

ZIX CORP
Form 10-K
March 09, 2012
Table of Contents

United States
SECURITIES AND EXCHANGE COMMISSION

Washington, D.C. 20549

Form 10-K

(Mark One)

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

For the fiscal year ended December 31, 2011

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)

Edgar Filing: ZIX CORP - Form 10-K

Texas
(State or Other Jurisdiction of

75-2216818
(I.R.S. Employer

Incorporation or Organization)

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:

Title of each class of stock
Common Stock

Name of each exchange on which registered

\$.01 Par Value

NASDAQ

Securities Registered Pursuant to Section 12(b) of the Act:

None

Indicate by check mark whether the Registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act.

Yes No

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 No

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 No

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

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.

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):

Large accelerated filer Accelerated filer

Non-accelerated filer (Do not check if a smaller reporting company) Smaller reporting company

Indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act).

Edgar Filing: ZIX CORP - Form 10-K

Yes No

As of March 6, 2012, there were 62,880,376 shares of Zix Corporation \$0.01 par value common stock outstanding. As of June 30, 2011, the aggregate market value of the shares of Zix Corporation common stock held by non-affiliates was \$243,642,616.

DOCUMENTS INCORPORATED BY REFERENCE

Portions of the Registrant's 2012 Proxy Statement are incorporated by reference into Part III of this Form 10-K.

Table of Contents

TABLE OF CONTENTS

	<u>PART I</u>	
Item 1.	<u>Business</u>	3
Item 1A.	<u>Risk Factors</u>	7
Item 1B.	<u>Unresolved Staff Comments</u>	13
Item 2.	<u>Properties</u>	13
Item 3.	<u>Legal Proceedings</u>	14
Item 4.	<u>Mine Safety Disclosures</u>	14
	<u>PART II</u>	
Item 5.	<u>Market for Registrant's Common Equity, Related Stockholder Matters and Issuer Purchases of Equity Securities</u>	15
Item 6.	<u>Selected Financial Data</u>	16
Item 7.	<u>Management's Discussion and Analysis of Financial Condition and Results of Operations</u>	17
Item 7A.	<u>Quantitative and Qualitative Disclosures About Market Risk</u>	28
Item 8.	<u>Financial Statements and Supplementary Data</u>	28
Item 9.	<u>Changes in and Disagreements with Accountants on Accounting and Financial Disclosure</u>	28
Item 9A.	<u>Controls and Procedures</u>	28
Item 9B.	<u>Other Information</u>	31
	<u>PART III</u>	
Item 10.	<u>Directors, Executive Officers and Corporate Governance</u>	32
Item 11.	<u>Executive Compensation</u>	32
Item 12.	<u>Security Ownership of Certain Beneficial Owners and Management and Related Stockholder Matters</u>	32
Item 13.	<u>Certain Relationships and Related Transactions, and Director Independence</u>	32
Item 14.	<u>Principal Accountant Fees and Services</u>	32
	<u>PART IV</u>	
Item 15.	<u>Exhibits and Financial Statement Schedules</u>	32

Table of Contents

PART I

Item 1. *Business*

Zix Corporation (ZixCorp®, the Company, we, our, or us) is a leader in providing email encryption services. 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. More than 1,200 hospitals and over 1,600 financial institutions, including some of the most influential companies and government organizations, use our Email Encryption Service. Wellpoint and the Securities and Exchange Commission (SEC) are among these notable customers. Our Email Encryption Service is enhanced by ZixDirectory®, which includes approximately 30 million members. ZixDirectory allows for emails to be sent seamlessly whenever possible, across the largest email encryption community in the world.

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 company- defined policies. 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 exceptional ease of use. The best example of this is our ability to provide 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 enables transparent delivery by (1) 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, which is an enterprise gateway that automatically decrypts the message. The result is secure encrypted email exchange that is transparent for both sender and receiver.

Our 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 SysTrustSM 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 ZixData Center is staffed 24 hours a day with a proven 99.99% reliability rate.

Our company was incorporated in Texas in 1988. Originally named Amtech Corporation, we changed our name to ZixIt® Corporation in 1999 when we entered the encrypted email market. In 2002, we became Zix Corporation. Our executive offices are located at 2711 North Haskell Avenue, Suite 2200, LB 36, Dallas, Texas 75204-2960, (214) 370-2000.

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, in addition to 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. For example, healthcare organizations are subject to the Health Information Portability Accountability Act (HIPAA), as revised by the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH ACT). Financial institutions are subject to data privacy laws included in the Gramm-Leach-Bliley Act (GLBA). In addition, individual states such as Massachusetts and Nevada have enacted state laws requiring encryption of certain emails and information.

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 allows a user to send encrypted email to any email user at any email address by using the ZixCorp Best Method of Delivery protocol which automatically determines the most direct and appropriate means of delivery, based on the sender's and recipient's communications environment and preferences. The protocol

Table of Contents

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 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 outbound email for an enterprise without the need to create, deploy or manage end user encryption keys or deploy desktop software. Our technology solutions are easy to use, 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 emails and apply policies that match specific industry criteria such as HIPAA, HITECH 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 and significantly reduce the risk of inadvertently sending sensitive content by regulating the method of delivery through preset policies.

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 approximately 30 million members. The ZixDirectory adds members at a rate of approximately 100,000 new members per week.

Today in the healthcare industry, our Email Encryption Service is used by over thirty Blue Cross Blue Shield organizations and over 1,200 hospitals. In the financial services sector, we serve over 1,600 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 agencies in those states.

Competition

The most significant differentiator for ZixCorp's Email Encryption Service as compared with our competition is ease of use. The best example of our unequalled ease of use is transparent delivery of encrypted email messages. We are able to deliver transparent email encryption as a result of our SaaS architecture, the ZixDirectory, the Best Method of Delivery and the ZixGateway. The most critical and highly differentiated component of our solution is the ZixDirectory which provides the ability to share user identities for encryption, which in turn provides interoperability between users in a community of interest such as healthcare, finance or government.

In addition, our service differs from the products and services of most of our competitors because we offer a SaaS architecture, while most of our competitors offer primarily a product-based approach that the customer builds and runs themselves. Some of our competitors have substantial information technology security and email protection products, however, 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 is 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-mail. We enable secure communications with other users via TLS, Open PGP, push delivery and secure portal pull 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-mail security market. We view our primary competitors as Cisco Systems Inc., Proofpoint Inc., and McAfee, Inc. Technically, while these companies offer "send-to-anyone" encrypted email, we believe they are

Table of Contents

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. There are other competitors but we do not view them as particularly significant.

Regulatory Drivers

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. 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 expanded the scope of HIPAA. Key elements of the HITECH ACT relating to HIPAA include increased penalties for violations, stricter and more onerous breach notification requirements, an expanded 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. Pursuant to the HITECH ACT, the Office for Civil Rights has announced plans to audit up to 150 covered entities during 2012 to assess privacy and security compliance. The Company believes these changes will continue to 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 promulgated under GLBA, HIPAA and HITECH and state laws and 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 state law requiring encryption of emails containing sensitive information was passed by Nevada on October 1, 2008. On March 1, 2010, new regulations in the state of Massachusetts became effective (201 CMR 17.00). The Massachusetts regulations bear the most comprehensive encryption requirements imposed on businesses by any state and, because they cover any business with a customer or business dealing in the state of Massachusetts, they reach far beyond Massachusetts state borders.

Even where there are no specific regulations, corporations may require email protection to adhere to evolving industry best practices for protecting sensitive information. We target the relevant regulators who themselves have placed an increased emphasis on the secure transmission of sensitive information. Our customers include all of the federal regulators who comprise the FFIEC as well as the state banking regulators in more than twenty states. Our service is also 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.

Sales and Marketing

We 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, including other service providers seeking an encryption offering in an original equipment manufacturing (OEM)-like relationship. New first year orders derived from our valued added resellers, OEM and third party distribution channels for 2011 were 52% of the total new first year orders compared to 53% in 2010. Google, Inc. continues to be our largest third party reseller representing approximately 15% of new first year orders in 2011. We now have over 170 managed security service providers and value added resellers across the U.S.

Employees

We had 127 employees as of December 31, 2011. 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 from continuing operations of \$5,229,000, \$5,089,000, and \$3,619,000 for the twelve-month periods ended December 31, 2011, 2010 and 2009, respectively.

Table of Contents

Over the course of 2011 we continued to make investments to strengthen our Email Encryption services through the development of a number of significant portfolio upgrades. We delivered ZixMobility which has set the new standard in simple mobile access for secure email. We also added Single Sign-on, customer web page integration, flexible form provisioning and application-driven email support features to our suite of ZixPort service capabilities. The ZixGateway appliance policy configuration and processing capabilities were expanded in a number of key areas including intelligent integration of transport layer security (TLS) technology into our comprehensive message delivery and reporting frameworks. The new TLS capabilities and the addition of the new ZixAccess inbound service were designed to support continued coverage expansion for our leading transparent message delivery network.

We have patents that protect certain elements of our core technology underlying the Email Encryption business, including one new U.S. patent issued in 2011. We have not realized any revenues from licensing any of our patents to third parties.

The following are registered trademarks of ours and certain of our subsidiaries: ZixCorp, 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

We have contracts with many local, state and federal agencies and regulators, which in aggregate contribute approximately five percent of our annual revenue.

Significant Customers

In each of 2011, 2010, and in 2009 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 recognize as revenue in the future. Our backlog was \$53,724,000 at December 31, 2011, compared to \$49,911,000 at December 31, 2010.

As of December 31, 2011, our backlog is comprised of the following elements: \$17,363,000 of deferred revenue that has been billed and paid, \$4,622,000 billed but unpaid, and approximately \$31,739,000 of unbilled contracts.

The backlog is recognized into revenue ratably as the services are performed. Approximately 57% of our total backlog at December 31, 2011 is expected to be recognized as revenue during 2012.

Seasonality

Our business is not materially impacted by seasonality.

Geographic Information

Our operations are primarily based in the U.S., with approximately 9% of our employees located in Canada. Except for a United Kingdom based data center, 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, 2011, were located in the U.S.

Table of Contents

Available Information

Our Internet address is www.zixcorp.com. 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 Securities Exchange Act of 1934, as amended (the Exchange Act), are available on our website, without charge, as soon as reasonably practicable after we electronically file such material with, or furnish it to, the SEC. The information found on our website shall not be considered to be part of this or any other report filed with or furnished to the SEC.

In addition to our website, 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 website 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 website is www.sec.gov.

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**, 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, hope, and other similar expressions. Any 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, but not limited to, the risks and uncertainties described in the "Risk Factors" section above.

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 1A. Risk Factors

The risks and uncertainties described below could materially and adversely affect our business, financial condition and financial results and reduce the value of an investment in our securities. This report also contains forward-looking statements and the following risks could cause our actual results to differ materially from those anticipated in such forward-looking statements.

Our 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 customers deploy and use our products and services to easily, securely and confidentially send and receive encrypted email messages. Our business and revenue substantially depend on our current and potential customers using email to exchange sensitive information electronically. New technologies, products, or 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.

Table of Contents

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 business employs 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. Successful decryption of encrypted information, or public reports of successful decryption, whether or not true, 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, increase our expenses 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 our 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 competition, which could negatively affect our business, financial condition and financial results.

The markets in which we compete are characterized by rapid change and converging technologies and are very competitive. With rising demand for private and secure email communications, there is strong competition for the email encryption products and services. Our business competes with products and services offered by companies such as Axway, Cisco Systems Inc., Echoworx, McAfee, Inc., Symantec, Proofpoint, Trend Micro and Voltage Security. Strong 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. As a result of the bundling of products by these competitors, it can be difficult for our customers to compare the cost of our products with competing products. In some instances, competing products may seem to be offered by our competitors at little to no additional cost to the customer. In addition, 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. Barriers to entry are relatively low, and new ventures are often formed that create products competitive with our products. 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 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.

Table of Contents

We increasingly rely on third party distributors to help us market our 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 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 sales cycles of 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 an 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 depends on market acceptance of our service, and our failure to achieve and maintain market penetration could negatively affect our business, financial condition and financial results.

In order to continue to operate profitably and grow, we must achieve and maintain 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 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 continue 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 or increase 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.

Challenging economic conditions worldwide have from time to time contributed, and may continue to contribute, to slowdowns in technology and networking industries at large, as well as in the specific markets in which we operate. 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 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. Specific economic trends, such as declines in the demand for PCs, services and other computing devices, or softness in corporate information technology spending, could have a more direct impact on our business. If these conditions 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, to keep pace with these developments. We

Table of Contents

must ensure that our products and services address evolving operating environments, devices, industry trends, certifications and standards. For example we have been required to expand our offerings for virtual computer environments and mobile environments to support a broader range of mobile devices. We also may need to 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. 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 and we could experience negative publicity, declining sales and legal liability.

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 prior to the product being introduced, 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. 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 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 or network traffic 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 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, cyber attacks, earthquakes, terrorist attacks, hostilities or war or other events. Computer viruses, equipment failure, denial of service attacks, 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 data center operations or our networks could result in loss of revenues, increased expenses, 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 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.

Table of Contents

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

Our business relies on third-party suppliers of the 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 as a result of internal system failures or external third party actions. Any of these outages or problems could materially adversely affect our business, financial condition and financial results.

The security of our networks and data centers is critical to our business and a breach of security through a cyber attack or otherwise could cause us to lose customers and could negatively affect our business, financial condition and financial results.

We are dependent on our networks and datacenters to provide our products and services. Due to the nature of the products and services we provide and the sensitive nature of the information we collect, process, store, use and transmit, we may face cyber attacks that attempt to penetrate our networks and datacenters. To reduce the risk of a successful cyber attack, we have implemented significant physical and logical security measures to detect and identify threats, breaches and potential incidents. Despite these security measures, our networks and datacenters remain vulnerable to cyber attack. Cyber attacks and other breaches of security at our datacenters and networks could cause negative publicity, interruption of our services, damage to our reputation, unauthorized disclosure of our customers' confidential or proprietary information (including personally identifiable information), disclosure of our intellectual property, loss of customers, lost revenue and increased expense (including potentially indemnification or warranty costs), any of which could have a material adverse effect on 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.

We rely on a combination of contractual rights, trademarks, trade secrets, patents and copyrights to establish and protect intellectual property rights and other proprietary rights in our products and services. These intellectual property rights 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 intellectual property rights or other proprietary technology into their products. Competitors may hire our former employees who may misappropriate our intellectual property rights or other proprietary technology. Some jurisdictions may not provide adequate legal protection of our intellectual property rights or other proprietary technology.

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. If we acquire technology to include in our products from third parties, our exposure to infringement actions may increase because we must rely upon these third parties to verify the origin and ownership of such technology. Intellectual property litigation and controversies are disruptive and expensive. Even unmeritorious claims brought against us or our customers may harm our reputation and customer relationships, may cause us to incur significant legal and other fees to defend, 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.

Table of Contents

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 use open source software in order to take advantage of common industry building blocks and 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 or require us to publically disclose proprietary information. We have processes and controls in place that are designed to address these risks and concerns, but we cannot be sure that all open source software is submitted for approval prior to use in our products nor that our process or controls will be sufficient to mitigate all risk in this regard.

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, many of whom are compensated, in part, based on the performance of our stock price. The loss of services of any of our key personnel, the inability to retain and attract qualified personnel in the future or delays in hiring required personnel could make it difficult to meet key objectives. Any of these impairments related to our key personnel could negatively affect our business, financial condition and financial results.

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

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 subject to confidentiality agreements with our clients and handling of this data is increasingly subject to regulation around the world. These regulations may result in conflicting requirements and may change over time. 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 or other confidential information (including due to a cyber attack) or other failure by us to comply with data privacy requirements could subject us to significant penalties, damages, 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 ours are generally restricted by the U.S. government. Although we have obtained U.S. government approval to export our service to almost all countries, the list of countries to which we (and our distributors) 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.

Table of Contents

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 to pay our expenses and we expect to remain profitable, we may not continue to produce sufficient cash flow or show a profit. Our balance sheets reflect 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 or otherwise. In addition, the stock market has experienced extreme price and volume fluctuations that have affected the market price of many technology companies in general, and such fluctuations were often unrelated to the operating performance of these companies. These fluctuations have and will continue to affect smaller capitalized technology companies like us. Any of these circumstances could cause our securities to decline in value.

Exercises of options 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 options, including options held by our employees. The exercise of 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.

Item 1B. *Unresolved Staff Comments*

None.

Item 2. *Properties*

During 2011 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. Our Burlington employees perform sales and marketing activities. Our Ottawa employees perform both client services and sales support activities. The United Kingdom facility provides data center support for our European customers. 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 primarily for fail-over and business continuity services and is used to some extent to support normal ongoing operations. Our facilities are suitable for our current needs and are considered adequate to support expected near term growth.

Table of Contents

Item 3. *Legal Proceedings*

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

Item 4. *Mine Safety Disclosures*

Not applicable.

Table of Contents**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 fiscal 2011 and 2010.

Quarter Ended	2011		2010	
	High	Low	High	Low
March 31	\$ 4.88	\$ 3.28	\$ 2.51	\$ 1.69
June 30	\$ 4.05	\$ 2.98	\$ 2.70	\$ 2.09
September 30	\$ 4.21	\$ 2.66	\$ 2.94	\$ 2.10
December 31	\$ 3.00	\$ 2.16	\$ 4.55	\$ 2.70

At March 6, 2012, there were 62,880,376 shares of common stock outstanding held by 479 stockholders of record. On that date, the last reported sales price of the common stock was \$2.88.

We have not paid any cash dividends on our common stock and do not anticipate doing so in the foreseeable future.

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.

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, 2011, 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, 2006, in our common stock and in each of the two indices and assumes reinvestment of dividends, if any. The stock price performance on the following graph is not necessarily indicative of future stock performance. A listing of the companies comprising each of the CRSP- NASDAQ indices used in the following graph is available, without charge, upon written request.

Table of Contents**Sale of Unregistered Securities**

None.

Purchases of Equity Securities by the Issuer

Period	Total Number of Shares		Average Price Purchased as part of Publicly Announced Plans or Programs ¹		Purchased Under the Plans or Programs
	Purchased		Paid per Share		
October 1, 2011 to October 31, 2011	0			0	\$ 0,000
November 1, 2011 to November 30, 2011	1,181,706		\$ 2.72	1,181,706	\$ 11,791,000
December 1, 2011 to December 31, 2011	1,002,647		\$ 2.78	1,002,647	\$ 9,000,000
Total	2,184,353		\$ 2.75	2,184,353	\$ 9,000,000

¹ The shares were repurchased under the \$15 million stock repurchase program announced November 9, 2011. No shares were purchased other than through publicly announced programs during the periods shown.

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. No cash dividends were declared in any of the five years shown below:

	Year Ended December 31,				
	2011	2010	2009	2008	2007