ZIX CORP
Form 10-K
March 08, 2019

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, 2018

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:

Title of each class of stock	Name of each exchange on which registered
Common Stock $0.01 Par Value	NASDAQ

Securities Registered Pursuant to Section 12(g) 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 every Interactive Data File required to be submitted 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 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, smaller reporting company, or an emerging growth company. See definitions of "large accelerated filer," "accelerated filer," "smaller reporting company," and "emerging growth company" in Rule 12b-2 of the Exchange Act.

Large accelerated filer	Accelerated filer
Non-accelerated filer	Smaller reporting company Emerging growth company

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13 (a) of the Exchange Act.

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

As of March 6, 2019, there were 54,089,273 shares of Zix Corporation $0.01 par value common stock outstanding. As of June 30, 2018, the aggregate market value of the shares of Zix Corporation common stock held by non-affiliates was $289,258,242.

DOCUMENTS INCORPORATED BY REFERENCE

Portions of the Registrant's 2019 Proxy Statement are incorporated by reference into Part III of this Form 10-K.

TABLE OF CONTENTS

PART I

Item 1. Business

Zix Corporation ("Zix®," the "Company," "we," "our," or "us") is a leader in email security. Trusted by the nation's most influential institutions in healthcare, finance, and government, Zix delivers a superior experience and easy-to-use solutions for email encryption, data loss prevention ("DLP"), advanced threat protection, archiving, and bring your own device ("BYOD") mobile security. Focusing on the protection of business communication, Zix enables its customers to better secure data and meet compliance needs. We primarily serve organizations in the healthcare, financial services, insurance and government sectors, including U.S. federal financial regulators, such as members of the Federal Financial Institutions Examination Council ("FFIEC"), divisions of the U.S. Treasury, the U.S. Securities and Exchange Commission ("SEC"), more than 30% of U.S. banks, more than 30% of Blue Cross Blue Shield plans and more than 1,200 U.S. hospitals.

ZixEncrypt℠ (formerly ZixGateway® and ZixQuarantine®) bundles email encryption and DLP capabilities to enable the secure exchange of email that includes sensitive information. Through a comprehensive secure messaging service, ZixEncrypt allows an enterprise to use policy-driven rules to determine which email messages should be sent securely or quarantined for review to comply with regulations or company-defined policies.

The main differentiation for Zix Encrypt in the marketplace is our exceptional ease of use. The best example of this is our ability to provide transparent delivery of encrypted email. Most email encryption solutions are focused on the sender. They typically introduce an added burden on recipients, often requiring additional user authentication with creation of new user identity and password. We designed our solution to alleviate the recipient's burden by enabling the delivery of encrypted email automatically and transparently. Zix enables transparent delivery by (1) ZixDirectory®, the world's largest email encryption community, which is designed to share identities of our tens of millions of members (growing by approximately 160,000 members per week), (2) Zix's patented Best Method of Delivery®, which is designed to deliver email in the most secure, most convenient method possible for the recipient, and (3) ZixEncrypt, which automatically encrypts and decrypts messages with sensitive content. The result is secure, transparent encrypted email, such that secure email can be exchanged without any impact to administrators or extra steps for both senders and recipients. Zix delivers more than 1.5 million encrypted messages on a typical business day. Of those, approximately 70% are exchanged transparently between senders and recipients.

ZixEncrypt also addresses a business's greatest source of data loss – corporate email – with an easy straightforward DLP approach. By focusing strictly on the risks of email, ZixEncrypt simplifies DLP in comparison to other DLP solutions by decreasing complexity and costs, reducing deployment time from months to hours and minimizing impact on customer resources and workflow. In addition, Zix offers a convenient experience for both employees interacting with our solution and administrators managing the system.

ZixEncrypt enables DLP capabilities for email by combining proven policy and content scanning capabilities with quarantine functionality. The quarantine system and its intuitive interface allows administrators to (1) easily define policies and create custom lexicons for quarantining email messages, (2) conveniently manage quarantined messages using flexible searching and filtering options, (3) release or delete individual or multiple quarantined messages with one click, (4) review reports that monitor quarantine activities and trends and (5) automate custom notifications informing employees of quarantined messages.

ZixEncrypt also provides greater visibility into an organization's data risks in email by capturing data in outbound emails and highlighting violations that trigger policy filters to encrypt or quarantine. Through our interactive, real-time interface, companies can monitor their greatest vulnerabilities, generate reports for business executives and train employees about the sensitivity of their company's data.

ZixEncrypt is available as a hosted solution, as a multi-tenant cloud solution, or as a physical or virtual on-premises appliance.

In March 2017, Zix acquired Greenview Data Inc. (“Greenview”), an email security company. Zix’s acquisition of Greenview addresses increasing buyer demand for email security bundles by adding advanced threat protection, antivirus, anti-spam and archiving capabilities to its industry-leading email encryption. Greenview is a good fit for Zix’s business based on its employees’ expertise in email security and its emphasis on customer success, which align with Zix’s reputation for delivering industry-leading solutions and a superior experience.

Through the acquisition of Greenview, Zix launched two new solutions in April 2017 – ZixProtect and ZixArchive. ZixProtect defends organizations from zero-day malware, ransomware, phishing, CEO fraud, W-2 phishing attacks, spam and viruses in email with multi-layer filtering techniques. Accuracy in protecting organizations from email threats is increased further with automated traffic analysis, machine learning and real-time threat analysis.

ZixProtect is available as a cloud-based service in three bundles. ZixProtect Essentials includes email threat protection, impersonation defense, 0-hour malware filtering, and business email continuity to enable access to emails during service disruption; ZixProtect Plus adds policy based Content Disarm and Reconstruction with on-demand sandboxing, as well as time-of-click link defense, to provide enhanced protection against sophisticated, targeted threats; and ZixProtect Premium delivers a comprehensive email security solution by including our leading email encryption and data loss prevention with our threat protection capabilities.

ZixArchive is a low-cost, cloud-based email retention solution that easily enables user retrieval, compliance and eDiscovery. Available as a standalone or add-on solution for ZixEncrypt or ZixProtect bundles, ZixArchive includes policy-based retention, automatic indexing and flexible search capabilities for audit and legal requirements. With on-demand access through the cloud, organizations can conveniently share messages with employees, auditors and outside consultants or legal counsel, as well as revoke access when needed.

In April 2018, Zix acquired CM2.COM, Inc., d/b/a Erado ("Erado"), a unified archiving company. Erado strengthens Zix's comprehensive archiving solutions with unified archiving, supervision, security, and messaging solutions for customers that demand bundled services. Erado's long standing focus on helping its customers comply with FINRA and SEC regulations helps further strengthen Zix's offerings for customers with compliance requirements. This acquisition also expands Zix's cloud-based email archiving capabilities into more than 50 content channels, including social medial, instant message, mobile, web, audio, and video.

ZixOne® is a unique mobile email app that solves the key IT challenge created by the BYOD trend in the workplace. BYOD describes employee's use of personal devices to conduct work. ZixOne provides mobile access to corporate email while never allowing that data to be persistently stored on an employee's device where it is vulnerable to loss or theft. If the device is lost or stolen, an administrator can simply disable access to corporate email from that device through ZixOne.

ZixOne is available as a standalone solution and easily integrates with ZixEncrypt as an add-on solution. One feature of ZixOne is the ability to encrypt an email from your mobile device with the simple slide of an "Encrypt" button, ensuring that sensitive information is secured either by the user or through automatic policies of ZixEncrypt.

Unlike other BYOD solutions, ZixOne meets employee desire for convenience, control and privacy while giving companies the ability to secure corporate data and meet compliance needs. With seamless access to work email in a secure, simple-to-use environment, employees can stay productive while preserving device independence. A BYOD solution that is acceptable to employees and yet provides strong data protection for corporate data solves one of today's greatest IT management challenges.

Our business operations and service offerings are supported by the ZixData Center™, which is PCI DSS 3.2 certified for applicable services, SOC2 accredited, and SOC3 certified. The operations of the ZixData Center are independently audited annually to maintain AICPA SOC3 certification in the areas of security, confidentiality, integrity and availability. Auditors also produce a SOC2 report on the effectiveness of operational controls used over the audit period. The ZixData Center is staffed 24 hours a day and has a track record that exceeds 99.99% availability.

On February 20, 2019, Zix completed its acquisition of AppRiver, LLC ("AppRiver"), a channel-first provider of cloud-based cyber security and productivity services, offering web protection, email encryption, secure archiving, and email continuity solutions. AppRiver is a channel-first provider of cloud-based cyber security and productivity services, offering web protection, email encryption, secure archiving, and email continuity solutions. AppRiver also provides Microsoft Office 365 and Secure Hosted Exchange services, which serve as an effective lead generation tool for the company's solutions. The acquisition of AppRiver can accelerate our offerings into the cloud at the point of initial cloud application purchase. Because AppRiver currently services over 60,000 worldwide customers using a network of 4,500 Managed Service Providers, this acquisition also helps us expand our customer base.

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, and in 2017, the Company rebranded to Zix. 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 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, business associates and sub-contractors are subject to the Privacy, Security, and Enforcement Rules of the Health

Information Portability and Accountability Act ("HIPAA") as amended by the Health Information Technology for Economic and Clinical Health Act ("HITECH Act"). Financial institutions are subject to data privacy laws including the Gramm-Leach-Bliley Act ("GLBA"). These federal laws help drive the use of encrypted email. In addition, individual states such as Massachusetts and Nevada have enacted privacy laws requiring the safeguard of personal data, and almost all states encourage email encryption by allowing exemptions from data breach notification laws.

Corporations require easy to use, cost-effective email protection that can be used on an enterprise-wide basis. They need it to be quickly deployed and regularly updated to evolve with innovative technology practices and meet changing regulatory standards. 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 anywhere and on any Internet-enabled device. Encrypted email is delivered through the patented 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 supports a number of encrypted email delivery mechanisms, including S/MIME, Transport Layer Security ("TLS"), Open Pretty Good Privacy ("PGP"), "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 is one of many differentiators that 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 matching specific industry criteria such as HIPAA, the HITECH Act and GLBA. Customers can also build their own custom policies. This policy driven email encryption for regulatory compliance means customers can reduce the training required of their staff and significantly reduce the risk of inadvertently sending sensitive content by controlling the method of delivery through preset policies.

Email is the number one communication tool for businesses and it is also one of the top vectors for cyberattacks. Attacks can jeopardize a company through malware, phishing, ransomware, business email compromise, viruses and other threats. Our advanced threat protection solution uses a multi-layer approach to accurately identify email threats and defend against email-borne attacks. Our threat filters first analyze IP addresses and URLs then examine content for targeted phrases, campaign patterns and both known and zero-hour malware attacks. Accuracy is increased further with real-time threat analysts, automated traffic analysis and machine learning.

To safeguard against increasingly targeted and sophisticated attacks, our advanced threat protection can also leverage attachment assurance and time-of-click link defense to provide enhanced protection. Attachment assurance offers quarantine and sandbox inspection of emails to perform forensic analysis of attachments in our secure, cloud-based sandbox environment. Testing efficiently handles evasive attacker techniques while fully examining files for suspicious and malicious activity. Time-of-click link defense reduces the risk of users clicking links in emails and inadvertently visiting malicious or compromised websites. This feature re-writes all full, shortened, or obfuscated links to safe versions and performs time-of-click analysis on the destination address, including IP address and domain blacklists, domain age and reputation, and other checks.

By combining our email encryption and advanced threat protection solutions, Zix meets customers' increasing desire for a bundled solution that protects inbound and outbound email with leading email security.

Competition

The most significant differentiators for Zix as compared with our competition is ease of use and exceptional support. 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 ZixDirectory, Best Method of Delivery and ZixEncrypt. The most critical and highly differentiated component of our solution is the ZixDirectory which provides the ability to share user identities for encryption, and in turn provides frictionless interoperability between users in a community of interest such as healthcare, finance or government.

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” enabling transparent secure communications with other ZixEncrypt customers using our centralized key management system and overall unique approach to implementing encrypted email. 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 exceptional support allows customers to reach Zix via phone or email 24/7/365 to address any questions or concerns. With the increasing cost and sophistication of email attacks, convenient access to our threat analysts at any time of the day provides our customers with unmatched peace of mind.

We view our primary competitors in the email security space to be Proofpoint Inc., Mimecast, and Barracuda Networks. Technically, while these companies offer advanced threat protection against email attacks and “send-to-anyone” encrypted email, we believe that Zix offers superior customer service and unparalleled benefits that come from access to the ZixDirectory, use of our Best Method of Delivery protocol, and the industry’s only transparent email encryption. Nevertheless, some of these competitors are large enterprises with substantial financial and technical resources that exceed those we possess.

Regulatory Drivers

We have been successful in securing market penetration in our target vertical markets of healthcare, finance services and government primarily due to regulations that address the need for data privacy and security.

In addition to the need to protect personal data and sensitive business communication, demand for email security in the healthcare sector, including business associates of healthcare providers, is augmented by regulatory requirements under HIPAA and HITECH Act. The Privacy and Security rules under those acts provide severe penalties for violations, include strict breach notification requirements, and allow states to pursue HIPAA violations. In the financial services industry, financial institutions and their service providers are subject to the GLBA, which is enforced by the U.S. Federal Trade Commission (“FTC”). The FTC has issued guidance saying that businesses that transmit sensitive data by email should be sure to encrypt the data.

In choosing an email security provider, companies are influenced by the solutions chosen by their regulators. Our customers include all of the federal regulators that 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 4,600 state-chartered banks in the U.S.

Additionally, state data breach laws and privacy regulations, along with highly publicized breaches, have enhanced security awareness in vertical markets outside of healthcare and financial services and have prompted affected organizations to consider adopting systems that ensure data security and privacy. Even where there are no specific regulations, businesses may require email protection to adhere to evolving industry best practices for protecting sensitive information.

Sales and Marketing

We sell our Zix Email Encryption, ZixProtect, ZixArchive, Zix DLP, and ZixOne Services 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 email encryption offering in an original equipment manufacturing (“OEM”)-like relationship. New first year orders (“NFYOs”), defined as the twelve-month value of orders received from both new customers and from our existing customers ordering additional products or features, derived from our value-added resellers, OEM and third party distribution channels for 2018 were 43% of the total new first year orders compared to 56% in 2017. The reduction in orders received from our

OEM channels was due in part to a migration of customers from our Google relationship into a direct relationship with Zix. In both years, the balance of our NFYOs were originated by our telesales and direct sales forces. As of December 31, 2018, we had 157 value-added resellers and 97 managed security service providers across the U.S.

Employees

We had 265 employees as of December 31, 2018. The majority of our employees are located in Dallas, Texas. We also have a sales office in Burlington, Massachusetts; an office in Ann Arbor, Michigan supporting ZixProtect and ZixArchive services; and smaller offices located in Renton, Washington, and in Ottawa, Ontario, Canada.

Research and Development

We incurred research and development ("R&D") expenses of $11.3 million, $11.0 million, and $9.6 million for the twelve-month periods ended December 31, 2018, 2017, and 2016, respectively.

Over the course of 2018 we continued to make investments toward strengthening and expanding our service portfolio while aligning with customer trends toward simplification of infrastructure management through the use of cloud technologies. A new cloud platform was delivered which allows Managed Service Providers to provision and handle traffic on infrastructure run and managed by Zix. The new services and infrastructure were also extended to become the foundation for new security and compliance bundles for direct and alternative channels which include enhanced variants of core Threat Protection, Encryption, Continuity and Archiving Technologies.

In delivering new security and compliance bundles, the R&D organization materially enhanced and integrated the subsystem platforms obtained by way of acquisitions in 2017 and 2018. Web technology implementations associated with Threat Protection/Continuity and Multimedia Archive/Compliance platforms, obtained by way of acquisitions of Greenview Data and Erado respectively, were restructured to align to a new unified user experience model as were legacy Encryption subsystems and associated reporting and management capabilities. Most related services were enhanced with technologies to enable automation of customer-driven provisioning. We also completed branding and mobile-first modernization of the web interface for the encryption appliance software we acquired from Entrust Datacard and are now in the process of binding it into our Encryption Best-Method-of-Delivery framework, thus enabling on-premises message delivery portal options for our customers.

Intellectual Property

We depend upon our ability to develop, maintain and protect our proprietary technology and our related intellectual property rights. We rely on a combination of patent, trademark, trade secret and copyright law and contractual restrictions to protect the proprietary aspects of our technology and related property rights and to defend against infringement and/or misappropriation claims from others. We own 25 U.S. patents with expiration dates ranging from 2019 through 2036, and 10 pending U.S. Applications. We have a program to file applications for and obtain patents and trademarks in the United States and in specific foreign countries where we believe filing for such protection is appropriate. While intellectual property rights are generally important to our business, we do not believe that our business is dependent on any single item of intellectual property, or that any single item of intellectual property is material to the operation of our business. Rather, we believe that our intellectual property rights provide us with a competitive advantage, and from time to time we have taken steps to enforce our intellectual property rights as a means of protecting that competitive advantage.

Our Company and certain of our subsidiaries are the owners of trademarks and service marks registered with the United States Patent & Trademark Office. These marks are renewable indefinitely, contingent upon continued use and payment of applicable renewal fees. Additionally, our Company and certain of our subsidiaries own several pending trademark applications with the United States Patent & Trademark Office as well as a number of United States common law trademarks and several service marks and trademarks and service marks registered in foreign countries. We consider our trademark and service marks as valuable assets of the Company due to their recognition by our customers. We are not aware of any valid claims of infringement or challenges to our right to use any of our trademarks or service marks in the United States.

Please see generally the risks that are more fully disclosed in "Item 1A. Risk Factors" for risks related to our intellectual property.

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 the aggregate contributed approximately 7% of our annual revenue in 2018.

Significant Customers

In each of 2018, 2017, and 2016, no single customer accounted for 10% or more of our total revenues.

Backlog

Our backlog is comprised of contractual commitments that we expect to recognize as revenue in the future. Our backlog was $73.0 million at December 31, 2018, compared to $72.6 million at December 31, 2017.

As of December 31, 2018, our backlog is comprised of the following elements: $32.1 million of deferred revenue that has been billed and paid, $10.7 million billed but unpaid, and approximately $30.2 million of unbilled contracts.

The backlog is recognized into revenue ratably as the services are performed. Approximately 65% of our total backlog at December 31, 2018, is expected to be recognized as revenue during the next twelve months.

Seasonality

The Company typically experiences lower NFYO's in the first quarter of the calendar year. Our budget anticipates fewer NFYO's in the first quarter, but historically this has not resulted in a material impact to our revenue or earnings on a seasonal basis.

Geographic Information

Our operations are primarily based in the U.S., with approximately 4% of our employees located in Canada. Except for a United Kingdom based data center, we did not operate in, or have dependencies on, any other foreign countries as of December 31, 2018. Our revenues and orders to-date are almost entirely sourced in the U.S. and all significant corporate assets at December 31, 2018, were located in the U.S.

Financial Information About Industry Segments

We have one reportable segment consisting of email encryption and security solutions. We internally evaluate all of our product offerings and other sources of revenue as one industry segment, and, accordingly, do not report segment information.

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 electronically file with the SEC through the SEC's website at www.sec.gov. The SEC's website contains reports, proxy and other information statements, and other information regarding issuers, including us, that file electronically with the SEC.

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, but not limited to: any projections of future business, market share, earnings, revenues, recognition of revenues from backlog, cash receipts, or other financial items; any statements of the plans, strategies,

and objectives of management for future operations, future acquisitions or the integration thereof; 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, but need not, include words such as “may,” “will,” “predict,” “project,” “forecast,” “plan,” “should,” “could,” “goal,” “estimate,” “intend,” “continue,” “believe,” “expect,” “outlook,” “anticipate,” “hope,” and other sim 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 “Item 1A. Risk Factors” section.

Although we believe that expectations reflected in and the assumptions underlying our forward-looking statements are reasonable, actual results or assumptions made 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, including, but not limited to, those disclosed in this document. Forward-looking statements speak only as of the date on which they are made, and we do not intend, and undertake no obligation, to update any forward-looking statement.

Item 1A. Risk Factors

The following is a cautionary discussion of risks, uncertainties and assumptions that we believe are significant to our business, financial condition and financial results. In addition to the factors discussed elsewhere in this Annual Report on Form 10-K, the following are some of the important factors that, individually or in the aggregate, we believe could make our results differ materially from those described in any forward-looking statements. It is impossible to predict or identify all such factors and, as a result, you should not consider the following factors to be a complete discussion of risks, uncertainties and assumptions.

Risks Related to our Business

Our business depends upon customers using email and certain social media platforms 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 electronic messages, by way of internet communications channels including email and certain social media platforms. Our business and revenue substantially depend on our current and potential customers using email and social media to exchange sensitive information electronically. New technologies, products, or business models that could support migration to alternative means of 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 email or the social media platforms that we support, our growth prospects and our business, financial condition and financial results could be materially adversely affected.

Our business depends on market acceptance of our products and services, and our failure to achieve and maintain influential customers 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 products and services at a price that provides us with an acceptable rate of return relative to our costs. We have been successful in selling our Email Encryption products and services to high-profile customers in the healthcare, financial services and government segments of the market. The acceptance and use of our products and services by those significant customers facilitates our sales to other potential customers, and an expanding base of users in the Zix Directory aids in our market penetration and expansion. The loss of an influential customer of our existing products and services, or the failure to achieve sufficient market adoption of new products including ZixProtect and ZixArchive, 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.

Our business relies on securing new customer subscriptions and subscription renewals from existing customers.

The vast majority of our revenue is derived from customer subscriptions, and existing customers have no contractual obligations to purchase beyond the initial subscription or contract period. Our ability to grow our business is dependent in part on customers renewing their existing subscriptions and purchasing additional solutions or services after the initial term of their agreement. Though we maintain and analyze historical data with respect to rates of customer renewals, upgrades and expansions, those rates may not accurately predict future trends in renewal of certain products and services offered by us. If our customers cancel or amend their agreements with us during their term, do not renew their agreements, renew on less favorable terms or do not purchase additional solutions or products during renewal periods, our revenue may grow more slowly than expected or decline and our profitability may be harmed.

Additionally, we have experienced, and expect to continue to experience, some level of attrition with existing customers and we may not maintain historical subscription rates, and we may be unable to accurately predict our

customer renewal rates. Although we have historically retained approximately 90% of our recurring revenue on an annual basis, there has been some recent decline in such retention and our customers' renewal rates may further decline or fluctuate as a result of a number of factors, including the level of their satisfaction with our products and technical support services, customer merger or acquisition activity, customer budgets, the pricing of our products compared with those offered by our competitors, technology trends, the prevailing regulatory regime and general market conditions. If new subscriptions or subscription renewals decline from their current levels, our revenue or revenue growth may decline, and our business may suffer which could have a materially adverse effect on our financial performance.

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

We are dependent on our networks and data centers 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, data protection breaches, computer viruses and other similar disruptions from unauthorized tampering or human error that attempt to penetrate and could harm our networks and data centers. Our business depends on customers having and maintaining confidence that we provide effective network and security protection. To reduce the risk of a successful cyber-attack or similar event, we have implemented significant physical and logical security measures to detect, identify and mitigate threats as well as to monitor for and respond to potential breaches and incidents. Despite these security measures, our networks and data centers may remain vulnerable. We may not be able to correct a security flaw or particular vulnerability promptly, or at all. Further efforts to limit the ability of malicious third parties to disrupt or undermine our security efforts may be costly to implement and may not be successful. If a cyber-attack or other breach of security occurs, or is perceived to have occurred, in our internal systems or at our data centers and networks, it 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, disclosure, modification or removal of our confidential or sensitive information, theft or unauthorized use or publication of our trade secrets, 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.

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 sensitive data. 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 intercepted encrypted email, or public reports of successful decryption, whether or not true, could reduce demand for our products and services. If new methods or technologies, such as quantum computing, 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 less marketable. That could require us to make significant changes to our products and 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.

Our business depends substantially on our data center facilities and other systems and infrastructure provided by third parties, 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.

Our business relies on third-party suppliers of computer, cloud and telecommunications infrastructure to provide our products and services through the global Internet and to provide network access between our data centers, our customers and end-users of our products and services. Much of the computer and communications hardware upon which our businesses depend is located in our data center facilities in North America and in the United Kingdom. Our data centers might be damaged or interrupted as a result of numerous factors, many of which are beyond our control, including fire, flood, power loss, mechanical failure, telecommunications failure, break-ins, cyber-attacks, sabotage, vandalism, earthquakes, terrorist attacks, hostilities or war or other events. Computer viruses, equipment failure, denial of service attacks, and similar disruptions affecting the internet, infrastructure supplied by third parties 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 the networks on which we rely, whether or not in our

control, could result in loss of revenues, increased expenses, failure to achieve market acceptance, diversion of resources, injury to our reputation, liability and increased costs, and may cause our customers to terminate or elect not to renew their agreements. We do not carry sufficient insurance to compensate us for all losses that may occur as a result of any of these events. Though our products generally tolerate isolated supplier failures, the occurrence of any of these events, including multiple supplier outages or problems, could materially adversely affect our business, financial condition and financial results.

Outages or problems with internet communication 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 and internet 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 products and 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. Though our products generally tolerate isolated supplier failures, multiple supplier outages or problems could materially adversely affect 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 systems or to timely increase capacity to accommodate increased traffic on our systems. 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.

The growth of our business may require significant investment in systems and infrastructure and these investments may achieve delayed, or lower than expected benefits, which could impair our profitability and negatively affect our business, financial condition and financial results.

As our operations grow in size and scope, we continually need to improve and upgrade our technology offerings, 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 technology offerings, 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. Developing and launching new product offerings adjacent to or outside of our core service offerings can be particularly costly in terms of capital investments for both product development and marketing. At the same time, these new offerings involve greater uncertainty concerning both market acceptance and our ability to successfully execute a sales and marketing strategy that justifies our investments. Our failure to properly manage and execute new product initiatives could materially adversely affect our business, financial condition and financial results.

Because we recognize subscription revenue over the term of the applicable customer agreement, a decline in subscription renewals or new service agreements may not be reflected immediately in our operating results.

We generally recognize revenue from customers ratably over the terms of their customer agreements, which are typically one year or two years. As a result, much of the revenue we report in each quarter is deferred revenue from customer agreements entered into during previous quarters. Consequently, a decline in new or renewed client agreements in any one quarter will not be fully reflected in our revenue or our results of operations until future periods. Accordingly, this revenue recognition model also makes it difficult for us to rapidly increase our revenue through additional sales in any period, as revenue from new clients must be recognized over the applicable subscription term.

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 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.

In addition, we are also focused on addressing new and accelerating market trends, such as the continued decline of on premise email security and advance threat protection solution(s) and the continued transition towards cloud-based solutions, which requires us to continue to improve our product and service offerings. We may experience delays in the anticipated timing of activities related to our efforts to address these challenges and higher than expected or unanticipated execution costs. 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 new and existing products and services, such as mobile device data protection, could have a material adverse effect on 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 email encryption products and services. Our Email Encryption Threat Protection, Archive, and Data Loss Prevention business competes with products and services offered by companies such as Barracuda Networks, Inc., Proofpoint, MIMECast, and Virtru. Our ZixOne business competes with products and services offered by companies such as AirWatch/VMWare, Citrix (with XenMobile), Blackberry, IBM/Fiberlink (with MaaS360), and MobileIron. Strong competition requires us to develop new technology solutions and service offerings to expand the functionality and value that we offer to our customers. Our competitors may develop products and services 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.

Industry consolidation may lead to increased competition and may negatively affect our operating results.

There has been a trend toward industry consolidation in our industry for several years. We expect this trend to continue as companies attempt to strengthen or hold their market positions in an evolving industry and as companies are acquired or are unable to continue operations. For example, some of our current and potential competitors have made acquisitions, or announced new strategic alliances. Companies that are strategic alliance partners in some areas of our business may acquire or form alliances with our competitors, thereby reducing their business with us. We believe that industry consolidation may result in stronger competitors that are better able to compete as sole-source vendors for customers. This could have a material adverse effect on 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.

If we do not effectively expand and train our sales force, we may be unable to add new customers or increase sales to our existing customers and our business may be negatively affected.

We continue to be substantially dependent on our sales force to obtain new customers and to sell additional solutions to our existing customers. We believe that there is significant competition for sales personnel with the skills and technical knowledge that we require. Our ability to achieve significant revenue growth will depend, in large part, on our success in recruiting, training and retaining sufficient numbers of sales personnel to support our growth. New hires require significant training and, in most cases, take significant time before they achieve full productivity. Our recent hires and planned hires may not become as productive as we expect, and we may be unable to hire or retain sufficient numbers of qualified individuals in the markets where we do business or plan to do business. If we are unable to hire and train sufficient numbers of effective sales personnel, or the sales personnel are not successful in obtaining new clients or increasing sales to our existing client base, our business will be harmed.

If we do not successfully manage our strategic alliances, we may not realize the expected benefits from such alliances and we may experience increased competition or delays in product development.

We have entered into several strategic alliances with other companies to offer complementary products and services. These arrangements are generally limited to specific projects or series of projects, and their main goal is generally to facilitate product compatibility and adoption of industry standards. There can be no assurance that we will realize the expected benefits from these strategic alliances. If successful, these relationships may be mutually beneficial and result in industry growth. However, alliances carry an element of risk because, in most cases, we must compete in some business areas with a company with which we have a strategic alliance and, at the same time, cooperate with that company in other business areas. Also, if these partner companies fail to perform or if these relationships fail to materialize as expected, we could suffer delays in product development or other operational difficulties.

We enlist third-party distributors to market our products and services, and our failure to succeed in those relationships could negatively affect our business, financial condition and financial results.

We distribute a significant percentage of our products and services by entering into alliances with third parties who can offer our products and services along with their own or our competitors' 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 and visibility into 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. In addition, 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 future growth and success may be affected by acquisitions. If we are not able to successfully identify, negotiate, complete and integrate acquisitions, our operating results and prospects could be negatively affected.

We have acquired and expect to continue to acquire new products and technology, as well as customers, through acquisitions. The success of our future acquisition strategy will depend on our ability to identify, negotiate, complete and integrate acquisitions. Acquisitions are inherently risky, and any acquisition we complete may not be successful. Acquisitions we pursue, including our recent AppRiver acquisition, involve numerous risks, including the following:

- difficulties in integrating and managing the operations and technologies of the companies and assets we acquire;
- diversion of our management's attention from normal daily operations of our business;
- our inability to maintain the customers, the key employees, the key business relationships and the reputations of the businesses and products we acquire;
- our inability to generate sufficient revenue from acquisitions to offset increased expenses generally associated with acquisitions;
- difficulties in predicting or achieving synergies and cost savings between our existing businesses and acquired businesses;
- our responsibility for the liabilities of the businesses we acquire, including liabilities arising out of their failure to operate correctly, maintain effective data security, data integrity, disaster recovery and privacy controls prior to acquisition, or their infringement or alleged infringement of third-party intellectual property, contract or data access rights prior to acquisition;
- difficulties in complying with new markets or regulatory standards to which we were not previously subject;
- difficulties or unanticipated expenses associated with development work that is necessary to achieve interoperability between our products and solutions and the products and solutions we acquire;
- difficulties or unanticipated expenses associated with migrating customers from products and solutions developed by our acquisition targets to our own products and solutions;
- delays in our ability to implement internal standards, controls, procedures and policies in the businesses we acquire; and
- adverse effects of acquisition activity on the key performance indicators we use to monitor our performance as a busines

Unanticipated events and circumstances occurring in future periods may affect the realizability of intangible assets that we are required to record on our balance sheet as a result of acquisitions. These events and circumstances could include significant under-performance relative to projected future operating results and significant changes in our overall business or product strategies. Such events and circumstances may cause us to revise our estimates and assumptions used in analyzing the value of our intangible assets, and any such revision could result in a non-cash

impairment charge that could have a material impact on our financial results.

Unfavorable economic environments, particularly in the U.S., could negatively affect our business, financial condition and financial results.

Challenging economic conditions worldwide have from time to time contributed, and may contribute to future slowdowns in the technology and networking industries at large, as well as in the email/data security market and in specific geographic markets in which we operate. If economic growth in those markets, particularly in the U.S., which accounts for a substantial majority of our revenue, slows, 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. Additionally, as we continue along our path of

exploring additional international markets, we may become more susceptible to unfavorable economic environments outside the U.S. and that could compound the negative effects of unfavorable economic environments in markets in which we currently operate. 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 cloud computing services and 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.

If our products do not work properly or have security vulnerabilities, our reputation, business, financial condition and financial results could be negatively affected and we could experience negative publicity, declining sales and legal liability.

The threats facing our customers are constantly evolving and the techniques used by experienced hackers to access or sabotage data change frequently, often are not recognized until launched against a target, and may originate from less regulated or remote areas around the world. As a result, we must constantly update our product solutions to respond to these threats. We produce complex solutions 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 or introduce security vulnerabilities that can lead to unauthorized use or data loss. 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 or mitigate vulnerabilities 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 from the market, a security breach, 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 reputation, business, financial condition and financial results.

Our transmission and storage of personally identifiable information, including the personal data of European data subjects and other confidential information, and the potential for inadvertent exposure of PII or CI, could cause us to violate data privacy laws or lose customers and could negatively affect our business, financial condition and financial results.

We transmit and store large amounts of personally identifiable information (“PII”) about individuals, which may include healthcare or financial information, and other confidential information (“CI”). Although we have established, and continue to develop and enhance, security measures and controls to help protect against unauthorized disclosure of such PII and other CI, an inadvertent disclosure of, or unauthorized third-party access to, PII or CI, could disrupt our operations, damage our reputation and subject us to claims or other liabilities.

In addition, our processing and storage of certain types of data is subject to confidentiality agreements with our clients and handling PII is increasingly subject to a variety of changing privacy and data security regulations around the world. For example, the collection and use of personal data in the European Union, previously governed by the provisions of the Data Protection Directive, were replaced with the General Data Protection Regulation, or GDPR, in May 2018. GDPR imposes several requirements relating to the collection, use, processing and transfer of personal data, such as requirements for using consent or other legal grounds to process personal data, providing information to individuals about how their personal data is used, maintaining adequate security and data protection measures, giving data breach notifications, complying with individuals’ requests to access, correct or delete their personal data and using third-party processors of personal data. GDPR also maintains the European Union’s strict rules limiting the transfer of personal data out of the European Economic Area. Failure to comply with the requirements of GDPR and the applicable national data protection laws of the European Union Member States may result in fines and other administrative penalties. GDPR will introduce substantial potential fines for violations and increase our responsibility

and liability in relation to personal data that we process. To comply with the GDPR, we may be required to put in place additional technical and administrative measures and controls mechanisms. This may be onerous and adversely affect our business, financial condition, results of operations and prospects. Such laws and regulations are subject to new and differing interpretations and may be inconsistent among jurisdictions. For example, in October 2015, the European Court of Justice invalidated the U.S.-EU Safe Harbor framework that had been in place since 2000, which allowed companies including us to meet certain European legal requirements for the transfer of personal data from the European Economic Area to the United States. In the wake of that decision, we decided to participate in the new EU-U.S. Privacy Shield framework established by the U.S. Department of Commerce and the European Commission and opened for participation on August 1, 2016. We applied for and were approved for certification and are now an Active Participant in the Privacy Shield program. Our Privacy Shield self-certification was finalized by the Department of Commerce and became effective as of November 9, 2016 and was renewed in November 2017. This allows us to transfer personal data of European data subjects that we receive from customers to the United States, in compliance with the Privacy Shield principles. While our Privacy Shield certification and other mechanisms (such as Model Clauses) to lawfully transfer such data remain in place, those mechanisms are also subject to pending legal challenges and these legal challenges may result in different European data protection regulators applying differing standards for the transfer of personal data. Future changes in requirements under these regulations may be inconsistent with our existing data management practices. If so, we could be required to fundamentally change our business activities and practices or modify our software, which could have an adverse effect on our business, including increased cost of compliance and limitations on data transfer for us and our customers.

Any inability to adequately address privacy concerns, even if unfounded, or to comply with applicable privacy or data protection laws, regulations and policies, could result in additional costs and liability to us, damage our reputation, inhibit sales, and harm our business. Furthermore, any inadvertent disclosure of, or unauthorized access (including due to a cyber-attack) to, PII or other CI or other failure by us to comply with data privacy requirements could subject us to significant penalties, damages, remediation and other expenses, and damage our reputation, any of which could have a material adverse effect on our business, financial condition and financial results.

Problems with protecting and enforcing our intellectual property rights 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 or assert our rights in intellectual property that we use in our products and 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 and services 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. Also, we may be required to spend significant resources to monitor and protect our intellectual property rights, including initiating claims or litigation against third parties for infringement or misappropriation. Intellectual property litigation and controversies are disruptive and expensive, whether or not resolved in our favor. 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 against us could require us to develop non-infringing products and 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 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. Depending upon how the open source software is deployed, we could be required to offer products that use the open source software for no cost, or make available the source code for modifications or derivative works. Any of these obligations could have an adverse impact on our intellectual property rights and revenue from products incorporating the open source software. Using open source code could also cause us to inadvertently infringe third-party intellectual property rights or require us to publicly 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 our process or controls will be sufficient to mitigate all risk in this regard. Open source software might also introduce security vulnerabilities or defective functionality. The open source community may not always respond with adequate urgency to mitigate the impacts of

such defects.

We rely on the availability of third-party intellectual property, which may not be accessible to us on reasonable terms or at all.

Some of our products include third-party intellectual property, which may require licenses for our use. For example, a significant portion of the revenue generated by our Erado business is dependent on the licensing of certain electronic message API's, such as those made available by LinkedIn Corporation, SMS providers, Facebook, and other social media channels, and a significant portion of the revenue generated by our AppRiver business is dependent on the licensing of Microsoft products such as Office 365. Based on past experience and industry practice, we believe that such licenses can be obtained on reasonable terms; however, there can be no assurance that we will be able to obtain or maintain the necessary licenses for new or current products on acceptable terms or at all. Changes in the terms of such licenses may decrease our product margins and our failure to obtain or maintain such licenses may limit our ability to sell our products, either of which could have a material adverse effect on our business, financial condition and financial results.

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.

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 importation and 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 sales to government entities are subject to a number of challenges and risks.

Sales to U.S. federal, state and local governmental agency customers have accounted for a significant portion of our revenue in past periods, and we may in the future increase sales to government agencies. Sales to government entities are subject to a number of challenges and risks. Selling to government entities can be highly competitive, expensive and time consuming, often requiring significant upfront time and expense without any assurance that these efforts will generate a sale. Government contractual requirements often carry a high compliance risk. Government certification requirements for solutions like ours may change and in doing so restrict our ability to sell into the federal government sector until we have attained the revised certification. Government demand and payment for our solutions may be impacted by public sector budgetary cycles and funding authorizations, with funding reductions or delays adversely affecting public sector demand for our solutions. Government entities also may have statutory, contractual or other legal rights to terminate contracts for convenience or due to a default, and any such termination may adversely impact our future operating results.

Risks Related to our Indebtedness, Capital Structure and Ownership of our Common Stock

Our indebtedness could adversely affect our business and limit our ability to expand our business or respond to changes, and we may be unable to generate sufficient cash flow to satisfy our debt service obligations.

In February 2019, we entered into a credit agreement with the lenders party thereto under which we established (i) a senior secured term loan facility in an aggregate principal amount of $175 million, (ii) a senior secured delayed draw term loan facility in an aggregate principal amount of $10 million and (iii) a senior secured revolving credit facility in an aggregate principal amount of $25 million (collectively, the “Credit Facilities”). The Credit Facilities are guaranteed by certain wholly-owned subsidiaries of Zix. The Credit Facilities are secured by substantially all assets of Zix and the guarantors, subject to certain customary exceptions. The Credit Facilities will mature in February of 2024. The incurrence of this indebtedness could have adverse consequences, including the following:

- reducing the availability of our cash flow for our operations, capital expenditures, future business opportunities, stock buybacks and other purposes;
- limiting our flexibility in planning for, or reacting to, changes in our business and the industry in which we operate;
- making it more difficult to pay or refinance our debts as they become due during periods of adverse economic, financial market or industry conditions;
- limiting our ability to obtain additional financing for working capital, acquisitions or other purposes, particularly since substantially all of our assets are subject to security interests relating to existing indebtedness;
- requiring our debt to become due and payable upon a change in control;
- increasing our vulnerability to general adverse economic and industry conditions; and
- lengthening or otherwise adversely affecting our sales process as customers evaluate our financial viability.

Optional prepayments of borrowings under the Credit Facilities will be permitted at any time, without premium (other than customary LIBOR breakage costs). We must prepay the term loan facility in equal quarterly installments of $437,500 on the last day of each March, June, September and December (commencing on June 30, 2019) until maturity in February of 2024. In addition to other customary mandatory prepayment requirements, the term loan facility requires annual prepayments based on a percentage of Zix's excess cash flow, which percentage will reduce as Zix's total net leverage ratio decreases. We depend on cash on hand and cash flows from operations to make scheduled debt payments. To a significant extent, our ability to do so is subject to general economic, financial, competitive, legislative, regulatory and other factors that are beyond our control. If our business does not generate sufficient cash flow from operating activities or if future borrowings are not available to us in amounts sufficient to enable us to fund our liquidity needs, our operating results, financial condition and ability to expand our business may be adversely affected.

The interest rate borne by our Credit Facilities will float over time and is initially LIBOR plus 3.50%, with future step downs in the interest rate margin as our total net leverage reduces. The floating rate nature of this interest rate exposes us to interest rate risk. Changes in economic conditions outside of our control could result in higher interest rates, thereby increasing our interest expense even though the amount borrowed remains the same.

Restrictive covenants in our credit agreement may adversely affect our financial and operational flexibility.

The credit agreement governing our Credit Facilities contains certain financial, operational and legal covenants. The financial covenant requires Zix to maintain a maximum total net leverage ratio (as defined in the credit agreement) and is tested on a quarterly basis (commencing March 31, 2019), based on the rolling four-quarter period that ends on the last day of each fiscal quarter. The non-financial covenants restrict our ability and the ability of our restricted subsidiaries to, among other things, incur indebtedness, incur liens, merge with or acquire other entities, make investments, dispose of assets, enter into sale and leaseback transactions, make dividends, distributions or stock repurchases, prepay junior indebtedness, enter into transactions with affiliates, enter into restrictive agreements, and amend our organizational documents or the terms of junior indebtedness.

These restrictions may make it more difficult or discourage a takeover of Zix, whether favored or opposed by our management and/or our Board of Directors.

Our ability to comply with some of these restrictive covenants can be affected by events beyond our control, and we may be unable to do so. Failure to comply could require us to seek waivers or amendments of covenants or alternative sources of financing, or to reduce expenditures. We cannot guarantee that such waivers, amendments or alternative financing could be obtained or, if obtained, would be on terms acceptable to us.

Upon the occurrence of a default, or if we are unable to make the representations and warranties in the credit agreement governing our Credit Facilities, we will not be able to borrow funds or issue letters of credit under our Credit Facilities. Upon the occurrence of an event of default, our lenders could elect to declare all amounts outstanding under our Credit Facilities to be immediately due and payable. If we are unable to repay that amount, our lenders could seize our assets securing the loans and our business and financial condition could be materially and adversely affected.

Our Series A Convertible Preferred Stock (the "Series A Preferred Stock"), Series B Convertible Preferred Stock (the "Series B Preferred Stock") and investment agreement restrict our ability to incur certain indebtedness which limits our flexibility in operating our business.

In February 2019, we issued Series A Preferred Stock established by a Certificate of Designations (the "Series A Certificate of Designations") and Series B Preferred Stock established by a Certificate of Designations (the "Series B Certificate of Designations"), which contain covenants that, among other things, require the consent of the holders of a majority of each of the then-outstanding shares of Series A Preferred Stock and Series B Preferred Stock before we

can incur indebtedness in excess of a specified leverage ratio.

In January 2019, we entered into an investment agreement with an investment fund managed by True Wind Capital (the “Investor”), which contains customary covenants, including among others, that for so long as any shares of preferred stock issued pursuant to the investment agreement are outstanding, the consent of the Investor will be necessary for us to issue, subject to certain exceptions, any debt securities convertible into any of our capital stock.

We may need additional capital, and we cannot be certain that additional financing will be available.

We may require additional financing in the future to operate or expand our business, acquire assets or repay or refinance our existing debt. Our ability to obtain financing will depend, among other things, on our business development efforts, business plans, operating performance and the condition of the capital markets at the time we seek financing, as well as other factors beyond our control. We cannot provide any assurance that additional financing will be available to us on favorable terms when required, or at all. Additionally, under the terms of our credit agreement, preferred stock and investment agreement, respectively, we are restricted from incurring additional debt, subject to certain exceptions. If we raise additional funds through the issuance of equity, equity-linked or debt securities, those securities may have rights, preferences or privileges senior to the rights of our common stock or preferred stock, and our stockholders may experience dilution.

If we need additional capital and cannot raise it on acceptable terms, we may not be able to, among other things:

- develop or enhance our solutions;
- continue to expand our sales and marketing and research and development organizations;
- repay or refinance our existing debt;
- acquire complementary technologies, solutions or businesses;
- expand operations, in the United States or internationally;
- hire, train and retain employees; or
- respond to competitive pressure or unanticipated working capital requirements.

Our failure to do any of these things could seriously impact our business, negatively affecting financial condition and operating results.

We may be able to incur more debt and take other actions that could diminish our ability to make payments on our indebtedness when due, which could further exacerbate the risks associated with our current level of indebtedness.

Despite our current indebtedness level, we may be able to incur more indebtedness in the future. We are not completely prohibited under the terms of the credit agreement, preferred stock, investment agreement or other agreements governing our current indebtedness from incurring additional debt, securing existing or future debt, recapitalizing our debt or taking a number of other actions, any of which could diminish our ability to make payments on our indebtedness when due and further exacerbate the risks associated with our current level of indebtedness. If new debt is added to our or any of our existing and future subsidiaries' current debt, the related risks that we now face could intensify.

Our preferred stockholders can exercise significant control over the Company, which could limit the ability of our common stockholders to influence the outcome of key transactions, including a change of control.

The Investor holds approximately 16.6% of our outstanding voting capital stock based on the number of shares of common stock and convertible Series A Preferred Stock outstanding as of March 6, 2019, on an as-converted basis. If Stockholder Approval (as defined in the investment agreement) is obtained, the Investor will have an aggregate voting power of at least 24.2% of our outstanding capital stock on the date of such Stockholder Approval, which amount may increase based on the accrued value of the Series B Preferred Stock at conversion. In addition, the Investor’s aggregate voting power will increase further in connection with future accretion of the Series A Preferred Stock for as long as the Series A Preferred Stock remains outstanding. The holders of our Series A Preferred Stock are entitled to vote their shares, on an as-converted basis, together with holders of our common stock on all matters submitted to a vote of the holders of our common stock. As a result, the holders of shares of the Series A Preferred Stock have the ability to significantly influence the outcome of any matter submitted for the vote of the holders of our common stock. The Investor is entitled to act separately in its own respective interests with respect to its ownership interests in the Company and has the ability to substantially influence the election of the members of our Board of Directors, thereby potentially controlling our management and affairs. In addition, the Investor has significant influence over all matters

that require approval by our stockholders, including the approval of significant corporate transactions.

Additionally, holders of a majority of the then-outstanding shares of Series A Preferred Stock are required to approve certain matters as a class, voting separately from the common stock, such as (1) any amendment, alteration or repeal to our Restated Articles of Incorporation (the "Articles of Incorporation") or the Series A Certificate of Designations in a manner that would adversely affect the rights, preferences, privileges or power of the Series A Preferred Stock; (2) any amendment or alteration to our Articles of Incorporation or any other action to authorize or create, or increase the number of authorized or issued shares of, or any securities convertible into shares of, or reclassify any security into, or issue any parity stock or senior stock as to dividend or liquidation rights; (3) the issuance of shares of Series A Preferred Stock other than in connection with the conversion of Series B Preferred Stock that

was issued on the Issue Date; (4) any action that would cause us to cease to be treated as a domestic corporation for U.S. federal income tax purposes; or (5) the incurrence of indebtedness that would cause us to exceed a specified leverage ratio.

Further, holders of a majority of the then-outstanding shares of Series B Preferred Stock, are required to approve certain matters as a class, voting separately from the common stock and the Series A Preferred Stock, such as (1) any amendment, alteration or repeal to our Articles of Incorporation or the Series B Certificate of Designations in a manner that would adversely affect the rights, preferences, privileges or power of the Series B Preferred Stock; (2) any amendment or alteration to our Articles of Incorporation or any other action to authorize or create, or increase the number of authorized or issued shares of, or any securities convertible into shares of, or reclassify any security into, or issue any parity stock or senior stock as to dividend or liquidation rights; (3) the issuance of any additional shares of Series B Preferred Stock; (4) any action that would cause us to cease to be treated as a domestic corporation for U.S. federal income tax purposes; or (5) the incurrence of indebtedness that would cause us to exceed a specified leverage ratio.

Any issuance of common stock upon conversion of the Series A Preferred Stock and the issuance of Series A Preferred Stock upon automatic conversion of the Series B Preferred Stock in connection with the Stockholder Approval will cause dilution to existing stockholders and may depress the market price of our common stock.

The Series A Preferred Stock has an initial stated value of $1,000 per share, which stated value will accrete at an annual rate of 8% per annum, compounded quarterly. Each share of Series A Preferred Stock is convertible, at the option of the holders, into (i) the number of shares of common stock equal to the product of (A) the stated value per share as it has accreted as of such date multiplied by (B) the Conversion Rate as of the applicable conversion date divided by (C) 1,000 plus (ii) cash in lieu of fractional shares. The initial Conversion Rate is equal to 166.11 shares of our common stock and is subject to adjustment from time to time upon the occurrence of certain customary events in accordance with the terms of the Series A Certificate of Designations. Each share of Series A Preferred Stock is entitled to participate in dividends paid in respect of the common stock on an as-converted basis.

The issuance of common stock upon conversion of the Series A Preferred Stock (including any shares of Series A Preferred Stock issued upon automatic conversion of the Series B Preferred Stock in connection with the Stockholder Approval) will result in immediate and substantial dilution to the interests of our common stock holders, and such dilution will increase over time in connection with the future accretion of the Series A Preferred Stock and the conversion of Series B Preferred Stock into Series A Preferred Stock (assuming Stockholder Approval is obtained).

Texas law and our Articles of Incorporation and bylaws contain certain provisions, including anti-takeover provisions, that limit the ability of stockholders to take certain actions and could delay or discourage takeover attempts that stockholders may consider favorable.

The Texas Business Organizations Code, as amended (“TBOC”), and our Articles of Incorporation and second amended and restated bylaws contain provisions that could have the effect of rendering more difficult, delaying, or preventing an acquisition deemed undesirable by our Board of Directors and therefore depress the trading price of our common stock. These provisions could also make it difficult for stockholders to take certain actions, including electing directors who are not nominated by the current members of our Board of Directors or taking other corporate actions,

including effecting changes in our management. Among other things, our certificate of incorporation and bylaws include provisions regarding:

- the ability of our Board of Directors to issue shares of preferred stock, including "blank check" preferred stock, and to determine the price and other terms of those shares, including preferences and voting rights, without stockholder approval, which could be used to significantly dilute the ownership of a hostile acquirer, and pursuant to which we have issued the Series A Preferred Stock and Series B Preferred Stock, each of which are entitled to receive a liquidation preference and certain amounts in connection with a change of control of the company and other similar extraordinary transactions;

- the limitation of the liability of, and the indemnification of, our directors and officers;

- the requirement that directors may only be removed from our Board of Directors by the affirmative vote of a majority of the issued and outstanding shares entitled to vote in the election of directors at a special meeting of the shareholders called for that purpose at which quorum is present;

- a prohibition on common stockholder action by written consent, which forces common stockholder action to be taken at an annual or special meeting of stockholders and could delay the ability of stockholders to force consideration of a stockholder proposal or to take other action, including the removal of directors;

- the requirement that a special meeting of stockholders may be called only by the chairperson of our Board of Directors, our Board of Directors or a holder of at least 10% of all of the shares of the Company entitled to vote at the proposed special meeting, and must be called by our president or secretary at the request in writing of a majority of the members of

our Board of Directors, which could delay the ability of stockholders to force consideration of a proposal or to take action, including the removal of directors;

- provisions enabling us to control the procedures for the conduct and scheduling of Board of Directors and stockholder meetings;

- the requirement for the affirmative vote of holders of at least a majority of all issued and outstanding shares entitled to vote in the election of directors at a properly called and convened annual or special meeting of shareholders, to amend, alter, change or repeal any provision of our Articles of Incorporation or our bylaws, which could preclude stockholders from bringing matters before annual or special meetings of stockholders and delay changes in our Board of Directors and also may inhibit the ability of an acquirer to effect such amendments to facilitate an unsolicited takeover attempt;

- the ability of our Board of Directors to amend our bylaws, which may allow our Board of Directors to take additional actions to prevent an unsolicited takeover and inhibit the ability of an acquirer to amend our bylaws to facilitate an unsolicited takeover attempt; and

- advance notice procedures with which stockholders must comply to nominate candidates to our Board of Directors or to propose matters to be acted upon at a stockholders' meeting, which could preclude stockholders from bringing matters before annual or special meetings of stockholders and delay changes in our Board of Directors and also may discourage or deter a potential acquirer from conducting a solicitation of proxies to elect the acquirer's own slate of directors or otherwise attempting to obtain control of our Company.

These provisions, alone or together, could delay or prevent hostile takeovers and changes in control or changes in our Board of Directors or management.

In addition, as a Texas corporation, we are subject to provisions of Texas law, including Section 21.606 of the TBOC, which may prohibit certain stockholders holding 20% or more of our outstanding capital stock from engaging in certain business combinations with us for a specified period of time.

Any provision of Texas law or our Articles of Incorporation or bylaws that has the effect of delaying or preventing a change in control could limit the opportunity for our stockholders to receive a premium for their shares of our capital stock and could also affect the price that some investors are willing to pay for our common stock.

Other Risks Related to our Series A Preferred Stock and Series B Preferred Stock

Future resales of our common stock held by our significant stockholders or of the shares of common stock issuable upon conversation of the Series A Preferred Stock may cause the market price of our common stock to drop significantly.

We are obligated to register the resale of the common stock issuable upon conversion of, or issued as dividends upon, the Series A Preferred Stock, and to take certain actions to facilitate the transfer and sale of such shares. Upon such registration, shares of common stock into which the Series A Preferred Stock are converted would be freely tradable. The common stock issuable upon conversion may represent overhang that may also adversely affect the market price of our common stock. Overhang occurs when there is a greater supply of a company's stock in the market than there is demand for that stock. When this happens, the price of the company's stock will decrease, and any additional shares which stockholders attempt to sell in the market, or the perception that such sales might occur, will only further decrease the share price. If the share volume of our common stock cannot absorb converted shares sold by the holders of the Series A Preferred Stock, then the value of our common stock will likely decrease.

Any sale of large amounts of our common stock on the open market or in privately negotiated transactions could have the effect of increasing the volatility in the price of our common stock or putting significant downward pressure on the price of our common stock.

Our Series A Preferred Stock and Series B Preferred Stock have rights, preferences and privileges that are not held by, and are preferential to, the rights of our common stockholders, which could adversely affect our liquidity and financial condition, and may result in the interests of the holders of our Series A Preferred Stock and Series B Preferred Stock differing from those of our common stockholders.

In the event of our liquidation, dissolution or the winding up of our affairs, the holders of our Series A Preferred Stock have the right to receive a liquidation preference entitling them to be paid out of our assets generally available for distribution to our equity holders, together with holders of our Series B Preferred Stock and before any payment may be made to holders of any other class or series of capital stock (including our common stock), in an amount equal to the greater of (i) $1,000 plus all accreted but unpaid

dividends and (ii) the amount such holder would have been entitled to receive if the Series A Preferred Stock had converted into common stock immediately prior to such liquidation.

In the event of our liquidation, dissolution or the winding up of our affairs, the holders of our Series B Preferred Stock have the right to receive a liquidation preference entitling them to be paid out of our assets generally available for distribution to our equity holders, together with holders of our Series A Preferred Stock and before any payment may be made to holders of any other class or series of capital stock (including our common stock), in an amount equal to $1,000 plus all accrued but unpaid dividends.

In addition, the $1,000 stated value per share of our Series A Preferred Stock will accrete at a fixed rate of 8.0% per annum, compounded quarterly. The holders Series A Preferred Stock are also entitled to receive any dividends paid in respect of our common stock on an as-converted basis. The holders of our Series B Preferred Stock are entitled to receive dividends accruing daily on a cumulative basis payable quarterly in arrears in cash at a fixed rate of 10.0% per annum on the $1,000 stated value per share (the "Dividend Rate"), which rate will automatically increase by 1.0% every six months that the Series B Preferred Stock remains outstanding and unconverted (subject to a cap of 12.0%). If cash dividends are not paid in respect of any dividend payment period, the liquidation preference of each outstanding share of Series B Preferred Stock will automatically increase at the Dividend Rate.

Further, the Series A Preferred Stock is mandatorily redeemable upon a change of control (as defined in the Series A Certificate of Designations), at a price per share of Series A Preferred Stock in cash equal to the greater of (i) the Series A Change of Control Redemption Price (as defined below) and (ii) (A) the amount of cash such holder of Series A Preferred Stock would have received plus (B) the fair market value of any other assets such holder would have received, in each case had such holder of the Series A Preferred Stock, immediately prior to such change of control, converted such shares of Series A Preferred Stock into shares of common stock. The "Series A Change of Control Redemption Price" per share of Series A Preferred Stock is the product of the accreted value of such share as of the date of determination multiplied by (1) 1.30 (if the change of control occurs before the first anniversary of the date of issuance); (2) 1.35 (if the change of control occurs on or after the first anniversary of the date of issuance but before the second anniversary of the date of issuance); (3) 1.40 (if the change of control occurs on or after the second anniversary of the date of issuance but before the third anniversary of the date of issuance); (4) 1.45 (if the change of control occurs on or after the third anniversary of the date of issuance but before the fourth anniversary of the date of issuance); and (5) 1.50 (if the change of control occurs on or after the fourth anniversary of the date of issuance).

Further, the holders of our Series B Preferred Stock also have redemption rights upon the occurrence of certain events. Specifically, the Series B Preferred Stock is mandatorily redeemable, upon the holder's election and after 90 days prior notice, any time after the seventh anniversary of the date of issuance at an amount per share of Series B Preferred Stock equal to the liquidation preference per share of the Series B Preferred Stock to be redeemed as of the applicable redemption date multiplied by 1.50. The Series B Preferred Stock is also mandatorily redeemable upon a change of control (as defined in the Series B Certificate of Designations), at a price per share of Series B Preferred Stock in cash equal to the greater of (i) the Series B Change of Control Redemption Price (as defined below) and (ii) (A) the amount of cash such holder of Series B Preferred Stock would have received plus (B) the fair market value of any other assets in each case had such holder of Series B Preferred Stock, immediately prior to such change of control, converted such shares of Series B Preferred Stock into shares of Series A Preferred Stock. The "Series B Change of Control Redemption Price" per share of Series B Preferred Stock is the product of the liquidation preference of such share as of the date of determination multiplied by (1) 1.30 (if the change of control occurs before the first anniversary of the date of issuance); (2) 1.35 (if the change of control occurs on or after the first anniversary of the date of issuance but before the second anniversary of the date of issuance); (3) 1.40 (if the change of control occurs on or after the second anniversary of the date of issuance but before the third anniversary of the date of issuance); (4) 1.45 (if the change of control occurs on or after the third anniversary of the date of issuance but before the fourth anniversary of the date of issuance); and (5) 1.50 (if the change of control occurs on or after the fourth anniversary of the date of issuance).

Finally, any time after the fourth anniversary of the date of issuance of the Series A Preferred Stock, we have the right to redeem the Series A Preferred Stock for cash at a redemption price equal to the accreted value per share of Series A Preferred Stock to be redeemed multiplied by 1.50. Likewise, at any time after the fourth anniversary of the date of issuance of the Series B Preferred Stock, we have the right to redeem the shares of the Series B Preferred Stock for cash at a redemption price equal to the liquidation preference per share of the Series B Preferred Stock to be redeemed multiplied by 1.50.

These dividend and redemption payment obligations could significantly impact our liquidity and reduce the amount of our cash flows that are available for working capital, capital expenditures, growth opportunities, acquisitions, and other general corporate purposes. Our obligations to the holders of Series A Preferred Stock and Series B Preferred Stock could also limit our ability to obtain additional financing or increase our borrowing costs, which could have an adverse effect on our financial condition. The preferential rights described above could also result in divergent interests between the holders of shares of Series A Preferred Stock and/or Series B Preferred Stock and the holders of our common stock.

Item 1B. Unresolved Staff Comments

None.

Item 2. Properties

We leased properties during 2018 that are considered significant to the operations of the business in the following locations: Burlington, Massachusetts; Ann Arbor, Michigan; Renton, Washington; Ottawa, Ontario, Canada; the United Kingdom; and Dallas and Austin, Texas. Our Burlington employees perform sales and marketing activities. Our Ann Arbor employees perform the support and development of our ZixProtect product line, which we acquired with our purchase of Greenview. Our Renton employees perform support and development for our ZixArchive product line, which we acquired with our purchase of Erado. 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 and 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.

Item 3. Legal Proceedings

We are subject to legal proceedings, claims, and litigation involving our business. While the outcome of these matters is currently not determinable, and the costs and expenses of resolving 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 condition or operating results.

Item 4. Mine Safety Disclosures

Not applicable.

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 2018 and 2017.

	2018		2017	
Quarter Ended	High	Low	High	Low
March 31	$4.75	$3.82	$5.41	$4.60
June 30	$5.62	$4.25	$6.67	$4.75
September 30	$5.93	$4.91	$6.04	$4.55
December 31	$7.09	$4.66	$5.40	$4.16

At March 6, 2019, there were 54,089,273 shares of common stock outstanding held by 397 shareholders of record. On that date, the last reported sales price of the common stock was $7.17.

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

For information regarding options and 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, 2018, 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, 2013, in our common stock and in each of the two indices and assumes reinvestment of all dividends, if any. The stock price performance on the following graph is not necessarily indicative of future stock price 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.

Sale of Unregistered Securities

None.

Purchases of Equity Securities by the Issuer

Period	Total Number of Shares Purchased[1]	Average Price Paid per Share	Total Number of Shares Purchased as part of Publicly Announced Plans or Programs	Maximum Number (or Appropriate Dollar Value) of Shares (or Units) that May Yet Be Purchased Under the Plans or Programs
October 1, 2018 to October 31, 2018	—	$ —	—	$ —
November 1, 2018 to November 30, 2018	914	$ 6.67	—	$ —
December 1, 2018 to December 31, 2018	—	$ —	—	$ —
Total	914	$ 6.67	—	$ —

[1] Of the total number of shares repurchased for the one month period ended November 30, 2018, 914 shares of Restricted Stock were withheld by us upon the vesting of outstanding Restricted Stock. These shares were withheld by us to satisfy the minimum statutory tax withholding for the employees for whom Restricted Stock vested during the applicable period, which is required once the Restricted Stock is vested.

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," and the consolidated financial statements and notes thereto. No cash dividends were declared in any of the five years shown below:

	Year Ended December 31,				
	2018	2017	2016	2015	2014
	(In thousands, except per share data)				
Statement of Operations Data:					
Revenues	$70,478	$65,663	$60,144	$54,713	$50,347
Cost of revenue	15,186	12,602	10,533	9,593	8,324
Gross margin	55,292	53,061	49,611	45,120	42,023
Research and development expenses	11,323	10,980	9,553	8,317	9,051
Selling, general and administrative expenses	33,999	31,871	30,742	28,887	26,222
Income tax expense (benefit)[1]	(4,720)	18,606	3,692	3,144	2,830
Net income (loss)	15,444	(8,057)	5,837	5,016	4,103
Basic income (loss) per common share	$0.29	$(0.15)	$0.11	$0.09	$0.07
Diluted income (loss) per common share	$0.29	$(0.15)	$0.11	$0.09	$0.07
Shares used in computing basic income per common share	52,592	53,430	53,820	56,422	57,949
Shares used in computing diluted income per common share	53,481	53,430	54,395	57,476	58,967
Statements of Cash Flows Data:					
Net cash flows provided by (used for):					
Operating activities	$16,671	$18,204	$15,251	$15,617	$13,317
Investing activities	(15,952)	(11,285)	(2,136)	(1,951)	(3,402)
Financing activities	(6,593)	(367)	(15,322)	(6,687)	(15,748)
Balance Sheet Data:					
Cash, Cash Equivalents and Marketable Securities	$27,109	$33,009	$26,457	$28,664	$21,685
Working capital[2]	(7,665)	2,104	2	3,821	2,249
Total assets	104,640	81,308	82,358	87,286	83,724
Stockholders' equity	60,947	43,520	49,070	56,772	56,270

(1) The $4.7 million income tax benefit in 2018 resulted from the release of a portion of our deferred tax asset valuation allowance. Based on analysis of both projected and current earnings, we have estimated our deferred tax asset as likely to be utilized prior to expiration, thus triggering this release. On December 22, 2017, the U.S. enacted the Tax Cuts and Jobs Act of 2017 (the "Tax Act") which significantly changed U.S. tax law. The Tax Act lowered the Company's statutory federal income tax rate from 34% to 21% effective January 1, 2018. At December 31, 2017, the Company adjusted its deferred tax balances to reflect the new tax rate that resulted in income tax expense of $12.5 million in that year. See "Income Taxes" in "Item 7. Management's Discussion and Analysis of Financial Condition and Results of Operations."

(2) Working capital includes deferred revenue totaling $30.6 million, $28.4 million, $25.8 million, $23.2 million and $21.6 million, as of December 31, 2018, 2017, 2016, 2015, and 2014, respectively.

25

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

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 in this report 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. See "NOTE ON FORWARD-LOOKING STATEMENTS AND RISK FACTORS" in "Item 1. Business."

The following discussion should be read in conjunction with the consolidated financial statements and related notes beginning on page F-1.