services could become unmarketable. That could require us to make significant changes to our services, which could increase our costs, damage our reputation, or otherwise harm our business. Any of these events could reduce our revenues and materially adversely affect our business, financial condition and financial results.

**The growth of our business may require significant investment in systems and infrastructure with no guarantee of revenue, which could impair our profitability and negatively affect our business, financial condition and financial results.**

As our operations grow in size and scope, we may need to improve and upgrade our systems and infrastructure to offer an increasing number of customers enhanced products, services, features and functionality, while maintaining the reliability and integrity of our systems and infrastructure and pursuing reduced costs per transaction. Expanding our systems and infrastructure may require us to commit substantial financial, operational and technical resources , with no assurance that the volume of business will increase, which could reduce our net income, deplete our cash, and materially adversely affect our business, financial condition and financial results.

**We face strong and increasing competition, which could negatively affect our business, financial condition and financial results.**

The markets for our products and services are very competitive. With rising demand for private and secure email communications, there is increasing competition to provide email encryption products and services. Our Email Encryption business competes with products and services offered by companies such as Axway, Cisco Systems Inc., DataMotion, Echoworx, EMC Corporation, McAfee, Inc., PGP Corporation, Proofpoint, Trend Micro and Voltage Security. Increased competition requires us to develop new technology solutions and service offerings to expand the functionality and value that we offer to our customers. Some of our competitors offer email encryption services together with products and services that we do not offer, which could make our offering less attractive by comparison. Our competitors may develop technology solutions and service offerings that are perceived by

customers as equivalent to, or having advantages over, our products and services. Competitors could capture a significant share in our markets, causing our sales and revenue to decline or grow more slowly. Competitive pressures could lead to price discounting or to increases in expenses such as advertising and marketing costs. Increased competition could also decrease demand for our products and services. Competition could reduce our revenues and net income and materially adversely affect our business, financial condition and financial results.

**Some competitors have advantages that may allow them to compete more effectively than us, which could negatively affect our business, financial condition and financial results.**

Some of our competitors have longer operating histories, more extensive operations, greater name recognition, larger technical staffs, bigger product development and acquisition budgets, established relationships with more distributors and hardware vendors, and greater financial and marketing resources than we do. These resource advantages might enable them (independently or through alliances) to develop and expand functionality of products and services faster than we can, to spend more money to market and distribute products and services than we can, or to offer their products and services at prices lower than ours. These advantages could reduce our revenues and net income and materially adversely affect our business, financial condition and financial results.

**We plan to increasingly rely on third party distributors to help us market our Email Encryption products and services, and our failure to succeed in those relationships could negatively affect our business, financial condition and financial results.**

We plan to increase the distribution of our Email Encryption products and services by entering into alliances with third parties who can offer our products and services along with their own products and services. Increased reliance on third parties to market and distribute our products and services exposes us to a variety of risks. For example, we have limited control over the timing of the delivery of our products to customers by third-party distributors, which could increase the length of our sales cycle, cause our revenue to fluctuate unpredictably and make it difficult to accurately forecast our revenue. We may not succeed in developing or maintaining marketing alliances. Companies with which we have marketing alliances may in the future discontinue their relationships with us, form marketing alliances with our competitors, or develop and market their own products and services that compete with ours. If a significant distributor were to discontinue its relationship with us, we could experience a interruption in the distribution of our products and services and our revenues could decline. Our failure to develop, maintain and expand strategic distribution relationships could reduce our revenues and net income and materially adversely affect our business, financial condition and financial results.

**Our business substantially depends on market acceptance of our Email Encryption service, and our failure to achieve market penetration could negatively affect our business, financial condition and financial results.**

Our revenue and financial results are increasingly dependent on our Email Encryption business. In order to operate profitably, we must achieve broad market acceptance of our Email Encryption service at a price that provides an acceptable rate of return relative to our costs. We have been successful in selling our products and services to various high-profile customers, particularly in the healthcare, financial services and government segments of our market. The acceptance and use of our Email Encryption products and services by those significant customers facilitates our sales to potential customers, and an expanding base of users in the Zix Directory aids in our market penetration and expansion. We must continue to respond to evolving business models for technology offerings in order to achieve market acceptance. The loss of an influential customer could impair our ability to expand the market penetration of our products and services, or cause us to reduce prices, which could reduce our revenues and net income and materially adversely affect our business, financial condition and financial results.

**Unfavorable economic and political environments could negatively affect our business, financial condition and financial results.**

Adverse economic conditions in markets in which we operate can harm our business. If economic growth in those markets is slow, or credit is unavailable at a reasonable cost, current and potential customers may delay or reduce technology purchases, including the deployment or expansion of our Email Encryption products and services.

This could result in reduced sales of our products and services, longer sales cycles, slower adoption of new technologies and increased price competition. In addition, adverse economic conditions could negatively affect the cash flow of our customers and distributors, which might result in failures or delays in payments to us. This could increase our credit risk exposure and delay our recognition of revenue. If these conditions remain uncertain or persist, spread or deteriorate further, our business, financial condition and financial results could be materially adversely affected.

**Our failure to keep pace with rapid technology changes could have a negative impact on our business, financial condition and financial results.**

The markets for our products and services are characterized by rapid technological developments and frequent changes in customer requirements. We must continually improve the performance, features and reliability of our products and services, particularly in response to competitive offerings. We must ensure that our products and services address evolving operating environments, industry trends, certifications and standards. For example we must expand our offerings for virtual computer environments and mobile environments to support a broader range of mobile devices. We also must develop products that are compatible with new operating systems while remaining compatible with existing, popular operating systems. Our business could be harmed by our competitors announcing or introducing new products and services that could be perceived by customers as superior to ours. We spend considerable resources on technology research and development, but our research and development resources are more limited than many of our competitors. Unforeseen requirements in our e-Prescribing business could cause us to divert resources from our Email Encryption business. Our business substantially depends on our ability to keep pace with rapid technological and market changes and we may be unable to introduce new or enhanced products into the market on a timely basis, or at all. Our enhancements to existing products and services, or our potential new products and services, may not receive customer acceptance. Our failure to introduce new or enhanced products on a timely basis, to keep pace with rapid industry, technological or market changes or to gain customer acceptance for our products and services could have a material adverse effect on our business, financial condition and financial results.

**If our products do not work properly, our business, financial condition and financial results could be negatively affected.**

We produce complex products that incorporate leading-edge technology, including both hardware and software, that must operate in a wide variety of technology environments. Software may contain defects or bugs that can interfere with expected operations. There can be no assurance that our testing programs will be adequate to detect all defects, which might decrease customer satisfaction with our products and services. The product reengineering cost to remedy a product defect could be material to our operating results. Defects or errors in our PocketScript system could cause us to divert resources from our Email Encryption business and could result in inaccurate prescriptions being generated, which could result in injury or death to patients. Our inability to cure a product defect could result in the temporary or permanent withdrawal of a product or service, negative publicity, damage to our reputation, failure to achieve market acceptance, lost revenue and increased expense, any of which could have a material adverse effect on our business, financial condition and financial results.

**The infrastructure supporting our Email Encryption business may suffer capacity constraints and business interruptions that could cause us to lose customers, increase our operating costs and could negatively affect our business, financial condition and financial results.**

Our business depends on our providing our customers reliable, real-time access to our data centers and networks. Customers will not tolerate a service hampered by slow delivery times, unreliable service levels, service outages, or insufficient capacity. System capacity limits or constraints arising from unexpected increases in our volume of business could cause interruptions, outages or delays in our services, or deterioration in their performance, or could impair our ability to process transactions. We may not be able to accurately project the rate of increase in usage of our network or to timely increase capacity to accommodate increased traffic on our network. System delays or interruptions may prevent us from efficiently providing services to our customers or other third parties, which could result in our losing customers and revenues, or incurring liabilities that could have a material adverse effect on our business, financial condition and financial results.

**Our Email Encryption business depends substantially on our data center facilities, and their unreliability or unavailability for a significant period could cause us to lose customers and could negatively affect our business, financial condition and financial results.**

Much of the computer and communications hardware upon which our businesses depend is located in our data center facilities in Dallas and Austin, Texas and in the United Kingdom. Our data centers might be damaged or interrupted by fire, flood, power loss, telecommunications failure, break-ins, earthquakes, terrorist attacks, hostilities or war or other events. Computer viruses, denial of service attacks, physical or electronic break-ins and similar disruptions affecting the internet or our systems might cause service interruptions, delays and loss of critical data, and could prevent us from providing our services. Problems affecting our systems might be expensive to remedy and could significantly diminish our reputation and prevent us from providing services. An incident that interrupts our data center operations or our networks could result in loss of revenues, failure to achieve market acceptance, diversion of resources, injury to our reputation, liability and increased costs. We do not carry sufficient insurance to compensate us for all reasonably conceivable losses that may occur as a result of any of these events. The occurrence of any of these events could materially adversely affect our business, financial condition and financial results.

**Outages or problems with systems and infrastructure supplied by third parties could negatively affect our business, financial condition and financial results.**

Our businesses rely on third-party suppliers of the global telecommunications infrastructure. We use various communications service suppliers and the global internet to provide network access between our data centers, our customers and end-users of our services. If those suppliers do not enable us to provide our customers with reliable, real-time access to our systems, we may be unable to gain or retain customers. These suppliers periodically experience outages or other operational problems. Any of these outages or problems could materially adversely affect our business, financial condition and financial results.

**Problems with enforcing our intellectual property rights or using third party intellectual property could negatively affect our business, financial condition and financial results. Our proprietary rights may be difficult to enforce and may offer limited protection of our intellectual property rights against potential infringers.**

We rely on a combination of contractual rights, trademarks, trade secrets, patents and copyrights to establish and protect proprietary rights in our products and services. These patents or other proprietary rights might be challenged, invalidated or circumvented. The steps we have taken to protect our proprietary information may not prevent its misuse, theft or misappropriation. Competitors may independently develop technologies or products that are substantially equivalent or superior to our products or that inappropriately incorporate our proprietary technology into their products. Some jurisdictions may not provide adequate legal protection of our intellectual property rights.

**We may have to defend our rights in intellectual property that we use in our services, and we could be found to infringe the intellectual property rights of others, which could be disruptive and expensive to our business.**

We may have to defend against claims that we or our customers are infringing the rights of third parties in patents, copyrights, trademarks and other intellectual property. Intellectual property litigation and controversies are disruptive and expensive. Even unmeritorious claims brought against our customers may harm our reputation and customer relationships, and may have to be settled for significant amounts. Infringement claims could require us to develop non-infringing services or enter into expensive royalty or licensing arrangements. Our business, financial condition and financial results could be materially adversely affected if we are not able to develop non-infringing technology or license technology on commercially reasonable terms.

**We may face risks from using open source software that could negatively affect our business, financial condition and financial results.**

Like many other software companies, we may use open source software in order to add functionality to our products quickly and inexpensively. Open source software license terms could adversely affect our intellectual property rights in our products that include open source software. We could lose the right to use the open source code if we fail to comply with the license obligations. Using open source code could also cause us to inadvertently infringe third-party intellectual property rights.

**We may fail to recruit and retain key personnel, which could impair our ability to meet key objectives.**

Our success depends on our ability to attract and retain highly-skilled technical, managerial, sales, and marketing personnel. Changes in key personnel may be disruptive to our business. It could be difficult, time consuming and expensive to replace key personnel. Integrating new key personnel may be difficult and costly. Volatility, lack of positive performance in our stock price or changes to our overall compensation program including our stock incentive program may adversely affect our ability to retain key employees, virtually all of whom are compensated, in part, based on the performance of our stock price. It may take significant time to locate, retain and integrate qualified management personnel, which could negatively affect our business, financial condition and financial results.

**Our usage of personal information, and inadvertent exposure of confidential information, could cause us to violate data privacy laws or lose customers and could negatively affect our business, financial condition and financial results.**

In our Email Encryption and e-Prescribing businesses, we collect, process, store, use and transmit large amounts of personally identifiable information about individuals, such as personal healthcare or financial information. Our handling of these types of data is increasingly subject to regulation around the world. These regulations may result in conflicting requirements. Our business could be materially adversely affected if legal restrictions on the use of personally identifiable information are expanded or are interpreted in ways that conflict with our business practices or increase our costs. Unauthorized disclosure of personal information (including through intrusion by a hacker) or other failure by us to comply with data privacy requirements could subject us to significant penalties, remediation and other expenses, and damage to our reputation, any of which could have a material adverse effect on our business, financial condition and financial results.

**Governmental restrictions on the sale of our products and services in non-U.S. markets could negatively affect our business, financial condition and financial results.**

Exports of software solutions and services using encryption technology, such as our Email Encryption Service, are generally restricted by the U.S. government. Although we have obtained U.S. government approval to export our Email Encryption service to almost all countries, the list of countries to which we cannot export our products and services could be expanded in the future. In addition, some countries impose restrictions on the use of encryption solutions and services such as ours. The cost of compliance with U.S. and other export laws, or our failure to obtain governmental approvals to offer our products and services in non-U.S. markets, could affect our ability to sell our products and services and could impair our international expansion. We face a variety of other legal and compliance risks. If we or our distributors fail to comply with applicable law and regulations, we may become subject to penalties, fines or restrictions that could materially adversely affect our business, financial condition and financial results.

**Our financial performance could be erratic and asset impairments could negatively affect our financial condition and financial results.**

Although we generate adequate cash flow from operations and we expect to be profitable, we may not continue to produce sufficient cash flow or show a profit. We have incurred significant operating losses in past years. Our liquidity and capital resources are limited. We expect our e-Prescribing business will generate sufficient cash to

offset its expenses as we wind it down during 2010, but we could experience a revenue shortfall if our e-Prescribing customers do not renew their contracts as we have planned throughout 2010. Our balance sheet reflects goodwill relating to our Email Encryption business, as well as other assets. We periodically evaluate the carrying value of our goodwill and other assets to determine if their values have been impaired, which could require us to recognize a non-cash charge to earnings. Any of these circumstances could materially adversely affect our business, financial condition and financial results.

**The market price of our securities could be volatile and our securities may decline in value.**

The market price of our common stock has fluctuated significantly in the past and is likely to fluctuate in the future. In addition to stock price volatility related to our business performance, our stock price may fluctuate due to events affecting our industry or our competitors, as well as general economic and political conditions. Any of these circumstances could cause our securities to decline in value.

**Exercises of options and warrants for our common stock would dilute the ownership interests of existing shareholders and could negatively affect the value of our securities.**

We have a significant number of outstanding warrants and options, including options held by our employees. The exercise of warrants or options, and the resulting issuance of additional shares of our common stock, would substantially dilute the ownership interests and voting rights of our current shareholders. Issuance or sales of those additional shares could cause our securities to decline in value.

**Our issuances of additional debt or equity securities could dilute the ownership interests of existing shareholders and could negatively affect the value of our securities.**

We may issue additional debt or equity securities, including convertible debt, common and convertible preferred stock, and warrants to acquire common or preferred stock. Those securities could be issued in public or private transactions, at or below the then-prevailing market price of our securities. In addition, we may grant our employees shares of our common stock and options to purchase those shares. Our issuance of additional securities could substantially dilute the ownership interests and voting rights of our current shareholders. Issuance or sales of those additional shares could cause our securities to decline in value.

**NOTE ON FORWARD-LOOKING STATEMENTS AND RISK FACTORS**

This document contains forward-looking statements (including the discussion appearing under the caption Liquidity Summary in **Item 7.** ***Management s Discussion and Analysis of Financial Condition and Results of Operations,*** on page 34 within the meaning of Section 27A of the Securities Act of 1933, as amended (the Act ) and Section 21E of the Exchange Act. All statements other than statements of historical fact are forward-looking statements for purposes of federal and state securities laws, including: any projections of future business, market share, earnings, revenues, cash receipts, or other financial items; any statements of the plans, strategies, and objectives of management for future operations; any statements concerning proposed new products, services, or developments; any statements regarding future economic conditions or performance; any statements of belief; and any statements of assumptions underlying any of the foregoing. Forward-looking statements may include the words may, will, predict, project, forecast, plan, should, could, goal, estimate, intend, continue, believe, expect, outloo other similar expressions. Such forward-looking statements may be contained in the Risk Factors section above, among other places.

Although we believe that expectations reflected in any of our forward-looking statements are reasonable, actual results could differ materially from those projected or assumed in any of our forward-looking statements. Our future financial condition and results of operations, as well as any forward-looking statements, are subject to change and to inherent risks and uncertainties, such as those disclosed in this document. We do not intend, and undertake no obligation, to update any forward-looking statement.

**Item 1B.** ***Unresolved Staff Comments***

None.

**Item 2.** ***Properties***

During 2009 we leased properties that are considered significant to the operations of the business in the following locations: Burlington, Massachusetts; Ottawa, Ontario, Canada; the United Kingdom; and Dallas and Austin, Texas. The Burlington location is used for Email Encryption sales and marketing activities. The Ottawa office is used for some of our client services and sales support activities for both product lines. The United Kingdom facility is used exclusively for Email Encryption activities and provides data center support for our large OEM partners outside of the U.S. The Dallas office is our headquarters, which includes research & development, marketing, sales and all general administrative services, and the ZixData Center. Our Austin location is used for fail-over and business continuity services and is not used to support normal ongoing operations. Our facilities are suitable for our current needs and are considered adequate to support expected near term growth.

We also had office space in Mason, Ohio. In April 2007 we sublet this office space, the terms of which coincided with our original property lease, which expired in October 2009.

**Item 3.** ***Legal Proceedings***

We are subject to legal proceedings, claims, and litigation arising in the ordinary course of our business. While the outcome of these matters is currently not determinable, we do not expect that the ultimate costs to resolve these matters will have a material adverse effect on our consolidated financial statements.

**Item 4.** ***(Removed and Reserved)***

**PART II**

**Item 5.** ***Market for Registrant s Common Equity, Related Stockholder Matters and Issuer Purchases of Equity Securities***

Our common stock trades on The Nasdaq Stock Market under the symbol ZIXI. The table below shows the high and low sales prices by quarter for 2009 and 2008. These prices do not include adjustments for retail mark-ups, mark-downs or commissions.

| | 2009 | | 2008 | |
|---|---|---|---|---|
| **Quarter Ended** | **High** | **Low** | **High** | **Low** |
| March 31 | $ 1.73 | $ 0.88 | $ 4.74 | $ 2.50 |
| June 30 | $ 1.94 | $ 0.95 | $ 4.16 | $ 2.25 |
| September 30 | $ 2.54 | $ 1.49 | $ 3.70 | $ 1.81 |
| December 31 | $ 2.30 | $ 1.53 | $ 2.34 | $ 0.94 |

At March 5, 2010, there were 63,887,125 shares of common stock outstanding held by 523 stockholders of record. On that date, the last reported sales price of the common stock was $2.19.

We have not paid any cash dividends on our common stock since 1995 and do not anticipate doing so in the foreseeable future. Applicable governing law prohibits the payment of any dividends unless our net assets (total assets minus total liabilities) exceeds the amount of dividends.

For information regarding stock-based compensation awards outstanding and available for future grants, see Item 12. Security Ownership of Certain Beneficial Owners and Management and Related Stockholder Matters.

During 2009, we did not engage in any share repurchase program of our common stock.

***Performance Graph***

The following graph compares the cumulative total return of an investment in our common stock over the five-year period ended December 31, 2009, as compared with the cumulative total return of an investment in (i) the Center for Research in Securities Prices ( CRSP ) Total Return Index for Nasdaq Stock Market (U.S. companies) and (ii) the CRSP Total Return Index for Nasdaq Computer and Data Processing Stocks. The comparison assumes $100 was invested on December 31, 2004, in our common stock and in each of the two indices and assumes reinvestment of dividends, if any. A listing of the companies comprising each of the CRSP- NASDAQ indices used in the following graph is available, without charge, upon written request.

**Item 6.** ***Selected Financial Data***

The following selected financial data should be read in conjunction with Item 7. Management s Discussion and Analysis of Financial Condition and Results of Operations, the consolidated financial statements and notes thereto included elsewhere herein. No cash dividends were declared in any of the five years shown below:

| | Year Ended December 31, | | | | |
|---|---|---|---|---|---|
| | **2009** | **2008** | **2007** | **2006** | **2005** |
| | **(In thousands, except per share data)** | | | | |
| **Statement of Operations Data:** | | | | | |
| Revenues (1) | $ 30,651 | $ 28,035 | $ 24,114 | $ 18,358 | $ 13,964 |
| Cost of revenues | 9,384 | 9,850 | 10,866 | 12,552 | 14,194 |
| Gross margin | 21,267 | 18,185 | 13,248 | 5,806 | (230) |
| Research and development expenses | 6,948 | 6,158 | 5,322 | 6,085 | 6,520 |
| Selling, general and administrative expenses | 18,880 | 18,033 | 17,961 | 23,188 | 26,358 |
| Customer deposit forfeiture (2) | | | (2,000) | (1,000) | (960) |
| Net (gain) loss on sale of product lines | | | | (53) | 3,716 |
| Loss on extinguishment of convertible debt (3) | | | 255 | 871 | 1,283 |
| Asset impairment charge | | | | 125 | 288 |
| Interest expense | 21 | | 171 | 1,126 | 6,848 |
| (Gain) on derivatives | | | | (4,043) | |
| Loss from continuing operations | (4,435) | (5,442) | (8,102) | (19,508) | (43,596) |
| Basic and diluted loss per common share from continuing operations | $ (0.07) | $ (0.09) | $ (0.13) | $ (0.34) | $ (1.20) |
| Shares used in computing basic and diluted loss per common share | 63,422 | 62,982 | 60,424 | 57,068 | 36,452 |
| **Statements of Cash Flows Data:** | | | | | |
| Net cash flows provided by (used for): | | | | | |
| Operating activities | $ 603 | $ 2,064 | $ (1,443) | $ (16,678) | $ (24,901) |
| Investing activities | (1,138) | 493 | (3,155) | 3,914 | 22,767 |
| Financing activities | 577 | 164 | 2,339 | 5,307 | 18,518 |
| **Balance Sheet Data:** | | | | | |
| Cash, Cash Equivalents and Marketable Securities | $ 13,312 | $ 13,245 | $ 12,258 | $ 12,783 | $ 20,240 |
| Working capital (deficit)(4) | (3,283) | (3,010) | (979) | (897) | 9,348 |
| Total assets | 19,748 | 19,357 | 19,474 | 20,366 | 34,115 |
| Debt obligations | 312 | | | 2,916 | 7,063 |
| Stockholders (deficit) equity | (1,989) | (1,303) | (289) | 927 | 10,397 |

Our consolidated financial statements include for 2005 the results from operations for a previously acquired business, Elron Software, in 2003, and a January 2004

acquisition, MyDocOnline. In 2005, the two product lines relating to the Elron Software acquisition were sold in March and the one remaining MyDocOnline product line, Dr. Chart, was sold in September.

(1) Revenues for the year 2005 include the previous acquisitions of MyDocOnline and Elron Software. Revenues resulting from these acquisitions, which were subsequently sold as indicated immediately above, totaled $0.9 million.

(2) See Note 11 to the consolidated financial statements for an explanation of the customer deposit forfeiture.

(3) See Note 12 to the consolidated financial statements for an explanation on the early extinguishment of debt items.

(4) Working capital includes deferred revenue totaling $14.5 million, $15.0 million, $12.6 million and $8.4 million as of December 31, 2009, 2008, 2007 and 2006 respectively. Working capital also includes customer deposits totaling $2.0 million as of December 31, 2006.

**Item 7.** ***Management s Discussion and Analysis of Financial Condition and Results of Operations***

***Forward-Looking Statements***

The following discussion and analysis contains forward-looking statements about trends, uncertainties and our plans and expectations of what may happen in the future. Forward-looking statements involve risks and uncertainties that could cause actual events or results to differ materially from the events or results described in the forward-looking statements, including risks and uncertainties described above in Item 1A. *Risk Factors*. Readers are cautioned not to place undue reliance on forward-looking statements. The forward-looking statements are based upon information available to us on the date of this report. We undertake no obligation to publicly update or revise any forward-looking statements, whether as a result of new information, future events or otherwise.

***Overview***

We are a leader in providing secure, Internet-based applications in a SaaS model. These applications connect, protect and deliver information in a secure manner, enabling the use of the Internet for applications requiring a high level of security in the healthcare, finance, insurance, and government sectors. Our core competency is the ability to deliver these complex service offerings with a high level of availability, reliability, integrity, and particularly security. We operate under two reporting segments, Email Encryption Service ( Email or Email Encryption ) and e-Prescribing Service ( e-Prescribing ) where we offer these services on a subscription basis to our customers who subscribe to use the services for a specified term. As stated in Item 1. Business , we have announced our intention to exit the e-Prescribing business by December 31, 2010, following the completion of existing obligations associate