

## Risk Factors Comparison 2024-11-25 to 2023-11-22 Form: 10-K

Legend: **New Text** ~~Removed Text~~ Unchanged Text **Moved Text** Section

• Unauthorized disclosure, destruction or modification of data or disruption of our services or other cybersecurity or technological risks, **including as a result of a cybersecurity incident**, could expose us to liability, protracted and costly litigation and damage our reputation. • Our software and systems and our third- party providers' software and systems may fail, or our third- party providers may discontinue providing their services or technology generally or to us specifically, which in either case could interrupt our business, cause us to lose business and increase our costs. • Some of our solutions contain "open source" software, and any failure to comply with the terms of one or more of applicable open- source licenses could negatively affect our business. • We have a history of operating losses and will need to generate significant revenues to attain and maintain profitability and positive cash flow and continue our acquisition program. • The vertical market software ~~and payment processing industries~~ **industry are is** highly competitive. Such competition could adversely affect the revenue we receive, and as a result, our margins, business, financial condition and results of operations. ~~• To acquire and retain customers, we depend in part on distribution partners that generally do not serve us exclusively, may not aggressively market our products and services, are subject to attrition and are not under our control.~~ • If we cannot keep pace with rapid developments and changes in our industry, the use of our products and services could decline, causing a reduction in our revenues. • If we fail to comply with the applicable requirements of the Visa and Mastercard payment networks, those payment networks could seek to fine us, suspend us or terminate our registrations through our bank ~~sponsors~~ **sponsor**. • If our bank ~~sponsorships~~ **sponsorship are is** terminated and we are not able to secure or successfully migrate ~~our payment facilitator customer portfolios~~ **portfolio to a** new bank ~~sponsors~~ **sponsor**, we will not be able to conduct our business. • **If our processing services agreement with Payroc is terminated and we are not able to enter into a replacement processing relationship with another party, our ability to provide payment processing services to our affected software customers may be adversely impacted.** • Consolidation in the banking and financial services industry could adversely affect our business, results of operations and financial condition. • We have faced, and may in the future face, ~~significant chargeback liability~~ **liabilities** if our customers refuse or cannot reimburse chargebacks resolved in favor of their customers, and we may not accurately anticipate these liabilities. • On occasion, we experience increases in interchange and sponsorship fees; if we cannot pass these increases along to our customers, our profit margins will be reduced. • Third- party hardware that we sell to our customers is generally procured from a limited number of suppliers. Thus, we are at risk of shortages, price increases, changes, delays or discontinuations of hardware, which could disrupt our business. • We are subject to economic and political risk, the business cycles of our customers and ~~distribution partners and~~ changes in the overall level of consumer and commercial spending, which could negatively impact our business, financial condition and results of operations. • ~~and risks associated with rapidly~~ **Rapidly** evolving domestic and global conditions ~~which are beyond our control~~ **and could materially adversely affect our business, operations and results of operations.** • A decline in the use of cards and ACH as payment mechanisms for consumers and businesses or adverse developments in the electronic payment industry in general could adversely affect our business, financial condition and operating results. • We may not be able to successfully execute our strategy of growth through acquisitions. • Revenues and profits generated via acquisition may be less than anticipated, the integration process could experience delays or difficulties, and we may fail to uncover all liabilities of acquisition targets through the due diligence process prior to an acquisition, resulting in unanticipated costs, losses or a decline in profits, as well as potential impairment charges. • We may not be able to successfully manage our intellectual property and we may be subject to infringement claims. • ~~If we lose key personnel, or if their reputations are damaged, our business, financial condition and results of operations may be adversely affected, and proprietary information of our company could be shared with our competitors.~~ • In a dynamic industry like ours, our success and growth depend on our ability to attract, recruit, retain and develop qualified employees, **and if we lose key personnel, or if their reputations are damaged, our business, financial condition and results of operations may be adversely affected, and proprietary information of our company could be shared with our competitors.** • Our operating results and operating metrics are subject to seasonality and volatility, which could result in fluctuations in our quarterly revenues and operating results or in perceptions of our business prospects. • We are the subject of various claims and legal proceedings ~~and~~, may become the subject of claims, litigation or investigations **and may be a party to regulatory and other proceedings.** • We are exposed to fluctuations in foreign currency exchange rates, which could negatively affect our financial condition and operating results. • Our international operations subject us to additional risks. • We are subject to extensive **laws and** government regulation, **the cost of compliance with which can be significant, and our actual or perceived failure to comply with such obligations may subject us to penalties and otherwise have and ~~an any~~ **unfavorable impact on our business, financial condition and results of operations.** • **Any** new laws and regulations, industry standards or revisions made to existing laws, regulations or industry standards affecting the electronic payments industry, and the other industries in which we provide services, or our actual or perceived failure to comply with such obligations, may have an unfavorable impact on our business, financial condition and results of operations. • ~~Changing laws and governmental rules and regulations designed to protect or limit access to or use of personal information could adversely affect our ability to effectively provide our products and services, and actual or perceived failure to comply with such legal and regulatory obligations may negatively impact our business, financial condition and results of operations.~~ • Actual or perceived failures to comply with applicable healthcare laws and regulations could result in a material breach of contract with one or more of our customers in our Healthcare vertical, harm our reputation and subject us to substantial civil and criminal **penalties.** • **Actual or perceived failures to comply with processing related disclosure or fee regulations****

could result in material breach of contract with one or more of our customers, harm our reputation, result in diminished revenue, or subject us to civil penalties. • We could be adversely affected by violations of the FCPA and similar anti-bribery laws of other countries in which we provide services or have employees. • Changes in tax laws or their interpretations, or becoming subject to additional U. S., state or local taxes that cannot be passed through to our customers, could negatively affect our business, financial condition and results of operations. • **Changing laws and governmental rules and regulations designed to protect or limit access to or use of personal information could adversely affect our ability to effectively provide our products and services, and actual or perceived failure to comply with such legal and regulatory obligations may negatively impact our business, financial condition and results of operations.** • Our indebtedness could adversely affect our financial health and competitive position ~~and we~~ → We may not be able to secure additional financing on favorable terms, or at all, to meet our future capital needs, **including the funds necessary to settle exchanges or the repurchase of Exchangeable Notes**. • We ~~are~~ may not have the ability to raise the funds necessary to settle exchanges of the Exchangeable Notes or to repurchase the Exchangeable Notes upon a **holding company with no** fundamental change. • The conditional exchange feature of the Exchangeable Notes, if triggered, may adversely affect our financial condition and operating **operations results of our own, and our principal asset is our controlling membership interest in i3 Verticals, LLC, and we depend on distributions from i3 Verticals, LLC**. • In certain cases, payments under the Tax Receivable Agreement to the Continuing Equity Owners may be accelerated or significantly exceed the actual benefits we realize in respect of the tax attributes subject to the Tax Receivable Agreement. • Our failure to maintain effective internal control over financial reporting in accordance with Section 404 of the Sarbanes- Oxley Act could have a significant and adverse effect on our business, financial condition, results of operations and reputation. • Certain provisions of Delaware law and anti- takeover provisions in our organizational documents could delay or prevent a change of control. • **Holders of our Class A common stock may be diluted by future issuances of preferred stock or additional Class A common stock or common units in connection with our incentive plans, acquisitions or otherwise; future sales of such shares in the public market could lower our stock price.** • **Due to the effect of discontinued operations for our Merchant Services Business, the Company’ s historical consolidated financial statements included in prior periodic reports are not comparable to the consolidated financial statements included in this Annual Report on Form 10- K and will not be comparable to the Company’ s future consolidated financial results.** • **There are certain risks associated with the sale of our Merchant Services Business which was completed in September 2024.**

**PART I Item 1. Business** Our Company i3 Verticals builds, acquires and grows software solutions in **strategic the Public Sector and Healthcare** vertical markets. Our broad array of **specialized enterprise** solutions ~~meet our~~ **deeply integrate within** customers’ **operations, specific enterprise needs** which leads to long- term partnerships. **Since our founding in 2012, we have compounded cash flow through a combination of organic growth and acquisitions.** Our cash flow generation and strong recurring revenue model has positioned us with an ideal financial structure to capitalize on **strategic growth opportunities for years to come.** Sale of Merchant Services Business On September 20, 2024, i3 Verticals, LLC, and i3 Holdings Sub, Inc., a wholly- owned subsidiary of i3 Verticals, LLC (“ Corporation Seller, ” and collectively with i3 Verticals, LLC, the “ Sellers ”) completed the transactions (such closing, the “ Closing ”) contemplated by that certain Securities Purchase Agreement dated as of June 26, 2024 (the “ Purchase Agreement ”), by and among i3 Verticals, LLC, Corporation Seller, the Company (solely for the purpose of providing a guaranty of the obligations of Sellers as set forth in the Purchase Agreement), Payroc Buyer, LLC (“ Buyer ”), and Payroc WorldAccess, LLC (solely for the purpose of providing a guaranty of the obligations of Buyer as set forth in the Purchase Agreement), the entry into which Purchase Agreement was previously disclosed in a Current Report on Form 8- K filed by the Company on June 26, 2024. Pursuant to the terms of the Purchase Agreement, the Sellers sold to Buyer the equity interests of certain direct and indirect wholly- owned subsidiaries of Sellers (the “ Acquired Entities ”) primarily comprising the Company’ s merchant services business, including its associated proprietary technology (the “ Merchant Services Business ”), after giving effect to the contribution of certain assets and the assignment of certain liabilities associated with the Merchant Services Business from i3 Verticals, LLC and certain affiliates to the Acquired Entities pursuant to a contribution agreement which was entered into immediately prior to the Closing. Pursuant to the terms of the Purchase Agreement, Buyer paid to Sellers an aggregate purchase price of approximately \$ 438 million (after giving effect to estimated net working capital, indebtedness and cash adjustments), payable in cash at the Closing, subject to post- closing purchase price adjustments.

**Organic Growth in Strategic Vertical Markets** The ability to organically grow revenue over the long term is the result of expanding recurring revenue streams, strategic selection of markets and continued investment in our products. **Approximately 80 % of our revenue from continuing operations is considered recurring.** We earn the majority of our revenue from software and related services. We also earn revenue from volume and transaction- based fees for **payments - payment processing services, all of which is integrated into our software.** Our proprietary payment facilitator platform seamlessly integrates into our **software** solutions, unlocking additional value. Revenue from software and related services accounts for 50 % of our total revenue for the twelve months ended September 30, 2023, up from 5 % for the twelve months ended September 30, 2017. Since our founding in 2012, we have steadily increased our market share and solution breadth through a combination of organic growth initiatives and acquisitions. Our cash flow generation has positioned us to capitalize on **strategic opportunities and position ourselves to expand our product offerings for years to come.** We focus on **strategic solutions in the Public Sector and Healthcare vertical and sub- vertical markets because of the following characteristics** where we can build lasting customer relationships. Our primary markets are underserved, fragmented, large, and growing. Our primary strategic vertical markets include: • **Technologically underserved markets** • **Large Public Sector** — We have products and solutions growing total addressable markets • **Fragmented competitive landscape** • **Ample opportunity for transaction- based revenues** • **Insulation from market cycles** With deep integration into our customers’ operations, we believe that **create we are well positioned to conceive an and build** efficient flow of information throughout a variety of public sector

entities, including states and local governments. Our solutions help our customers provide more responsive and efficient services to their citizens. We have products that enable upper **meet their growing needs. Ongoing investment into improving existing platforms and strategically creating new platforms and products is** and **an lower essential part of court -- our long** case management, collections, finance and accounting, motor vehicle and carrier registration, e- **term strategy** filing and taxation, license plate inventory, property tax management, utility billing, professional licensing, document workflow, and law enforcement software. **Ability** We deliver integrated payments solutions throughout many of these products and these solutions allow our customers to **Use Acquisitions to** efficiently process court, tax, registration, utility and other payments. We also assist public schools in completing payment processing functions such as accepting payments for school lunches (online or at school) and school activities. • **Healthcare** — We provide entities in the healthcare market with software platforms that drive **Drive Growth** process efficiency and ensure compliance. These include electronic healthcare records ("EHR") and revenue cycle management solutions, often paired together. We offer our software as a service and often bundle it with professional services that specialize in outsourced revenue cycle management, including coding. We also provide insurance adjudication, patient engagement platforms, billing, scheduling and integrated payments solutions. Our payment solutions in the healthcare market seamlessly integrate into our own proprietary software, as well as that of our distribution partners, consisting of independent software vendors ("ISVs"). We also provide workflow software and associated professional services to medical insurance payers. Our customers include multiple large academic medical institutions, multiple large payer networks, billing organizations and individual physician practices. A core component of our growth strategy includes a disciplined approach to acquisitions of companies and technology, evidenced by **48-50** acquisitions since our inception in 2012. Our acquisitions have opened new strategic vertical markets, increased the number of businesses and organizations to whom we provide solutions and extended our existing software solutions and capabilities. We target vertical markets where businesses and organizations often lack integrated payment functionality within their business management systems. When we present software solutions that integrate the customer's operations with their payments, we can build a long-term relationship primed to grow together. Our management team has significant experience acquiring and integrating vertical market software businesses that complement our existing suite of products and solutions. **Due to Acquisitions have extended** our **product offerings team's long-standing relationships and domain capabilities, thereby allowing us to enhance our value proposition to our customers. They have also increased our addressable markets. Target businesses are generally founder lead, growing, generating cash flow, and have been in our core vertical markets. Through our proprietary payment facilitator platform we have scale, pricing and expertise in payments. As a result**, we often identify targets who lack integrated payment functionality within their solutions or have **under- monetized the opportunity. We** maintain a strong pipeline of acquisition targets and are constantly evaluating businesses against our acquisition criteria. We generate revenue from software licenses and subscriptions, ongoing support, and other software-related solutions. We also generate revenue from volume-based fees generated by payment processing services provided to customers throughout North America. Our software and integrated payment solutions coupled with our distribution network derive significant scale from operating efficiencies, which enables us to generate strong operating margins and cash flows. Our Segments We **As a result of the sale of the Merchant Services Business as described above, our entire former Merchant Services segment and a small portion of the historical Software and Services segment which were included in the Merchant Services Business have been reflected in discontinued operations in the Company's consolidated financial statements. After giving effect to these developments, the Company has** two reportable segments, Software-Public Sector and **Healthcare** Services and Merchant Services, and an Other category. For additional information on our segments, see Note 17-**18** to our consolidated financial statements and "Management's Discussion and Analysis of Financial Condition and Results of Operations." Our Software **We have products** and Services segment delivers vertical market software solutions **that create** to customers across all of our strategic vertical markets. These solutions often include embedded payments or other recurring services. Our Merchant Services segment provides comprehensive payment solutions to businesses and **an efficient flow of** organizations. Our Merchant Services segment includes third-party integrated payment solutions as well as traditional merchant processing services across our strategic vertical markets. Our Other category includes corporate overhead expenses, when presenting reportable segment information **throughout**. Our Products and Solutions We deliver a **variety** comprehensive array of **public sector** vertical market software solutions and integrated payment technology to our customers and distribution partners. Our products and solutions are strategically aligned to support new customer growth and promote customer retention. Some solutions are broadly applicable across many different types of entities and departments, while others are specific to certain markets. Our Public Sector vertical is comprised of more than 100 unique software products designed to make governments run more efficiently. Payments are often embedded into these software products, providing customers with a seamless experience as well as an additional revenue stream. We serve customers at both the state and local level and our geographic reach covers most of the United States and some of Canada. Our software products **solutions help our customers provide more responsive and efficient services to their citizens and stakeholders. There** are designed to align **five sub-verticals** with within the specific needs of our customers and their **the** communities. Solutions **Public Sector vertical:** • **JusticeTech and Public Safety: Product** categories include (1) **Judiciary & Courts: Fully fully** integrated digital solutions offering dynamic processes to plan, coordinate, evaluate, record, and provide up to date information within court systems, (2) **E- Filing and revenue cycle management solutions for courts, and (4) Solutions for computer aided dispatch, law records management, evidence management, jail management, mobile solutions, and livescan**. • **Motor Vehicle- Transportation: Products include** Comprehensive **comprehensive** solutions for driver license, vehicle title and registration and motor carrier compliance for departments of transportation in the United States and Canada. • **Utility-Utilities : Product categories include** (1) **Billing** Complete suite of billing and back-office management software solutions and services to enhance enterprise applications, improve customer experience, and increase efficiency of utility operations. • **Digital digital** Customer Engagement-Digital customer engagement platform, including web, mobile, chat, and voice options, enables intuitive self-service options for

customers to manage their data & accounts, and (2) complete suite of billing and back-office management software solutions and services to enhance enterprise applications, improve customer experience, and increase efficiency of utility operations.

- Finance and Enterprise Resource Planning ("ERP - Enterprise resource planning"): Product categories include (1 "ERP") solutions that connect the organization and its data to create a flow of information providing insight across multiple departments.
- School Lunches - Comprehensive solution for schools and districts including meal account management, (2) point of sale, menu planning, nutritional analysis, food inventory and free and reduced meal applications.
- Land & Records Management - Fully digital land records solutions to that boost proficiency and maintain records to enable submission of index information, scanning of document images and secure instantaneous retrieval of information.
- Public Safety - Solutions for computer aided dispatch, (3) licensing and permitting law records management, evidence management, jail management, mobile solutions that automate and livescan.
- Licensing & Permitting - Automation for every step of the licensing application, renewal process and payment process. These include workflow and user driven customization solutions.
- Property, Recording and Tax - (4) Digital digital solutions designed for appraisal information, tax collection management, revenue collection, and Computer Assisted Mass Appraisal.
- Education: Products include (1) comprehensive solutions for school lunch programs, including meal account management, point of sale, menu planning, nutritional analysis, food inventory and free and reduced meal applications and (2) school event solutions, including ticketing and concessions. We deliver integrated payments with our proprietary payment facilitator platform throughout many of these products. These solutions allow our customers to efficiently process court, tax, registration, utility, school and other payments.

Our Healthcare vertical segment is dedicated to delivering integrated solutions across the healthcare ecosystem, catering to providers and payers, with a strong emphasis on enhancing process efficiency and ensuring compliance. Our core offering is **There are two sub-verticals within the Healthcare vertical:**

- **Provider Software Solutions:** Products include our versatile care delivery platform, which encompasses a range of solutions, including EHR, practice management tools, patient engagement applications, and patient payment solutions. These solutions are designed to adapt to the diverse needs of healthcare organizations, from small physician practices to large academic medical institutions and multi-location health systems. By providing flexible and scalable technology solutions, we empower our clients to navigate the evolving landscape of healthcare. Complementing our technology platform, we offer a comprehensive portfolio of revenue cycle management services. These services provide our clients with a full end-to-end experience, covering all aspects of their financial operations. From revenue optimization and billing to claims processing and coding, our services are designed to streamline financial processes and maximize revenue performance for healthcare organizations.
- **Finally, our healthcare payer Payer Software solutions**

**Solutions : Products include (1)** provide payers with the tools to manage the complex healthcare industry more effectively. We offer tailored solutions for managing compliance requirements, including Appeals appeals & Grievances grievances. Additionally, **and (2) our Network-network Management management** platform assists payers in provider contracting, credentialing, and outreach, enabling them to expand and adapt to changing market dynamics. We continuously refine and expand our software offerings to stay aligned with the latest industry and current market trends. Agile Development Our flexible approach to digital delivery is centered around agility. We prioritize rapid development, continuous improvement, and dynamic responsiveness in our ever-changing environment. This means our customers receive software solutions that evolve with their needs as well as the market, ensuring they stay ahead of the curve. Our product management lifecycle life cycle ensures our products remain robust and flexible. Product roadmaps drive our investments. Our development is supported by streamlined back office technology to increase efficiency. This includes consolidated instant messaging, file sharing, and telephony ensure our solutions remain innovative. We have reduced dependency on multiple vendors across the enterprise while creating efficiency and reducing expense never grow stale. Together, **Continuous investment is these the key** initiatives support our commitment to our success operational efficiency and exceptional service delivery. Scalable Platforms We understand that scalability is critical to meeting the growing demands of the digital landscape. Our cloud-first strategy drives solutions that are designed to expand seamlessly, empowering our systems to adapt, grow, and thrive without constraints. Remaining New development is always cloud agnostic allows us native SaaS solutions. We are a sealed partner of both Amazon Web Services ("AWS") and Microsoft Azure ("Azure") cloud services. Our AWS cloud consolidation initiative is nearing successful completion, with collocated and on-premises data centers successfully migrated to choose best of breed solutions allowing us to meet the needs of our customers cloud and unifying disparate subscriptions into an enterprise account. Our strategic partnerships with multiple cloud providers give us flexibility, as well as capabilities beyond that of many of our competitors. Secure Solutions Further strengthening our technology infrastructure, we have centralized cybersecurity. **Cybersecurity is at the core of our digital strategy. We employ the latest security** measures using fully to safeguard our customers' data and systems, which are designed to protect the integrity and confidentiality of their valuable information. Our increasing investment in security protects against the ever-evolving threats in the digital realm. We rigorously adhere to data protection regulations, industry-specific compliance standards, and best practices to ensure that our customers' sensitive data is handled with the utmost care. Our solutions are designed to meet the requirements of regulatory and legal compliance. Payment Technology In addition to our broad suite of vertical market software described above, we have developed a proprietary suite of payment technology facilitation platform. We have centralized our payment solutions onto that serves customers across our vertical markets proprietary gateway, providing us excellent scale and pricing with our processing partner. Consolidation of the payments platform also reduces our overall PCI scope and increases margins by lowering expenses. Capabilities include:

- traditional merchant processing or payment facilitator models,
- integration with customer business management systems,
- integration with EMV / contactless devices,
- unified reporting for our customers across ACH, card, etc.,
- risk management,
- validated point-to-point encryption, and
- PCI-compliant security and extensive reporting tools. We offer our customers a single point of access through our powerful, but simple and capable proprietary core platform. From there we offer a suite of proprietary payment and software solutions ;

enabling omni-channel POS, spanning brick and mortar locations and electronic, web-based and mobile-commerce, including app-based payments. Our payment technology platforms include an unified Application Programming Interface ("API") suite that provides access to traditional merchant processing, ACH processing and payment facilitator merchant processing capabilities. The platform APIs allow access to Europay, Mastercard and Visa ("EMV") devices using an implementation that shields software providers from the requirements of PCI or payment application data security standard certifications. Our Technology As a forward-thinking software company that excels in delivering cutting edge solutions, we are committed to agile delivery, scalable platforms, and secure solutions. Our team of highly skilled and experienced technologists is dedicated to implementing software products that cater to the diverse and evolving needs of our customers. We continuously refine also support Paypal and Venmo payments expand our software offerings to stay aligned..... the requirements of regulatory and legal compliance. Our Sales and Marketing Our sales strategy includes both employee sales representatives and a broad network of distribution partners. We utilize our direct sales team, our largest channel, to sell our proprietary software and payment technology solutions directly to customers in our vertical markets. Sales teams are organized and coordinated by vertical and sub-vertical market, leading to extensive cross-selling opportunities across our broad array of solutions. Leveraging our vertically focused suite of products and services, we are able to maximize the performance of our employee sales force, and our external distribution channels, as we continue to attract new partners. Our external channel partners are comprised of ISVs, value-added resellers ("VARs") and a few select independent sales organizations ("ISOs"). These distribution partners are a consistent and scalable source for new customer customers acquisition. Our product and partner marketing is are delivered through a shared-services model which is coordinated with each vertical market. Marketing is tightly aligned with our sales efforts by providing event coordination, demand-generation resources, physical and electronic marketing campaigns and partner marketing collateral. Our enterprise marketing function establishes our overall corporate marketing strategy to enhance brand awareness and demand generation. We use a broad variety of traditional and digital marketing mediums to engage prospective customers. Our Operations Our operations team is uniquely structured to optimize the experience of our customers and distribution partners. These vertically focused business support teams allow us to establish a level of expertise that delivers a scalable support structure and enables us to align our services with the economic goals and specific expectations of our company the respective business unit. Each operations team is positioned to support the functions of their customer base. Key performance indicators mark their progress toward achieving the goals established by each business unit vertical and sub-vertical. A strong network of shared services, such as marketing, legal, finance and HR, support our decentralized operating vertical and sub-vertical units and ensure they are focused on providing best in-class service to our customers. Our corporate technology department is structured to rapidly enhance, deploy and effectively maintain our products and services. Our operations team is structured to effectively support the individual needs of our customers. This includes: • customer onboarding; • data conversions and migrations; • software configurations and integrations; • customer support and retention; • customer training and activations; • contract renewals, billing and financial review; • credit underwriting and risk management; • payment facilitator processing support; and • end-user customer support. Our technical operations team oversees the execution of development, quality control, delivery and support for our vertical software solutions and proprietary payment processing applications facilitator platform. Products are developed and tested according to the software development lifecycle, composed of iterative backlog refinement, feature prioritization, development and testing with a dedicated focus on planning and execution. Releases are modeled on continuous deployment and added to the live environment on a routine basis. Each application is built with redundancy to foster resiliency and built to be easily managed during a disaster recovery scenario. Our hosted solutions are maintained managed within a managed, dedicated environment environments which upholds multiple within AWS and Azure that align with various compliance standards according specific to the vertical each industry. This includes, including but is not limited to PCI, Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and National Institute of Standards and Technology ("NIST"), to ensuring the protect protection of all personal and transactional data. Our Competition We compete with a variety of vertical market software providers that have different business models, go-to-market strategies and technical capabilities. We believe the most significant competitive factors in our markets are: 1. quality, including the ability of our products and solutions to addresses-- address the specific needs of our customers; 2. service, including our ability to bring value-added solutions and strong customer support; 3. trust, including a strong reputation for quality service and trusted distribution partners; 4. convenience, such as speed in customer onboarding and approving applications; 5. pricing, including fees charged to customers and residuals and incentives offered to distribution partners. Our competitors range from large and well-established companies to smaller, earlier-stage businesses. See "Risk Factors — Risks Related to Our Business and Industry — The vertical market software and payment processing industries are highly competitive. Such competition could adversely affect the revenue we receive, and as a result, our margins, business, financial condition and results of operations." in Part I, Item 1A of this Annual Report on Form 10-K. Human Capital To facilitate talent attraction and retention, we strive to make i3 Verticals a safe and healthy workplace, with opportunities for our employees to grow and develop in their careers, supported by competitive compensation and benefits programs and opportunities for advancement. The success of our business is fundamentally connected to the well-being of our people. Accordingly, we provide our eligible employees with access to flexible and convenient medical programs intended to meet their needs and the needs of their families. In addition to standard medical coverage, for our domestic employees, we offer dental and vision coverage, health savings and flexible spending accounts, paid time off, flexible work schedules on a case-by-case basis, employee assistance programs, voluntary short term and long-term disability insurance and term life insurance. For our non-U.S. employees, in addition to standard medical coverage, we offer benefits that are consistent with local practices for similarly situated companies. We provide competitive compensation and benefits programs to help meet the needs of our employees. In addition to salaries, these programs (which vary across our businesses) include bonus opportunities and, for our domestic employees, a 401(k) Plan. We use targeted stock option grants and restricted stock units ("RSUs") with vesting

conditions to facilitate retention of personnel, and we are proud that a large percentage of our workforce owns i3 Verticals shares, RSUs or options to purchase i3 Verticals shares. We believe this dynamic aligns important economic incentives and encourages an entrepreneurial spirit. We have built a collaborative culture that recognizes and rewards innovation and offers employees a variety of opportunities and experiences. We believe that our culture is critical to our success. As of September 30, 2023-2024, 60 % of our employees work in one of our 38-25 offices and 40 % of our employees are fully remote or hybrid. We encourage our employees to take advantage of our flexible work arrangements to meet their individual circumstances. We are an acquisitive company and have regularly add-added new employees and locations as a result of our acquisition activity. As Our employee headcount has significantly increased since our Initial Public Offering in June 2018, and as of November 21-22, 2023-2024, after giving effect to the disposition of our Merchant Services Business which was completed on September 20, 2024, we have had approximately 1, 663-480 employees in 42-44 states and two countries. No employees are represented by unions. We believe that our employee retention rates are competitive and we think this is a result of strong emphasis on workforce culture in our acquisition process and in our operational decision making. As of September 30, 2023-2024, after giving effect to the completion of the sale of our Merchant Services Business, the Company's workforce was 48-54 % female and 52-46 % male. In addition, our workforce ethnicity, as of September 30, 2023-2024, was as follows: 66-62 % White, 15-22 % Asian, 8 % Black or African American, 6-4 % Hispanic or Latino and 5-4 % Other. Race and gender disclosures are based on information self-reported by employees. Government Regulation We operate in an increasingly complex legal and regulatory environment. Our business and the products and services that we offer are subject to a variety of federal, state and local laws and regulations and the rules and standards of the payment networks that we utilize to provide our electronic payment services, as more fully described below. Dodd- Frank Act The 2010 Dodd- Frank Wall Street Reform and Consumer Protection Act (the "Dodd- Frank Act") and the related rules and regulations have resulted in significant changes to the regulation of the financial services industry. Changes impacting the electronic payment industry include providing merchants with the ability to set minimum dollar amounts for the acceptance of credit cards and to offer discounts or incentives to entice consumers to pay with cash, checks, debit cards or credit cards, as the merchant prefers. The Durbin Amendment to the Dodd- Frank Act provides that the Federal Reserve regulate interchange fees that certain issuers charge merchants for debit transactions and these fees must be "reasonable and proportional" to the cost incurred by the issuer in authorizing, clearing and settling the transactions. Rules released by the Federal Reserve in July 2011 to implement the Durbin Amendment mandate a cap on debit transaction interchange fees for issuers with assets of \$ 10 billion or greater. Federal Reserve approval of a final rule effective October 1, 2021 permit debit card issuers to receive a fraud- prevention adjustment to the interchange fee standards. New rules effective July, 2023 contain certain prohibitions on payment network exclusivity and merchant routing restrictions of debit card transactions. The Dodd- Frank Act also created the Consumer Financial Protection Bureau (the "CFPB"), which has assumed responsibility for most federal consumer protection laws of a financial nature, and the Financial Stability Oversight Council, which has the authority to determine whether any non- bank financial company, such as us, should be supervised by the Board of Governors of the Federal Reserve System because it is systemically important to the U. S. financial system. Any new rules or regulations implemented by the CFPB or the Financial Stability Oversight Council or in connection with the Dodd- Frank Act that are applicable to us, or any changes that are adverse to us resulting from litigation brought by third parties challenging such rules and regulations, could increase our cost of doing business or limit permissible activities. Privacy and Information Security Regulations We provide services that are subject to privacy laws and regulations of a variety of jurisdictions. Relevant federal privacy laws include the Gramm- Leach- Bliley Act of 1999, which applies directly to a broad range of financial institutions and indirectly, or in some instances directly, to companies that provide services to financial institutions. These laws and regulations restrict the collection, processing, storage, use and disclosure of personal information, require notice to individuals of privacy practices and provide individuals with certain rights to prevent the use and disclosure of certain nonpublic or otherwise legally protected information. These laws also impose requirements for safeguarding and proper destruction of personal information through the issuance of data security standards or guidelines. Our business also may be subject to the Fair Credit Reporting Act and the Fair and Accurate Credit Transactions Act of 2003, which regulate the use and reporting of consumer credit information and impose disclosure requirements on entities who take adverse action based on information obtained from credit reporting agencies. All fifty states, Puerto Rico, and the U. S. Virgin Islands have enacted data breach notification laws requiring businesses that experience a security breach of their computer databases that contain personal information to notify affected individuals, consumer reporting agencies and governmental agencies. Eleven-Many states have implemented (though not all laws, including Texas, are presently in effect) comprehensive data privacy and security laws. Certain of these laws restrict the ability to collect and utilize certain types of personal information, such as Social Security and driver's license numbers, impose secure disposal requirements for personal data and contain regulations surrounding data protection and information security. For example, Massachusetts requires any business that processes the personal information of a Massachusetts resident to adopt and implement a written information security program. In addition, states are increasingly legislating data protection requirements for a broader list of personal data and are strengthening protections for students' personal information. For example, Illinois regulates the collection of biometric information under its Biometric Information Privacy Act. Texas and Washington have also passed legislation regulating the collection of biometric information, and additional at least ten other states have legislation pending regarding the collection of biometric data. Additionally, many states have passed comprehensive consumer privacy laws, that are either currently in effect or are set to become effective in the near term including California Consumer Privacy Act of 2018 (the "CCPA"), Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Rhode Island, Oregon, Tennessee, Texas, Utah, and Virginia. These laws requires- require companies that process personal information of California- certain residents of those states to make certain disclosures to consumers about data practices, grants consumers specific access- rights to their data, and allows- allow consumers to opt out of certain data sharing activities, and the California Consumer Privacy Act of 2018 (the "

CCPA”), as amended by the California Privacy Rights Act of 2020 (the “CPRA”), creates a private right of action for data breaches. The California Privacy Rights Act of 2020 (the “CPRA”), which came into effect on January 1, 2023, applies to certain personal information collected on or after January 1, 2022, amends and expands the CCPA to create additional consumer privacy rights, such as the right of correction and right to limit the use of sensitive personal information, and establishes a privacy enforcement agency known as the California Privacy Protection Agency (the “CPPA”). Virginia passed the Consumer Data Protection Act, effective January 1, 2023 which offers consumers some rights similar to those offered by the CCPA. Colorado (the Colorado Privacy Act) and Connecticut (Public Act 22-15) both passed privacy laws that went into effect on July 1, 2023, and Utah updated its code with respect to a number of privacy and data security-related issues that go into effect on December 31, 2023. In addition, various other states are expected to enact in the near future, new laws and regulations concerning privacy, data protection and information security. To the extent we are subject to such legislation, the potential effects on our business are often far-reaching and may require us to modify our data processing practices and policies and to incur substantial costs and expenses in an effort to comply. **Such** The recently enacted laws often provide for civil penalties or fines for violations. Each privacy law and regulation that applies to us could increase our cost of doing business or limit permissible activities. We are also subject to numerous federal and state laws and regulations related to the privacy and security of health information. See “— Healthcare Regulatory Matters” below. As an entity that provides services to educational institutions, we are indirectly subject to the Family Educational Rights and Privacy Act (“FERPA”) or Protection of Pupil Rights Amendment (“PPRA”), and we may not transfer or otherwise disclose or use any personally identifiable information from a student record to another party other than on a basis and in a manner permitted under the statutes. See “Risk Factors — If we violate the FERPA or PPRA, it could result in a material breach of contract with one or more of our customers in our Education **sub-** vertical and could harm our reputation. Further, if we disclose student information in violation of FERPA or PPRA, our access to student information could be suspended.” Our Healthcare vertical business provides services to healthcare providers who are highly regulated and subject to frequently changing political, legislative, regulatory and other influences. Although some regulatory requirements do not directly apply to our operations, these requirements affect the business of our healthcare customers and the demand for our services. Failure to satisfy those legal and regulatory requirements, or the adoption of new laws or regulations, could have a significant negative impact on our Healthcare vertical operations and financial condition. U. S. federal, state, local laws and regulations are evolving and can be subject to significant change. In addition, the application and interpretation of these laws and regulations are often uncertain. These laws are enforced by federal, state and local regulatory agencies in the jurisdictions where we operate, and in some instances also through private civil litigation. Examples of the most significant of these laws include, but are not limited to, the following: HIPAA Privacy and Security Requirements There are numerous federal and state laws and regulations related to the privacy and security of health information. In particular, regulations promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic Clinical Health Act of 2009 (“HITECH”) and other laws (collectively “HIPAA”) establish privacy and security standards that limit the use and disclosure of certain individually identifiable health information (known as “protected health information”) and require covered entities, including health plans and most healthcare providers, to implement administrative, physical and technical safeguards to protect the privacy of PHI and ensure the confidentiality, integrity and availability of electronic PHI. **Currently, a Notice of Proposed Rulemaking to strengthen the HIPAA security rule is under review by the U. S. Office of Management and Budget and is expected to be published before the end of 2024. Although the specific requirements of this proposed rule have not been published, we would expect the proposed rule to modernize requirements for protecting PHI against healthcare cybersecurity threats, which have dramatically increased over the past few years.** In addition, the HIPAA administrative simplification provisions require the use of uniform electronic data transmission standards of healthcare claims and payment transactions submitted or received electronically. Certain provisions of the security and privacy regulations promulgated pursuant to HIPAA apply to business associates (entities that handle PHI on behalf of covered entities), and business associates are subject to direct liability for violation of these provisions. As a provider of services to entities subject to HIPAA, we are a “business associate” of our customers and must safeguard the PHI we handle. To the extent permitted by applicable regulations and contracts and associated business associate agreements with our customers, we are permitted to use and disclose PHI to perform our services and for other limited purposes, but other uses and disclosures, such as marketing communications, require written authorization from the patient or must meet an exception specified under the privacy regulations. Violations of the HIPAA privacy and security regulations may result in substantial civil monetary penalties and, in certain circumstances, criminal penalties. The U. S. Department of Health and Human Services (“HHS”) enforces the privacy and security regulations, and state attorneys general may also enforce the regulations in response to violations that threaten the privacy of state residents. To the extent we are permitted under our customer contracts, we may de-identify PHI and use de-identified information for our purposes without obtaining patient authorization or further complying with HIPAA. Determining whether PHI has been sufficiently de-identified to comply with the HIPAA privacy standards and our contractual obligations may require complex factual and statistical analyses. Any failure by us to meet HIPAA requirements with respect to de-identification could subject us to penalties and harm our reputation. Other Privacy and Security Requirements In addition to HIPAA, numerous other U. S. federal and state laws govern the collection, dissemination, use, access to and confidentiality of personal information, including **certain demographic information, such as social security numbers, financial information,** health and wellness data that is not protected health information. In many cases, state laws are more restrictive than, and not preempted by, HIPAA, and may allow personal rights of action with respect to privacy or security breaches, as well as fines. State laws are contributing to increased enforcement activity and are subject to interpretation by various courts and other governmental authorities. Further, a number of states have introduced or passed legislation relating to the collection, storage, handling and transfer of personal data, as discussed above. Also, the Substance Abuse Confidentiality Regulations, restrict the use and disclosure of certain information that relates to

substance abuse disorders. Data Protection and Breaches Most states require holders of personal information to maintain safeguards, and all states have laws that require such holders to take certain actions in response to a data breach, such as providing prompt notification of the breach to affected individuals or the state's attorney general. In some states, these laws are limited to electronic data, but states increasingly are enacting or considering stricter and broader requirements. The laws are inconsistent across states, which can increase the costs of compliance. Additionally, HIPAA imposes certain notification requirements on business associates. In certain circumstances involving large breaches, media notice is required. A non-permitted use or disclosure of PHI is presumed to be a breach under HIPAA unless the business associate or covered entity establishes that there is a low probability the information has been compromised consistent with the risk assessment requirements enumerated under HIPAA. Further, the FTC regulations require creditors, which may include some of our customers, to implement identity theft prevention programs to detect, prevent and mitigate identity theft in connection with customer accounts. Although Congress passed legislation that restricts the definition of "creditor" and exempts many healthcare providers from complying with this identity theft prevention rule, we may be required to apply additional resources to our existing processes to assist our affected customers in complying with this rule.

Information Blocking and Interoperability Requirements Government initiatives promoting interoperability of electronic health information ("EHI") have driven increasing demand among customers, industry groups, and patients for health information technology ("HIT") products that are compatible with one another and capable of facilitating access, exchange, and use of EHI without delay or other interference. For example, the 21st Century Cures Act ("The Cures Act") and implementing regulations (the "Information Blocking Rule"), prohibit information blocking by health care providers, health information exchanges ("HIEs"), and developers that offer or develop one or more HIT modules certified ~~by~~ **through** the Office of the National Coordinator of Health Information Technology ("ONC") **Certification Program ("Certified Health Information Technology")**. One of our subsidiaries is considered to be a HIT developer since its product, iMed EMR, is ~~ONC-certified~~ **Certified Health Information Technology** and is, therefore, subject to these restrictions. Information blocking by a HIT developer or HIE is any practice that the actor knows or should know is likely to interfere with, prevent or materially discourage access, exchange or use of EHI, unless it is required by law or meets an exception. Under the Cures Act and a final rule published in July 2023 by the HHS Office of the Inspector General ("OIG"), developers of ~~certified~~ **Certified HIT-Health Information Technology** that commit information blocking may be subject to civil penalties of up to \$ 1 million per violation. In 2020, ONC published a final rule that imposes HIT technology standards, implementation specifications, certification criteria, and conditions and maintenance of certification requirements that apply to HIT developers ("HIT Standards and Certification Criteria Final Rule"). The HIT Standards and Certification Criteria Final Rule includes new criteria related to EHI export and standardized APIs for patient services. As a result of this rule, HIT developers of certified HIT must ensure that their products and services meet the requisite technical standards by the relevant deadlines, **most of** which ~~roll-rolled~~ **out through 2024**, and that their HIT continues to evolve as developers and other stakeholders release revised versions of these standards. In addition, to participate in the ONC Health IT Certification Program, HIT developers must make various certifications regarding their HIT, and attest to compliance with applicable conditions of certification, including those related to information blocking. In 2020, the Centers for Medicare & Medicaid Services ("CMS") published the Interoperability and Patient Access Final Rule, which, among other things, requires hospitals with certain EHR capabilities to send admission, discharge, and transfer notifications to other providers, and imposes requirements on certain payors to support Patient Access and Provider Directory APIs. While not directly applicable to HIT developers, the Interoperability and Patient Access Final Rule further demonstrates the government's drive toward interoperability of EHI and the resulting need of healthcare providers and other consumers of HIT for tools that meet these requirements. In January 2022, ONC published the Trusted Exchange Framework, Common Agreement- Version 1 ("TEFCA") and Qualified Health Information Network ("QHIN") Technical Framework- Version 1. In November 2023, ONC published TEFCA Version 1.1. The overall goal of the TEFCA is to establish a universal floor for interoperability across the country. The TEFCA will establish the infrastructure model and governing approach for users in different networks to securely share basic clinical information with each other — all under commonly agreed- to expectations and rules, agnostic to the network in which they participate. The Trusted Exchange Framework describes a common set of non- binding, foundational principles for trust policies and practices that can help facilitate exchange among HINs. Although implementation of the Trusted Exchange Framework is not mandatory, the federal government encourages its adoption through the establishment of a publicly available directory of networks that are capable of trusted exchange and by permitting federal agencies to require implementation of the Trusted Exchange Framework by network contractors as the contractors update their health IT or operational practices. In February 2023, ONC approved the first group of networks to implement the TEFCA as prospective QHINs, and **currently these** ~~there candidate~~ **are seven QHINs that are expected to go-live**. **ONC, now known as the Assistant Secretary for Technology Policy / Office of the National Coordinator for Health IT, or "ASTP ONC," has finalized one update to the HIT Standards and Certification Criteria Final Rule since 2020, and has another one pending. The finalized update, a Final Rule entitled "Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing," or "HTI- 1," became effective February 8, 2024. HTI- 1 further advances health IT interoperability by updating health IT standards, establishing transparency requirements for artificial intelligence and the other end-predictive algorithms that are part of Certified Health Information Technology, and revising and adding Information Blocking Rule exceptions (including one for TEFCA). The other update is a rule proposed by ASTP ONC called "Health Data, Technology, and Interoperability: Patient Engagement, Information Sharing, and Public Health Interoperability," or "HTI- 2." HTI- 2 proposes two sets of new certification criteria (to enable public health as well as health IT for payors), continues to build ~~of~~ **off HTI- 1 in terms of technology and standards updates, proposes additional Information Blocking Rule exceptions, and establishes governance rules for TEFCA. Public comments closed on HTI- 2 October 4, 2023-2024**, and the Final Rule for HTI- 2 has not yet been**

**released**. Anti- Kickback Laws A number of federal and state laws govern patient referrals, financial relationships with physicians and other referral sources and inducements to providers and patients, including restrictions commonly known as the federal Anti- Kickback Statute (“ AKS ”). The AKS prohibits any person or entity from offering, paying, soliciting or receiving, directly or indirectly, anything of value with the intent of generating referrals of items or services covered by Medicare, Medicaid or other federal healthcare programs. Courts have interpreted the law broadly and held that there is violation of the statute if any one of the purposes of an arrangement is to encourage patient referrals or other federal healthcare program business, regardless of whether there are other legitimate purposes for the arrangement. Actual knowledge of the statute or specific intent to violate it is not required to commit a violation. Violation of the AKS is a felony, and penalties for AKS violations can be severe, and include imprisonment, criminal fines, civil penalties with treble damages and exclusion from participation in federal healthcare programs. In addition, submission of a claim or services or items generated in violation of the AKS may be subject to additional penalties under the federal False Claims Act (“ FCA”). The AKS contains a limited number of exceptions, and the OIG has created regulatory safe harbors to the AKS. Activities that comply with a safe harbor are deemed protected from prosecution under the AKS. Failure to meet a safe harbor does not automatically render an arrangement illegal under the AKS. The arrangement, however, does risk increased scrutiny by government enforcement authorities, based on our particular facts and circumstances. Our contracts and other arrangements may not meet an exception or a safe harbor. Additionally, many states have similar anti- kickback laws or laws that otherwise prohibit fraudulent or abusive arrangements within the healthcare industry. These laws are often broad in scope and may apply regardless of the source of payment for care. Although we believe that our relationships with referral sources and recipients have been structured to comply with current law and available interpretations, we cannot provide assurance that regulatory authorities enforcing these laws will determine these financial arrangements comply with the AKS or other applicable laws. False or Fraudulent Claim Laws; Medical Billing and Coding Medical billing, coding and collection activities are governed by numerous federal and state civil and criminal laws, regulations, and sub- regulatory guidance. We provide billing and coding services, claims processing and other solutions to providers that relate to, or directly involve, the reimbursement of health services covered by Medicare, Medicaid, other federal and state healthcare programs and private payers. These services may subject us to, or we may be contractually required to comply with, numerous federal and state laws that prohibit false or fraudulent claims including but not limited to the FCA, the federal Civil Monetary Penalties Law (“ CMP Law”), and state equivalents. We rely on our customers to provide us with accurate and complete information and to appropriately use the solutions we provide to them, but they may not always do so. The FCA prohibits the knowing submission of false claims or statements to the federal government, including to the Medicare and Medicaid programs. The FCA defines the term “ knowingly ” broadly to include not only actual knowledge of a claim’ s falsity, but also reckless disregard of the truth of the information, or deliberate ignorance of the truth or falsity of a claim. Specific intent to defraud is not required. The FCA may be enforced by the federal government directly or by a qui tam plaintiff, or whistleblower, on the government’ s behalf. The government may use the FCA to prosecute Medicare and other government program fraud in areas such as coding errors and billing for services not rendered. Further, submission of a claim for an item or service generated in violation of the AKS constitutes a false or fraudulent claim for purposes of the FCA. When an entity is determined to have violated the FCA, it may be required to pay three times the actual damages sustained by the government, plus substantial civil penalties for each false claim, and may be excluded from participation in federal healthcare programs. Exclusion from Participation in Government Healthcare Programs The OIG is required to or may choose to exclude individuals and entities involved in misconduct related to federal healthcare programs, including Medicare and Medicaid, from participation in those programs. Federal law prohibits federal healthcare programs from paying for items or services furnished, ordered, or prescribed by an individual or entity excluded from participation. The prohibition against federal program payment extends to payment for administrative and management services not directly related to patient care. Civil penalties may be imposed against providers and entities that employ or enter into contracts with excluded individuals or entities to provide items or services to federal healthcare program beneficiaries and submit a claim for reimbursement to a federal healthcare program, or cause such a claim to be submitted. In addition to civil monetary penalties, violations may result in exclusion and treble damages, for each item or service furnished during the period in which the individual or entity was excluded. Our customers have an affirmative duty to check the exclusion status of individuals and entities prior to entering into contractual relationships and periodically re-check thereafter. We have implemented compliance policies and procedures to screen for excluded individuals **at our entities subject to these laws**. However, if we employ or contract with an excluded individual or entity, we could face significant consequences as outlined above. In addition, we could be liable under our customer contracts if we are excluded by the OIG or employ or contract with an excluded individual or entity. Anti- Money Laundering and Counter- Terrorism Regulation Our business is subject to U. S. federal anti- money laundering laws and regulations, including the Bank Secrecy Act of 1970, as amended by the USA PATRIOT Act of 2001, which we refer to collectively as the “ BSA. ” The BSA, among other things, requires money services businesses to develop and implement risk- based anti- money laundering programs, report large cash transactions and suspicious activity and maintain transaction records. We are also subject to certain economic and trade sanctions programs that are administered by the Office of Foreign Assets Control (“ OFAC ”) that prohibit or restrict transactions to or from (or transactions dealing with) specified countries, their governments and, in certain circumstances, their nationals, such as those who might be narcotics traffickers and terrorists or terrorist organizations. Similar anti- money laundering, counter terrorist financing and proceeds of crime laws apply to movements of currency and payments through electronic transactions and to dealings with persons specified on lists maintained by organizations similar to OFAC in several other countries and which may impose specific data retention obligations or prohibitions on intermediaries in the payment process. We have developed and continue to enhance compliance programs and policies to monitor and address related legal and regulatory requirements and developments. Unfair or Deceptive Acts or Practices We and many of our customers are subject to Section 5 of the Federal Trade Commission Act prohibiting unfair or deceptive acts or practices. In addition, laws prohibiting

these activities and other laws, rules and or regulations, including the Telemarketing Sales Act, may directly impact the activities of certain of our customers, and in some cases may subject us, as the customer's payment processor or provider of certain services, to investigations, fees, fines and disgorgement of funds if we are deemed to have aided and abetted or otherwise provided the means and instrumentalities to facilitate the illegal or improper activities of the customer through our services. Various federal and state regulatory enforcement agencies, including the Federal Trade Commission and the states attorneys general, have authority to take action against non-banks that engage in unfair or deceptive acts or practices or violate other laws, rules and regulations and to the extent we are processing payments or providing services for a customer that may be in violation of laws, rules and regulations, we may be subject to enforcement actions and as a result may incur losses and liabilities that may impact our business. In addition, the CFPB has recently attempted to extend certain provisions of the Dodd- Frank Act that prevent the employment of unfair, deceptive or abusive acts or practices ("UDAAP") to payment processors. Though there is still litigation involving whether payment processing companies are subject to these requirements (and the extent of their application), these requirements may apply or be applicable in the future. UDAAPs could involve omissions or misrepresentations of important information to consumers or practices that take advantage of vulnerable consumers, such as elderly or low-income consumers. ~~Prepaid Products~~ ~~General-use prepaid~~ ~~Prepaid cards~~ ~~products, such as~~ store gift cards and gift certificates issued as a card, code or other device, often referred to as stored value, are subject to various federal and state laws and regulations, which may include laws and regulations related to consumer and data protection, licensing, consumer disclosures, escheat, anti-money laundering, banking, trade practices and competition ~~and wage and employment~~. The customers who utilize ~~prepaid the gift card processing~~ products and services that we may sell may be subject to these laws and regulations. In the future, if we seek to expand these ~~prepaid stored value~~ card products and services, or as a result of regulatory changes, we may be subject to additional regulation and may be required to obtain additional licenses and registrations which we may not be able to obtain. The Credit Card Accountability Responsibility and Disclosure Act of 2009 (the "Card Act") gift card provisions created requirements applicable to general-use prepaid cards, store gift cards and gift certificates. The Card Act, along with the Federal Reserve's amended Regulation E, created new requirements with respect to general-use prepaid cards, store gift cards and gift certificates. These include restrictions to impose dormancy, inactivity or service fees, expiration date not less than five years from the date of issuance and revised pre-purchase disclosure obligations. Products offered on a prepaid basis may also be subject to the rules and regulations of Visa, Mastercard, Discover and American Express and other payment networks with which our customers and the card issuers do business. The customers who utilize the gift card processing products and services that we may sell are responsible for compliance with all applicable rules and requirements relating to their gift product program. Additionally, the Financial Crimes Enforcement Network of the U. S. Department of the Treasury ("FinCEN"), issued a final rule in July 2011 regarding the applicability of the BSA's regulations to "prepaid access" products and services. This rulemaking clarifies the anti-money laundering obligations for entities engaged in the provision and sale of prepaid access including prepaid gift cards. We are not registered with FinCEN based on our determination that our current products and services do not constitute a "prepaid program" as defined in the BSA and we are not a "provider" of prepaid access. We may in the future need to register with FinCEN as a "money services business-provider of prepaid access" in accordance with the rule based on changes to our products or services. Indirect Regulatory Requirements Certain of our ~~distribution~~ partners are financial institutions that are directly subject to various regulations and compliance obligations issued by the CFPB, the Federal Reserve System, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the National Credit Union Administration and other agencies responsible for regulating financial institutions, which includes state financial institution regulators. While these regulatory requirements and compliance obligations do not apply directly to us, many of these requirements materially affect the services we provide to our customers and us overall. The financial institution regulators have imposed requirements on regulated financial institutions to manage their third-party service providers. Among other things, these requirements include performing appropriate due diligence when selecting third-party service providers; evaluating the risk management, information security, and information management systems of third-party service providers; imposing contractual protections in agreements with third-party service providers (such as performance measures, audit and remediation rights, indemnification, compliance requirements, confidentiality and information security obligations, insurance requirements, and limits on liability); and conducting ongoing monitoring, diligence and audits of the performance of third-party service providers. Additionally, certain of our customers are governmental entities, which may be subject to further federal, state or local requirements. Accommodating these requirements applicable to our customers imposes additional costs and risks in connection with both our operations and our financial institution relationships. We expect to expend significant resources on an ongoing basis in an effort to assist our customers in meeting their legal requirements. Payment Network Rules and Standards Payment networks establish their own rules and standards that allocate liabilities and responsibilities among the payment networks and their participants. These rules and standards, including the PCI DSS, govern a variety of areas of the payments industry, including how we can process transactions, how consumers and customers may use their cards, how our customers may conduct their business regarding the acceptance of payments (including the types and amounts of fees that can be assessed for the acceptance of payments), the security features of cards, security standards for processing, data security and allocation of liability for certain acts or omissions including liability in the event of a data breach. The payment networks may change these rules and standards from time to time as they may determine in their sole discretion and with or without advance notice to their participants. These changes may be made for any number of reasons, including as a result of changes in the regulatory environment, to maintain or attract new participants, or to serve the strategic initiatives of the networks and may impose additional costs and expenses on or be disadvantageous to certain participants. Changes to these rules and standards could alter or prohibit certain current industry business practices which could impact our ability to provide services to various market segments we service. Participants are subject to audit by the payment networks to ensure compliance with applicable rules and standards. The networks may fine, penalize or suspend the registration of participants for certain acts

or omissions or the failure of the participants to comply with applicable rules and standards. A significant network rule is the “chip and pin” or “chip and signature” card requirement, known as EMV, which was mandated by Visa, Mastercard, American Express and Discover to be supported by payment processors by April 2013 and merchants by October 2015. This mandate set new requirements and technical standards, including requiring integrated point of sale systems to be capable of accepting the more secure “chip” enabled cards that utilize the EMV standard and setting new rules for data handling and security. Processors and customers that do not comply with the mandate or do not use systems that are EMV compliant risk fines and liability for fraud-related charges. We have invested significant resources to ensure our systems’ compliance with the mandate, and to assist our customers in fulfilling their EMV compliance responsibilities. To provide our electronic payment services, we must be registered ~~either indirectly or directly as a service provider~~ with each of the payment networks that we utilize. Because we are not a bank, we are not eligible for primary membership in certain payment networks, including Visa and Mastercard, and are therefore unable to directly access these networks. The operating regulations of certain payment networks, including Visa and Mastercard, require us to be sponsored by a member bank ~~as a service provider~~. We are registered with certain payment networks, including Visa and Mastercard, through ~~various a sponsor banks- bank~~ **sponsor give gives**. The agreements with our bank ~~sponsors-~~ **sponsor give gives** them substantial discretion in approving certain aspects of our business practices including our solicitation, application and qualification procedures for customers and the terms of our agreements with customers. We are also subject to network operating rules and guidelines promulgated by the National Automated Clearing House Association (“NACHA”) relating to payment transactions we process using the ACH Network. Like the card networks, NACHA may update its operating rules and guidelines at any time and we will be subject to these changes. For example, NACHA’s Micro-Entry Rule to improve the means of account validation was implemented in two stages effective September 16, 2022 and March 17, 2023, and requires originators of ACH transaction to use commercially reasonable fraud detection and to monitor forward and return micro-entry volumes. The NACHA Operating Rules and Guidelines allocate responsibility and liabilities to the various participants in the payment network, including us and our partner financial institutions. NACHA continues to focus on data security and privacy and delegation of responsibilities. We are subject to audit by our partner financial institutions for compliance with the rules and guidelines. Our sponsor financial institutions have substantial discretion in approving certain aspects of our business practices, including the terms of our agreements with our ACH processing customers. Money Transmitter Regulation We are subject to various U. S. federal, state, and foreign laws and regulations governing money transmission and the issuance and sale of payment instruments, including various prepaid access products we may sell. In the United States, each state besides Montana has money transmitter license requirements and many have licenses for issuers of payment instruments and stored value. These states not only regulate and control money transmitters, but they also license entities engaged in the transmission of funds. Many states exercise authority over the operations of our services related to money transmission and payment instruments and, as part of this authority, subject us to periodic examinations. Many states require, among other things, that proceeds from money transmission activity and payment instrument sales be invested in high-quality marketable securities before the settlement of the transactions or otherwise restrict the use and safekeeping of such funds. Such licensing laws may cover matters including regulatory approval of consumer forms, required consumer disclosures, the filing of periodic and updated reports by the licensee and require the licensee to demonstrate and maintain specified levels of net worth. Many states also require money transmitters, issuers of payment instruments and stored value, and their agents to comply with federal and / or state anti-money laundering laws and regulations. Other Regulation We are subject to U. S. federal and state unclaimed or abandoned property (escheat) laws which require us to remit to certain government authorities property of others we hold that has been unclaimed for a specified period of time such as account balances due to a ~~distribution partner or~~ customer following discontinuation of its relationship with us. The Housing Assistance Tax Act of 2008 requires certain merchant acquiring entities and third-party settlement organizations to provide information returns for each calendar year with respect to payments made in settlement of electronic payment transactions and third-party payment network transactions occurring in that calendar year. Reportable transactions are also subject to backup withholding requirements. The foregoing is not an exhaustive list of the laws and regulations to which we are subject and the regulatory framework governing our business is changing continuously. See “Risk Factors — Risks Related to Our Business and Industry” in Part I, Item 1A of this Annual Report on Form 10-K. Our Intellectual Property Certain of our products and services are based on proprietary software and related payment systems solutions. We rely on a combination of copyright, trademark, and trade secret laws, as well as employee and third-party non-disclosure, confidentiality, and contractual arrangements to establish, maintain, and enforce our intellectual property rights in our technology, including with respect to our proprietary rights related to our products and services. In addition, we license technology from third parties that is integrated into some of our solutions. We own a number of registered federal service marks, including, without limitation, i3 Verticals®, **i3 Education®**, **ImageSoft®**, **JusticeTech®**, **TrueSign®**, **Milestone®** and **PaySchools®** and **Axia®**. We also own a number of domain names, including, without limitation, www.i3verticals.com. Available Information Our Annual Report on Form 10-K, Quarterly Reports on Form 10-Q, Current Reports on Form 8-K, and amendments to reports filed pursuant to Sections 13(a) and 15(d) of the Securities Exchange Act of 1934, as amended (the “Exchange Act”), are filed with the Securities and Exchange Commission (the “SEC”). We are subject to the informational requirements of the Exchange Act and file or furnish reports, proxy statements and other information with the SEC. The SEC maintains an Internet site that contains reports, proxy and information statements and other information regarding issuers that file electronically with the SEC at www.sec.gov. We also maintain a website at www.i3verticals.com, through which you may access these materials free of charge as soon as reasonably practicable after they are electronically filed with, or furnished to, the SEC. Information contained on our website is not a part of this Annual Report on Form 10-K and the inclusion of our website address in this report is an inactive textual reference only. Item 1A. Risk Factors Our business faces significant risks and uncertainties. If any of the following risks are realized, our business, financial condition and results of operations could be materially and adversely affected. The following risk factors, some of which contain statements that constitute forward-looking statements, should be read in conjunction with “

Management's Discussion and Analysis of Financial Condition and Results of Operations" and our consolidated financial statements and related notes. ~~Unauthorized disclosure, destruction or modification of data or disruption of our services or other cybersecurity or technological risks, including as result of a cybersecurity incident, could expose us to liability, protracted and costly litigation and damage our reputation.~~ We are responsible both for our own business and to a significant degree for acts and omissions by certain of our ~~distribution partners and third-party vendors~~ under the rules and regulations established by the payment networks, such as Visa and Mastercard, Discover and American Express, and the debit networks. We and other third parties collect, process, store and transmit sensitive data, such as names, addresses, social security numbers, credit or debit card numbers and expiration dates, drivers' license numbers and bank account numbers, and we have ultimate liability to the payment networks and member financial institutions that register us with the payment networks for our failure, or the failure of certain ~~distribution partners and~~ third parties with whom we contract, to protect this data in accordance with payment network requirements. The loss, destruction or unauthorized modification of customer or cardholder data could result in significant fines, sanctions and proceedings or actions against us by the payment networks, governmental bodies, consumers or others, which could have a material adverse effect on our business, financial condition and results of operations. Any such sanction, fine, proceeding or action could damage our reputation, force us to incur significant expenses in defense of these proceedings, disrupt our operations, distract our management, increase our costs of doing business and may result in the imposition of monetary liability. We are subject to risk associated with information technology and cybersecurity matters. For example, on June 2, 2021, the State of Louisiana, Division of Administration (~~the "State"~~) and a putative class of Louisiana law enforcement districts filed a petition in the 19th Judicial District Court for the Parish of East Baton Rouge against i3- Software & Services, LLC ("S & S"), a subsidiary of the Company located in Shreveport, Louisiana, seeking monetary damages related to a third-party remote access software product used in connection with services provided by S & S to certain Louisiana Parish law enforcement districts and alleged inadequacies in the Company's cybersecurity practices. For additional information about this litigation, see Note ~~15-16~~ to our consolidated financial statements. The current cyber threat environment presents increased risk for all companies, in our industry and otherwise, including as a result of cyberattacks **as well as, and in some cases, ransomware attacks** (through which an attacker **renders an** gains access to the organization's computer files **, renders inaccessible and demands a payment to return** them temporarily inaccessible and **or reinstate access**), **malicious software, advanced persistent threats** --- **threats, phishing and other attempts** to permanently delete them if a cash ransom is not paid by a **specified deadline** **malicious threat actors, including nation-state actors, ransomware groups and others to access, acquire, use disclose, shut down or manipulate information, systems, databases, processes and people**. Like other companies in our industry, our systems are subject to recurring attempts by third parties to access information, manipulate data or disrupt our operations. Although we proactively employ multiple measures to defend our systems against intrusions and attacks and to protect the data we collect, our measures may not prevent unauthorized access or use of sensitive data. In addition, the cybersecurity-related threats that we face may remain undetected for an extended period of time. **In addition, the rapid evolution and increased adoption of artificial intelligence ("AI") and other emerging technologies also may heighten our cybersecurity risks by making cyberattacks and social engineering more difficult to detect, contain and mitigate.** While we have experienced cyber threats and incidents, we have not (~~whether directly and, to our~~ **or knowledge indirectly**, ~~including through our distribution partners, third-party vendors or, customers have not~~ **or other business relations**) been subject to a **cybersecurity event of which we are aware that has had a material ransomware or cyber-extortion attack impacting** --- **impact on us, including our business strategy, financial condition or results of operations. However, despite our security measures, there is no assurance that we, or the third parties with which we interact, will not experience a cybersecurity incident in the future that materially impacts** us. If such an event were to occur it could **significantly materially** disrupt our operations, expose us to liability under ~~HIPAA and / or state~~ data breach laws, adversely impact our reputation, impact our customer relationships or subject us to other material losses or liability. In addition, a breach of our system or a third-party system upon which we rely may subject us to material losses or liability, including payment network fines, assessments and claims for unauthorized purchases with misappropriated credit, debit or card information, impersonation or other similar fraud claims. A misuse of such data or a cybersecurity breach could harm our reputation and deter our customers and potential customers from using electronic payments generally and our products and services specifically, thus reducing our revenue. In addition, any such misuse or breach could cause us to incur costs to correct the breaches or failures, increase our risk of regulatory scrutiny, subject us to lawsuits and result in the imposition of material penalties and fines under state and federal laws (including HIPAA) or by the payment networks. These risks may be heightened in connection with employees working from remote work environments, as our dependency on certain service providers, such as video conferencing and web conferencing services, has significantly increased. In addition, to access our network, products and services, customers and other third parties may use personal mobile devices or computing devices that are outside of our network environment and subject to their own security ~~risk risks~~. While we maintain insurance coverage that may, subject to policy terms and conditions, cover certain aspects of cyber risks, such insurance coverage may be insufficient to cover all losses. A significant cybersecurity breach could also result in payment networks prohibiting us from processing transactions on their networks or the loss of our financial institution sponsorship that facilitates our participation in the payment networks, either of which could materially impede our ability to conduct business. In addition, as cybersecurity threats continue to evolve, we have expended, and expect to continue to expend, significant resources to continue to modify or enhance our protective measures or to investigate and remediate any information security vulnerabilities, but we still might be unable to successfully prevent certain cyberattacks. Although we generally require that our agreements with ~~third our distribution partners~~ **parties and service providers** who have access to customer data include confidentiality obligations that restrict these parties from using or disclosing any customer data except as necessary to perform their services under the applicable agreements, there can be no assurance that these contractual measures will prevent the unauthorized disclosure of business or customer data, nor can we be sure that such third parties would be

willing or able to satisfy liabilities arising from their breach of these agreements. Any failure by such third parties to adequately take these protective measures could result in protracted or costly litigation. In addition, our ~~agreements~~ **agreement** with our bank ~~sponsors~~ **sponsor and applicable** (as well as payment network requirements) require us to take certain protective measures to ensure the confidentiality of business and consumer data. Any failure to adequately comply with these protective measures could result in fees, penalties, litigation or termination of our bank sponsor ~~agreements~~ **agreement**. Any significant unauthorized disclosure of sensitive data entrusted to us would cause significant damage to our reputation, impair our ability to attract new integrated technology ~~and distribution partners~~ and may cause parties with whom we already have such agreements to terminate them. Our services are based on software and computing systems that often encounter development delays, and the underlying software may contain undetected errors, viruses or defects. Defects in our software services or errors or delays could result in additional development costs, diversion of technical and other resources from our other development efforts, loss of credibility with current or potential customers, harm to our reputation and exposure to liability claims. Our systems and operations or those of our third- party technology vendors could be exposed to damage or interruption from, among other things, fire, natural disaster, power loss, telecommunications failure, unauthorized entry, computer viruses, denial- of- service attacks, acts of terrorism, human error, vandalism or sabotage, financial insolvency and similar events. Our property and business interruption insurance may not be adequate to compensate us for all losses or failures that may occur. Likewise, while we have disaster recovery policies and arrangements in place, they have not been tested under actual disasters or similar events. Although we seek to minimize these risks through security measures, controls, back- up data centers and emergency planning, there can be no assurance that such efforts will be successful or effective. Defects in our systems or those of third parties, errors or delays in the processing of payment transactions, telecommunications failures or other difficulties could result in: • loss of revenues; • loss of customers; • loss of customer and cardholder data; • fines imposed by payment networks or regulators; • harm to our business or reputation resulting from negative publicity; • exposure to fraud losses or other liabilities; • additional operating and development costs; or • diversion of management, technical and other resources, among other consequences. We rely on third parties for specific services, software and hardware used in providing our products and services. **Some of these third parties, including hosting providers such as AWS, are necessary for our internal business needs and for the delivery of various cloud and other hosted solutions to customers. These hosting providers rely on the uninterrupted operation of data centers and the ability to protect computer equipment and information stored in these organizations' data centers against unanticipated failures, intrusions, viruses, acts of terrorism and service-similar damaging events. If one or more of our hosting providers are our competitors were unable to support or our requirements provide similar services and technology to our competitors, and we may not have long-term contracts with them. If these contracts are canceled or for an extended period, and we are not unable-- able to renew them on commercially reasonable terms find an alternative solution in a timely fashion, or our customer relationships could be at all-risk of termination, and** our business, financial condition and results of operation could be adversely impacted. The termination by our service or technology providers of their arrangements with us or their failure to perform their services efficiently and effectively may adversely affect our relationships with our customers and, if we cannot find alternate providers quickly, may cause those customers to terminate their processing ~~agreements with us~~. We also rely in part on third parties for the development and access to new technologies, or for updates to existing products and services for which they provide ongoing support. Failure by these third- party providers to devote an appropriate level of attention to our products and services could result in delays in introducing new products or services, or delays in resolving any issues with existing products or services for which third- party providers provide ongoing support. In addition, ~~in the remote work environments~~, the daily activities and productivity of our workforce is ~~now more closely~~ tied to key vendors, such as video conferencing services **and internet providers**, consistently delivering their services without material disruption. ~~Our ability to deliver information using the internet and to operate in a remote working environment may be impaired because of infrastructure failures, service outages at third- party internet providers, malicious attacks or other factors.~~ Some of our solutions contain "open- source" software, and any failure to comply with the terms of one or more of applicable open- source licenses could negatively affect our business. We use certain software licensed under open- source licenses and may continue to use such software in the future. Some open- source licenses require us to make available source code for modifications or derivative works that we create based upon the open -source software, and that we license such modifications or derivative works pursuant to a particular open source license or other license allowing further use by third parties. Some open- source licenses could require us to release the source code of our proprietary software if we combine our proprietary software with the open- source software subject to that license. Additionally, the terms of many open- source licenses have not been interpreted by United States or other courts, and there is a risk that these licenses could be construed in a manner that imposes unanticipated conditions or restrictions on our ability to commercialize our solutions. Using open- source software can also be riskier than using software subject to a more restrictive license because open- source licenses generally do not contain such protections as warranties. Many of the risks associated with using open- source software cannot be eliminated and using such software could adversely affect us. Since inception in 2012, we have been engaged in growth activities and have made a significant number of acquisitions that have grown our business. This acquisition activity requires substantial capital and other expenditures. **While we had substantial net income attributable to i3 Verticals, Inc. in the year ended September 30, 2024 as a result of the gain associated with the divestiture of our Merchant Services Business, Taking taking these factors into account the factors above,** we incurred net losses attributable to i3 Verticals, Inc. in the years ended September 30, 2023 ~~and~~ **2024**, and 2021 ~~and~~ **2022** ~~and~~ **2021-prior years**, and we may continue to incur losses in the future. A substantial portion of our historical revenue growth has resulted from acquisitions. For the year ended September 30, 2023 ~~2024~~, **the incremental impact of** revenues attributable to the acquisitions we completed in 2022 ~~and~~ 2023 **and 2024** were \$ 21.2, 5.4 million, or 5.1, 8.0 % of our total revenues, **net of intercompany eliminations**. We expect our cash needs to increase ~~significantly~~ for the next several years as we: • make additional acquisitions; • market our products and services; • expand our customer support and service operations; •

hire additional marketing, customer support and administrative personnel; and • implement new and upgraded operational and financial systems, procedures and controls. As a result of these continuing costs and expenses, we need to generate significant revenues to attain and maintain profitability and positive cash flow. To date, our operations have been supported by equity and debt financings. If we do not continue to increase our revenues, our business, results of operations and financial condition could be materially and adversely affected. The **vertical market software industry for payment processing services** is highly competitive. **Such competition could adversely affect the revenue we receive, and has as relatively low barriers to entry a result, our margins, business, financial condition and results of operations.** Other **software** providers of payment processing services have established a sizable market share in **our vertical markets** the merchant acquiring sector and service more customers than we do. Our growth will **largely** depend, in part, on a combination of the continued growth of the **electronic payment market** and our ability to increase our market share. Our **payment and competitors in the vertical market industry solutions** compete against many peers. Our competitors include, among others, Tyler Technologies, Inc., EverCommerce, Inc., EngageSmart, LLC, Constellation Software, Inc. **Verra Mobility Corp, EverCommerce Inc.**, Roper Technologies, Inc., Global Payments, Inc., Axon Technologies, **Paymentus and PowerSchool Holdings, Inc., Flywire Corp, Weave Communications Inc., Phresia Inc. and Waystar Holding Corp.** Many of our competitors have substantially greater financial, technological, and marketing resources than we have. Accordingly, if these competitors specifically target our business model, they may be able to offer more attractive solutions to our customers **and more attractive compensation to our distribution partners.** They also may be able to offer and provide products and services that we do not offer. Additionally, larger financial institutions may decide to perform in-house some or all of the services we provide or could provide, which may give them **with** a competitive advantage in the market. There are also a large number of small providers of vertical market software services or payment processing services that provide various ranges of services to our customers and our potential customers. This competition may effectively limit the prices we can charge and requires us to control costs aggressively in order to maintain acceptable profit margins. Competition could also result in a loss of **existing distribution partners and** customers and greater difficulty attracting new **distribution partners and** customers. One or more of these factors could have a material adverse effect on our business, financial condition and results of operations. In addition, we are also subject to risks as a result of changes in business habits of our vendors and customers as they adjust to the competitive marketplace. Because our standing arrangements and agreements with our vendors and customers typically contain no purchase or sale obligations and are terminable by either party upon no or relatively short notice, we are subject to significant risks associated with the loss or change at any time in the business habits and financial condition of key vendors as they adapt to changes in the market. **The vertical** **To acquire and retain customers,** we depend in part on distribution partners that generally do not serve us exclusively, may not aggressively market **software** our products and services, are subject to attrition and are not under our control. We rely heavily on the efforts of our distribution partners to market our products and services to existing customers and potential customers. Generally, our agreements with distribution partners are not exclusive and these partners retain the right to refer potential customers to other merchant acquirers. Gaining and maintaining loyalty or exclusivity may require financial concessions to maintain current distribution partners or to attract potential distribution partners from our competitors who may be offering significantly more enticing pricing terms, such as increased signing bonuses or residuals payable to our referral partners, which could have a negative impact on our results of operations. If these distribution partners switch to another merchant acquirer, focus more heavily on promoting the products and services of one or more other merchant acquirers, cease operations or become insolvent, we may no longer receive new referrals from them or may receive fewer new referrals from them, and we also risk losing existing customers with whom the distribution partner has a relationship. Additionally, some of our distribution partners are subject to the requirements imposed by our bank sponsors, which may result in fines to them for non-compliance and may, in some cases, result in these entities ceasing to market our products and services. If we are unable to maintain our existing base of distribution partners or develop relationships with new distribution partners, our business, financial condition and results of operations would be materially adversely affected. Further, we may be named in legal proceedings in connection with the actions of our distribution partners where it is alleged that our distribution partners have intentionally or negligently misrepresented pricing or other contractual terms to customers or potential customers related to our processing solutions or related products. Our distribution partners are independent businesses and we have no control over their day-to-day business activities, including their customer marketing and solicitation practices. While in some cases we may have indemnification rights against our distribution partners for these activities, there is no guarantee that we will be able to successfully enforce those indemnification rights or that our distribution partners are adequately capitalized in a manner necessary to satisfy their indemnification obligations to us. If one or more judgments or settlements in any litigation or other investigation, plus related defense and investigation costs, significantly exceed our insurance coverage and we are unable to enforce our indemnification rights against a distribution partner or partners, our business, financial condition and results of operations could materially suffer. The electronic payments market is subject to constant and significant changes. This market is characterized by rapid technological evolution, new product and service introductions, evolving industry standards, changing customer needs and the entrance of non-traditional competitors, **including products and services that enable card networks and banks to transact with consumers directly.** To remain competitive, we continually pursue initiatives to develop new products and services to compete **in an effective manner** with these new market entrants. These projects carry risks, such as cost overruns, delays in delivery, performance problems and lack of customer acceptance. In addition, new products and offerings may not perform as intended or generate the business or revenue growth expected. Additionally, we look for acquisition opportunities, investments and alliance relationships with other businesses that will increase our market penetration and enhance our technological capabilities, product offerings and distribution capabilities. Any delay in the delivery of new products and services or the failure to differentiate our products and services or to accurately predict and address market demand could render our products and services less desirable, or even obsolete, **to our customers and to our distribution partners.** Furthermore, **Further,** even though the **development of**

AI market for integrated payment processing products and services is **complex and uncertain, and presents various risks and uncertainties, including as the result of the rapidly evolving legal, it may develop regulatory and ethical landscape associated with the use of AI. Our inability to successfully rapidly or not rapidly enough for or effectively implement AI initiatives, or other deficiencies or failures in our AI systems or initiatives, could subject us to competitive harm, legal** recover the costs we have incurred in developing new products and services targeted at this market **regulatory risk, and increase our cybersecurity, intellectual property, and privacy risks**. Any of the foregoing could have a material and adverse effect on our operating results and financial condition. The continued growth and development of our **payment processing activities software and related services** will depend on our ability to anticipate and adapt to changes in consumer behavior. For example, consumer behavior may change regarding the use of payment card transactions, including the relative increased use of cash, crypto-currencies, other emerging or **our alternative payment methods and payment card systems that we or our processing partners do not adequately support or that do not provide adequate commissions to parties like us. Any failure to timely integrate emerging payment methods into our software, to anticipate consumer behavior changes or to contract with processing partners that support such emerging payment technologies** could cause us to lose traction among our customers or referral sources, resulting in a corresponding loss of revenue, if those methods become popular among end-users of their services. **Our payment** The products and services we deliver are designed to process complex transactions and provide reports and other information on those transactions, all at very high volumes and processing speeds. Our technology offerings **in connection with our software** must also integrate with a variety of network, hardware, mobile and software platforms and technologies, and we need to continuously modify and enhance our products and services to adapt to changes and innovation in these technologies. Any failure to deliver an effective, reliable and secure service or any performance issue that arises with a new product or service could result in significant processing or reporting errors or other losses. **If we do not deliver a promised new product or service to our customers or distribution partners in a timely manner or the product or service does not perform as anticipated, our development efforts could result in increased costs and a loss in business that could reduce our earnings and cause a loss of revenue. We also rely in part on third parties, including some of our competitors and potential competitors, for the development of and access to new technologies, including software and hardware.** Our future success will depend in part on our ability to develop or adapt to technological changes and evolving industry standards. If we are unable to develop, adapt to or access technological changes or evolving industry standards on a timely and cost-effective basis, our business, financial condition and results of operations would be materially adversely affected. We do not directly access the payment card networks, such as Visa and Mastercard, that enable our acceptance of credit cards and debit cards, including some types of prepaid cards. Accordingly, we must rely on **our banks bank sponsor or other payment processors processing providers** to process transactions and must pay fees for the services. To provide our **merchant acquiring payment facilitator** services, we are registered through our bank **sponsors sponsor** with the Visa and Mastercard networks **as service providers for member institutions**. The majority of our **\$ 24.4 billion in payment volume in fiscal year 2023-2024** was attributable to transactions processed on the Visa and Mastercard networks. **We** As such, we, our bank **sponsors sponsor** and many of our customers are subject to complex and evolving payment network rules. The payment networks routinely update and modify requirements applicable to **merchant acquirers payment facilitators**, including rules regulating data integrity, third-party relationships (such as those with respect to **our bank sponsors sponsor and ISOs**), merchant chargeback standards and **Payment Card Industry Data Security Standard ("PCI DSS")**. The rules of the card networks are set by their boards, which may be influenced by card issuers, some of which offer competing transaction processing services. The PCI **Security Standards Council Council** released **fulsome revisions in** version 4.0, which **has been further updated by version 4.0.1, and** includes stronger standards that increase the compliance burden on processors and require additional training, education and support tools for processors to support their merchants. If we or our bank **sponsors sponsor fail fails** to comply with the applicable rules and requirements of the Visa or Mastercard payment networks, Visa or Mastercard could suspend or terminate our member registration or certification, which would make it impossible for us to conduct our business on its current scale. Further, our transaction processing capabilities, including with respect to settlement processes, could be delayed or otherwise disrupted, and recurring non-compliance could result in the payment networks seeking to fine us. In addition, card networks and their member financial institutions regularly update, and generally expand, security expectations and requirements related to the security of cardholder data and environment. Under certain circumstances, we are required to report incidents to the card networks within a specified time frame. We may also be subject to penalties from the payment card networks if we fail to detect that our customers are engaging in activities that are illegal, contrary to the payment card network operating rules, or considered "high-risk." We must either prevent high-risk merchants from using our products and services or register such merchants with the payment card networks and conduct additional monitoring with respect to such merchants. Such penalties could be material and could result in termination of registration or could require changes in our process for registering new customers. This could materially and adversely affect our business. Under certain circumstances specified in the payment network rules, we may be required to submit to periodic audits, self-assessments or other assessments of our compliance with the PCI DSS. Such activities may reveal that we have failed to comply with the PCI DSS. In addition, even if we comply with the PCI DSS, there is no assurance that we will be protected from a security breach. The termination of our registration with the payment networks, or any changes in payment network or issuer rules that limit our ability to provide **merchant acquiring payment facilitation** services, could have an adverse effect on our payment processing volumes, revenues and operating costs. If we are unable to comply with the requirements applicable to our settlement activities, the payment networks may no longer allow us to provide these services, which would require us to spend additional resources to obtain settlement services from a third-party provider. In addition, if we were precluded from processing Visa and Mastercard electronic payments, we would lose substantially all of our **payments-related** revenues. We are also subject to the operating rules of **NACHA-Nacha**, a self-regulatory organization which administers and facilitates private-sector operating rules for ACH payments and defines the roles and responsibilities of

financial institutions and other ACH network participants. The NACHA **Nacha Operating Rules and Operating Guidelines** impose obligations on us and our partner financial institutions. These obligations include audit and oversight by the financial institutions and the imposition of mandatory corrective action, including termination, for serious violations. If an audit or self-assessment under PCI DSS or NACHA **Nacha** identifies any deficiencies that we need to remediate, the remediation efforts may distract our management team and be expensive and time consuming. If ~~the our banks-~~ **bank sponsorship is terminated and we are not able to secure or successfully migrate customer portfolios to a new bank sponsor, we will not be able to conduct our business.** If the bank ~~that sponsor sponsors~~ us with the Visa and Mastercard networks stop sponsoring us, we would need to find other financial institutions to provide those services, which could be difficult and expensive. If we were unable to find a replacement financial institution to provide sponsorship, we could no longer provide processing services to affected customers, which would negatively impact our revenues and earnings. Furthermore, ~~some agreements with our bank sponsors-~~ **sponsor retains** give them substantial discretion in approving certain aspects of our business practices, including our solicitation, application and qualification procedures for customers and the terms of our agreements with customers. Our bank ~~sponsors-~~ **sponsor**'s discretionary actions **could have a material adverse effect on our business, financial condition, and results of operations.** If our processing services agreement with Payroc is terminated and we are not able to enter into replacement processing relationship with another party, our ability to provide payment processing services to our affected software customers may be adversely impacted. In connection with the sale of our Merchant Services Business, we entered into a processing services agreement with Payroc (the "Payroc Processing Agreement"). ~~Under the Payroc Processing Agreement, Payroc agreed to, among other things, process payments for a portion of our software customers in accordance with Payroc's relationships with certain payment processors and sponsor banks. This processing structure for these specific software customers is intended to be temporary, and we expect such customers will eventually transition into our payment facilitation platform. If, however, the Payroc Processing agreements-~~ **Agreement is terminated and we are unable to enter into a replacement processing relationship with another party on acceptable terms or in a timely fashion, or if Payroc's relationship with its processors or sponsor banks is terminated or significantly modified in fashion that is adverse to us or our customers, our ability to provide payment processing services to our affected software customers may be adversely impacted, which** could have a material adverse effect on our business, financial condition, and results of operations. Consolidations have been, and continue to be, active in the banking and financial services industry. It is possible that larger financial institutions that result from consolidations will have increased bargaining power when negotiating, which could result in less favorable contractual terms for us. Larger financial institutions resulting from consolidations may also decide to perform in-house some or all of the services we provide or could provide. These foregoing matters could have an adverse effect on our business, result of operations and financial condition. We have potential liability for chargebacks associated with our customers' processing transactions. In most circumstances, if a billing dispute between a customer and a cardholder is not ultimately resolved in favor of our customer, the disputed transaction is "charged back" to the customer's bank and credited to the account of the cardholder. Anytime our customer is unable to satisfy a chargeback, we are responsible for that chargeback. If we are unable to collect the chargeback from the customer's account or reserve account (if applicable), or if the customer refuses or is financially unable due to bankruptcy or other reasons to reimburse us for the chargeback, we bear the loss for the amount of the refund paid to the cardholder's bank. While we did not incur material chargeback losses in our **2024 or 2023 or 2022** fiscal years, any increase in chargebacks not paid by our customers could have a material adverse effect on our business, financial condition and results of operations. We are potentially liable for losses caused by fraudulent card transactions. Card fraud occurs when a customer's customer uses a stolen or counterfeit credit, debit or prepaid card, card number or other credentials to purchase merchandise or services. In a traditional card-present transaction, if the customer swipes the card, receives authorization for the transaction from the card issuing bank and verifies the signature on the back of the card against the paper receipt signed by the customer, the card issuing bank remains liable for any loss. In a fraudulent card-not-present transaction, even if the customer receives authorization for the transaction, the customer is liable for any loss arising from the transaction. Many of our ~~smaller-~~ **sales transactions** over the Internet or in response to telephone ~~or mail~~ orders. Because their sales are card-not-present transactions, these customers are more vulnerable to customer fraud than ~~larger other~~ **larger other** customers. ~~We may experience chargebacks arising from cardholder fraud more frequently than providers of payment processing services that service larger businesses and organizations.~~ Business fraud occurs when a business or organization, rather than a cardholder, knowingly uses a stolen or counterfeit card or card number to record a false sales transaction, or intentionally fails to deliver the merchandise or services sold in an otherwise valid transaction. Business fraud also occurs when employees of businesses change the business demand deposit accounts to their personal bank account numbers, so that payments are improperly credited to the employee's personal account. We have established systems and procedures to detect and reduce the impact of business fraud, but there can be no assurance that these measures are or will be effective. Incidents of fraud could increase in the future. Failure to effectively manage risk and prevent fraud could increase our chargeback liability and other liability, which could have a material adverse effect on our business, financial condition and results of operations. ~~New Visa rules associated with chargeback and fraud are now in-being consolidated effect-effective that tighten~~ **April 1, 2025, into the Visa Acquirer monitoring Monitoring and control of risks to combat Program, which will phase out the existing high rates of fraud and disputes.** These new rules impact when merchants are enrolled in the Visa Fraud Monitoring Program (the "VFMP") and the Visa Chargeback **Dispute** Monitoring Program (the "VCMP"). The VFMP and the VCMP target merchants with higher levels of chargebacks ~~and fraud~~. Visa's new rules could have serious implications for the types of businesses that we can support, and high-risk merchants will be impacted by the changes. We pay interchange fees or assessments to ~~the issuing banks-~~ **bank** through the card associations for each transaction that is processed using their credit and debit cards. From time to time, the card associations increase the interchange fees that they charge processors and the sponsoring ~~banks-~~ **bank**. At their sole discretion,

our sponsoring banks— ~~bank may have the right to pass any~~ increases in interchange fees on to us. In addition, our sponsoring banks— ~~bank~~ may seek to increase ~~their~~ its sponsorship fees charged to us, all of which are based upon the dollar amount of the payment transactions we process. If we are not able to pass these fee increases along to customers through corresponding increases in our processing fees, our profit margins will be reduced. ~~Many~~ **Some** of our solutions require or benefit from the use of third- party hardware products that we sell to our customers, such as **kiosks**, payment terminals and point of sale equipment. A number of such products come from limited number of suppliers. Due to our reliance on the products produced by a limited number of suppliers, we are subject to the risk of shortages and long lead times in the supply of certain products. Additionally, various sources of supply- chain risk, including strikes or shutdowns at delivery ports or loss of or damage to our products while they are in transit or storage, intellectual property theft, losses due to tampering, issues with quality or sourcing control, failure by our suppliers to comply with applicable laws and regulation, potential tariffs or other trade restrictions, or other similar problems could limit or delay the supply of our products or harm our reputation. In the event of a shortage or supply interruption from suppliers, we may not be able to develop alternate sources quickly, cost- effectively, or at all. Any interruption or delay in manufacturing supply, any increases in costs, or the inability to obtain these products from alternate sources at acceptable prices and within a reasonable amount of time, could harm our ability to provide products to our customers. We are ~~subject to economic and political risk, the business cycles of our customers and distribution partners and changes in the overall level of consumer and commercial spending, which could negatively impact our business, financial condition and results of operations. The electronic payment industry depends heavily on the overall level of consumer and commercial spending. We are exposed to general economic conditions that affect consumer confidence, consumer spending, consumer discretionary income and changes in consumer purchasing habits , as well as changes in political conditions~~ . Economic conditions in the United States continue to be challenging in various **certain** respects, and the United States economy ~~has continues to experience~~ **experienced** significant ~~inflationary --- inflation pressures~~, elevated interest rates, and challenging labor market conditions. Such ~~adverse~~ **Adverse** economic conditions may adversely affect our financial performance ~~by reducing the number or aggregate volume of transactions made using electronic payments. In addition, demand for consumer products may be adversely affected by increases in interest rates and the reduced availability of financing. A reduction in the amount of consumer or commercial spending could result in a decrease in our revenue and profits. If our customers make fewer purchases or sales of products and services using electronic payments, or consumers spend less money through electronic payments, we will have fewer transactions to process at lower dollar amounts, resulting in lower revenue. Additionally, credit card issuers may reduce credit limits and become more selective in their card issuance practices.~~ We have been adversely impacted by **challenging** ~~current negative~~ economic conditions in the United States and may continue to adversely impacted by such conditions, particularly if current ~~negative~~ economic conditions ~~persist or deteriorate~~ . ~~Further, credit card issuers may reduce credit limits and become more selective in their card issuance practices. We also have a certain amount of fixed and semi- fixed costs, including rent, debt service and salaries, which could limit our ability to quickly adjust costs and respond to changes in our business and the economy.~~ Rapidly evolving domestic and global conditions are beyond our control and could materially adversely affect our business, operations, and results of operations. U. S. and international markets are experiencing uncertain and volatile economic and geopolitical conditions, including from the impacts of **military conflict in the Middle East**, Russian aggression in Ukraine , ~~military conflict in the Middle East~~, rises in fuel costs, sustained inflation, threats or concerns of recession, and supply chain disruptions. These conditions make it extremely difficult for us to accurately forecast and plan future business activities. Together, these circumstances create an environment in which it is challenging for us to predict future operating results. If these uncertain business, macroeconomic or political conditions continue or further decline, ~~or if the military conflicts noted above escalate,~~ our business, financial condition and results of operations could be materially adversely affected. In addition, our business, financial condition and results of operations could be materially adversely affected by outbreaks of illnesses, epidemics or pandemics, climate- related events, including extreme weather events and natural disasters, riots, strikes, civil insurrection or social unrest, terrorist or criminal activities, or other catastrophic events or other political and economic instability. If consumers and businesses do not continue to use cards or ACH as payment mechanisms for their transactions or if the mix of payments among the types of cards and ACH changes in a way that is adverse to us, it could have a material adverse effect on our business, financial condition and results of operations. Regulatory changes may also result in our customers seeking to charge their customers additional fees for use of credit or debit cards. Additionally, in recent years, increased incidents of security breaches have caused some consumers to lose confidence in the ability of businesses to protect their information, causing certain consumers to discontinue use of electronic payment methods. Security breaches could result in financial institutions canceling large numbers of credit and debit cards, or consumers or businesses electing to cancel their cards following such an incident. Our future growth and profitability depend, in part, upon our continued ~~expansion-growth~~ **expansion-growth** within the vertical markets in which we currently operate , ~~the emergence of other vertical markets for electronic payments and our integrated solutions, and our ability to penetrate new vertical markets and our current distribution partners' customer base.~~ As part of our strategy to expand into new ~~vertical markets~~ **customer bases** , we look for acquisition opportunities and partnerships with other businesses that will allow us to increase our market penetration, technological capabilities, product offerings and distribution capabilities. Although we expect to continue to execute our acquisition strategy: • we may not be able to identify suitable acquisition candidates or acquire additional assets on favorable terms; • we may compete with others to acquire assets, which competition may increase, and any level of competition could result in decreased availability or increased prices for acquisition candidates; • we may compete with others for select acquisitions and our competition may consist of larger, better- funded organizations with more resources and easier access to capital; • we may experience difficulty in anticipating the timing and availability of acquisition candidates; • we may not be able to obtain the necessary financing, on favorable terms or at all, to finance any of our potential acquisitions; and • we may not be able to generate cash necessary to execute our acquisition strategy. The occurrence of any of these factors could adversely affect our growth strategy. ~~Our expansion into new~~ **Growth in our current** vertical

markets also depends upon our ability to adapt our existing technology or to develop new technologies to meet the particular needs of each new vertical market and existing customers. We may not have adequate financial or technological resources to develop effective and secure services or distribution channels that will satisfy the demands of these new customers vertical markets. Penetrating these new customers in our existing vertical markets may also prove to be more challenging or costly or take longer than we may anticipate. If we fail to expand into new vertical markets and increase our penetration into existing vertical markets, we may not be able to continue to grow our revenues and earnings. **In September 2024, we completed the sale of our Merchant Services Business. There is no assurance that we will be able to realize the anticipated benefits from the disposition of our Merchant Services Business. Moreover, there are post-closing risks associated with the ancillary agreements entered into by us at the closing, including the transition services agreement, the processing services agreement, and the restrictive covenant agreement. In addition, pursuant to the Purchase Agreement, we agreed to indemnify Payroc with respect to certain matters and we agreed to retain certain liabilities related to the Merchant Services Business, which in any such case could result in liability to us following the closing. Further, we are now highly dependent on the success of our two remaining business segments, our Public Sector segment and Healthcare segment.**

In evaluating and determining the purchase price for a prospective acquisition, we estimate the future revenues and profits from that acquisition based largely on historical financial performance. Following an acquisition, we may experience some customer attrition in the number of customers serviced by an acquired provider of payment processing services or included in an acquired portfolio of merchant accounts. Should the rate of post-acquisition customer attrition exceed the rate we forecasted, the revenues and profits from the acquisition may be less than we estimated, which could result in losses or a decline in profits, as well as potential impairment charges. We perform a due diligence review of each of our acquisition partners. This due diligence review, however, may not adequately uncover all of the contingent or undisclosed liabilities we may incur as a consequence of the proposed acquisition, exposing us to potentially significant, unanticipated costs, as well as potential impairment charges. An acquisition may also subject us to additional regulatory burdens that affect our business in potentially unanticipated and significantly negative ways. The acquisition of a provider of payment processing services, as well as a portfolio of merchant accounts, requires the transfer of various data processing functions and connecting links to our systems and those of our third-party service providers. If the transfer of these functions and links does not occur rapidly and smoothly, payment processing delays and errors may occur, resulting in a loss of revenues, increased customer attrition and increased expenditures to correct the transitional problems, which could preclude our attainment of, or reduce, our anticipated revenue and profits. Additionally, any integrations **Integrations** that do not occur rapidly and smoothly could divert the attention of management away from other strategic matters, including, but not limited to, acquisitions or product development. In connection with some acquisitions, we may incur non-recurring severance expenses, restructuring charges or change of control payments. These expenses, charges or payments, as well as the initial costs of integrating the personnel and facilities of an acquired business with those of our existing operations, may adversely affect our operating results during the initial financial periods following an acquisition. In addition, the integration of newly acquired companies may lead to diversion of management attention from other ongoing business concerns. We may not be able to successfully manage our intellectual property. Our intellectual property is critical to our future success, particularly in our strategic verticals where we may offer proprietary software solutions to our customers. We rely on a combination of contractual license rights and copyright, trademark and trade secret laws to establish and protect our proprietary technology. Third parties may challenge, invalidate, circumvent, infringe or misappropriate our intellectual property or the intellectual property of our third-party licensors, or such intellectual property may not be sufficient to permit us to take advantage of current market trends or otherwise to provide competitive advantages, which could result in costly redesign efforts, discontinuance of certain service offerings or other competitive harm. Others, including our competitors, may independently develop similar technology, duplicate our products and services, design around or reverse engineer our intellectual property, and in such cases neither we nor our third-party licensors may be able to assert intellectual property rights against such parties. Further, our contractual license arrangements may be subject to termination or renegotiation with unfavorable terms to us, and our third-party licensors may be subject to bankruptcy, insolvency and other adverse business dynamics, any of which might affect our ability to use and exploit the products licensed to us by these third-party licensors. We may have to litigate to enforce or determine the scope and enforceability of our intellectual property rights (including litigation against our third-party licensors), which is expensive, could cause a diversion of resources and may not prove successful. The loss of intellectual property protection or the inability to obtain third-party intellectual property could harm our business and ability to compete. We may be subject to infringement claims. We may be subject to costly litigation if our products or services are alleged to infringe upon or otherwise violate a third party's proprietary rights. Third parties may have, or may eventually be issued, patents that could be infringed by our products and services. Any of these third parties could make a claim of infringement against us with respect to our products and services. We may also be subject to claims by third parties for patent infringement, breach of copyright, trademark, license usage or other intellectual property rights. Any claim from third parties may result in a limitation on our ability to use the intellectual property subject to these claims. Additionally, in recent years, individuals and groups have been purchasing intellectual property assets for the sole purpose of making claims of infringement and attempting to extract settlements from companies like ours. Even if we believe that intellectual property related claims are without merit, defending against such claims is **time-consuming resource intensive** and expensive and could result in the diversion of the time and attention of our management and employees. Claims of intellectual property infringement also might require us to redesign affected products or services, enter into costly settlement or license agreements, pay costly damage awards for which we may not have insurance, or face a temporary or permanent injunction prohibiting us from marketing or selling certain of our products or services. Even if we have an agreement for indemnification against such costs, the indemnifying party, if any in such circumstances, may be unable to uphold its contractual obligations. If we cannot or do not license the infringed technology on reasonable terms or substitute similar technology from another source, our revenue and earnings could be materially and

adversely affected. **If we lose key personnel, or if their reputations are damaged, our business, financial condition and results of operations may be adversely affected, and proprietary information of our company could be shared with our competitors.** We depend on the ability and experience of a number of our key personnel, particularly Messrs. Daily, Whitson and Stanford, who have substantial experience with our operations, the rapidly changing payment processing industry and the vertical markets in which we offer our products and services. Many of our key personnel have worked for us for a significant amount of time or were recruited by us specifically due to their experience. **Our success depends in part upon the reputation and influence within the industry of our senior managers who have, over the years, developed long standing and favorable relationships with our vendors, card associations, bank sponsors and other payment processing and service providers.** It is possible that the loss of the services of one or a combination of our senior executives or key managers could have a material adverse effect on our business, financial condition and results of operations. In addition, contractual obligations related to confidentiality and assignment of intellectual property rights may be ineffective or unenforceable, and departing employees may share our proprietary information with competitors in ways that could adversely impact us. **In a dynamic industry like ours, our success and growth depend on our ability to attract, recruit, retain and develop qualified employees.** Our business functions at the intersection of rapidly changing technological, social, economic and regulatory developments that require a wide- ranging set of expertise and intellectual capital. For us to continue to successfully compete and grow, we must attract, recruit, develop and retain the necessary personnel who can provide the needed expertise across the entire spectrum of our intellectual capital needs. While we have a number of key personnel who have substantial experience with our operations, we must also develop our personnel to provide succession plans capable of maintaining continuity in the midst of the inevitable unpredictability of human capital. The market for qualified personnel is competitive, and we may not succeed in recruiting additional personnel or may fail to effectively replace current personnel who depart with qualified or effective successors. Our effort to retain and develop personnel may also result in significant additional expenses, which could adversely affect our profitability. We can make no assurances that qualified employees will continue to be employed or that we will be able to attract and retain qualified personnel in the future. Failure to retain or attract key personnel could have a material adverse effect on our business, financial condition and results of operations. We have experienced in the past, and expect to continue to experience, seasonal fluctuations in our revenues **as a result of consumer spending patterns. Historically our revenues have been strongest in our first, third and fourth fiscal quarters and weakest in our second fiscal quarter. This is due to the increase in the number and amount of electronic payment transactions related to seasonal retail events, such as holiday and vacation spending.** The number of business days in a month or quarter also may affect seasonal fluctuations. **We also experience volatility in certain Certain revenues in our Public Sector segment fluctuate with other -- the metrics fiscal calendars of our customers. Transactional revenue for our Education customers is strongest in August, such September, October, January and February, at the start of each semester, and generally weakens throughout the semester, with little revenue in the summer months of June and July. Operating expenses show less seasonal fluctuation, with the result that net income is subject to the same seasonal factors as customers' our revenues. The growth in our business may have partially overshadowed seasonal trends to date, transactions and dollar volume seasonal impacts on our business may be more pronounced in the future.** Volatility in our key operating metrics or their rates of growth could have a negative impact on our financial results and investor perceptions of our business prospects. We are the subject of various claims and legal proceedings and may become the subject of claims, litigation or investigations which could have a material adverse effect on our business, financial condition or results of operations. In the ordinary course of business, we are the subject of various claims and legal proceedings and may become the subject of claims, litigation or investigations, including commercial disputes and employee claims, such as claims of age discrimination, sexual harassment, gender discrimination, immigration violations or other local, state and federal labor law violations, and from time to time may be involved in governmental or regulatory investigations or similar matters arising out of our current or future business. Any claims asserted against us or our management, regardless of merit or eventual outcome, could harm our reputation or the reputation of our management and have an adverse impact on our relationship with our customers, distribution partners and other third parties and could lead to additional related claims. In light of the potential cost and uncertainty involved in litigation, we have in the past and may in the future settle matters even when we believe we have a meritorious defense. Certain claims may seek injunctive relief, which could disrupt the ordinary conduct of our business and operations or increase our cost of doing business. Our insurance or indemnities may not fully cover all claims that may be asserted against us. Furthermore, there is no guarantee that we will be successful in defending ourselves in pending or future litigation or similar matters under various laws. Any judgments or settlements in any pending litigation or future claims, litigation or investigation could have a material adverse effect on our business, financial condition and results of operations. Our contracts are primarily denominated in U. S. dollars, and therefore, substantially all of our revenue is not subject to foreign currency risk. However, there has been, and may continue to be, significant volatility in global stock markets and foreign currency exchange rates that result in the strengthening of the U. S. dollar against foreign currencies in which we conduct business. The strengthening of the U. S. dollar increases the real cost of our products to our end- customers outside of the United States and may lead to reduced demand for our services. If the U. S. dollar continues to strengthen, this could adversely affect our financial condition and operating results. Our operating expenses incurred outside the United States and denominated in foreign currencies are increasing and are subject to fluctuations due to changes in foreign currency exchange rates. If we are not able to successfully hedge against the risks associated with foreign currency fluctuations, our financial condition and operating results could be adversely affected. Our international operations subject us to additional risks which could have an adverse effect on our business, operating results, and financial condition. We employ resources in India, to support our onshore operations. Countries outside of the United States may be subject to relatively higher degrees of political and social instability and may lack the infrastructure to withstand political unrest or natural disasters. The occurrence of natural disasters, pandemics, or political or economic instability in these countries could interfere with work performed by these labor sources or could result in our having

to replace or reduce these labor sources. If countries in which we operate experience civil or political unrest or acts of terrorism, our operations in such countries could be materially impaired. Our vendors in other countries could potentially shut down suddenly for any reason, including financial problems or personnel issues. Such disruptions could decrease efficiency, increase our costs and have an adverse effect on our business or results of operations. Further, many foreign data privacy regulations (including India's Digital Personal Data Protection Act) can be more stringent than those in the United States. These laws and regulations are rapidly evolving and changing and could have an adverse effect on our operations. Our obligations and requirements under these laws and regulations are subject to uncertainty in how they may be interpreted by government authorities and regulators. The costs of compliance with, and the other burdens imposed by, these and other laws or regulatory actions may increase our operational costs, affect our customers' willingness to permit us to use and store personal data, prevent us from selling our products or services, and / or affect our ability to invest in or jointly develop products. Failure to comply with these laws may result in governmental enforcement actions, private claims, including class action lawsuits, and damage to our reputation. We may also face audits or investigations by one or more foreign government agencies relating to our compliance with these regulations. Risks Related to Regulation We are subject to extensive laws and government regulation, the costs of compliance with which can be significant, and our actual or perceived failure to comply with such obligations may subject us to penalties and otherwise have an unfavorable impact on our business, financial condition and results of operations. We are subject to numerous federal and state laws and regulations that affect the electronic payments industry and the other industries in which we provide services. Regulation of our industry has increased significantly in recent years and is constantly evolving. We are also subject to other laws and regulations, including those addressing U. S. financial services, consumer protection, escheat and privacy and information security, among other subjects. Changes to statutes, regulations or industry standards, including interpretation and implementation of statutes, regulations or standards, could increase our cost of doing business or affect the competitive balance. Failure to comply with laws and regulations may have an adverse effect on our business, including the limitation, suspension or termination of services provided to, or by, third parties, and the imposition of other penalties or fines. To the extent these laws and regulations negatively impact the business, operations or financial condition of our customers, our business and results of operations could be materially and adversely affected because, among other matters, our customers could have less capacity to purchase products and services from us, could decide to avoid or abandon certain lines of business, or could seek to pass on increased costs to us by negotiating price reductions. In addition, we could be required to invest a significant amount of time and resources in response to new or changes to existing laws, regulations or oversight, or to modify the manner in which we contract with or provide products and services to our customers; and those laws and regulations could directly or indirectly limit how much we can charge for our services. We may not be able to update our existing products and services, or develop new ones, to satisfy our customers' needs. Any of these events, if realized, could have a material adverse effect on our business, results of operations and financial condition. Various laws and regulations, including those in other industries in which we provide services, even if such laws and regulations are not directed at us, may require us to make significant efforts to change our products and services and may require that we incur additional compliance costs and change how we price our products and services to our customers and distribution partners. Implementing new compliance risk mitigation strategies efforts can be significant with the complexity of regulatory requirements, and we are devoting and will continue to devote significant resources to address compliance requirements. Furthermore, regulatory actions may cause changes in business practices by us and other industry participants which could affect how we market, price and distribute our products and services, and which could materially adversely affect our business, financial condition and results of operations. In addition, even an inadvertent failure to comply with laws and regulations, as well as rapidly evolving social expectations of corporate fairness, could damage our business or our reputation. Compliance with the Dodd- Frank Act and other federal and state regulations applicable to our business may increase our compliance costs, limit our revenues and otherwise negatively affect our business. Since the enactment of the Dodd- Frank Act, there have been substantial reforms to the supervision and operation of the financial services industry, including numerous new regulations that have imposed additional compliance costs and, in some cases, limited revenue sources for us and our financial institution partners and customers. Among other things, the Dodd- Frank Act established the CFPB, which is empowered to conduct rule- making and supervision related to, and enforcement of, federal consumer financial protection laws. The CFPB has issued guidance that applies to " supervised service providers, " which the CFPB has defined to include service providers, like us, to CFPB supervised banks and nonbanks. In **that regard the CFPB July 25, 2024 report entitled The Cost of Electronic Payments in K- 12 Schools, the report included discussion on the CFPB's Fall 2023 edition of their Supervisory Highlights report and a 2014 USDA Policy Memorandum regarding school lunch fees. The CFPB report concluded that certain payment processing practices utilized by the Company and other participants in our industry may violate consumer financial protection laws. The appearance of being involved in unfair trade practices and violating consumer protection laws when offering payment processing services to our customers could harm our reputation with our customers. Further, compliance with emerging sector- specific regulations may negatively impact our business, financial condition and results of operations by requiring us to alter our fee structure or payment processing practices. The CFPB's focus on these payment processing practices may also lead to litigation against the Company. Other companies in our industry that serve the public school sector have been the target of litigation related to the CFPB's increased focus on certain payment processing company practices as potentially volatile of consumer financial laws and as unfair trade practices. As sector- specific laws, governmental rules and regulations develop to implement restrictions on payment processing services within certain sectors, we could become the subject of similar litigation, which could adversely impact our reputation, business and financial results.** In addition, federal and state agencies have recently proposed or enacted cybersecurity regulations, such as the Cybersecurity Requirements for Financial Services Companies issued by the New York State Department of Financial Services and the Cyber Security Resource Guide for Financial Institutions issued November 2022 by the Federal Financial Institutions Examination Council replacing the

2018 Cyber Security Resource Guide. Cybersecurity regulations and guidance are applicable to large bank holding companies and their subsidiaries, as well as to service providers to those organizations. Any new rules and regulations implemented by the CFPB, state or other authorities or in connection with the Dodd- Frank Act could, among other things, slow our ability to adapt to a rapidly changing industry, require us to make significant additional investments to comply with them, redirect time and resources to compliance obligations, modify our products or services or the manner in which they are provided, or limit or change the amount or types of revenue we are able to generate. Interchange fees, which the payment processor typically pays to the card issuer in connection with credit and debit card transactions, are subject to ~~increasingly intense~~ legal, regulatory and legislative scrutiny. In particular, the Dodd- Frank Act regulates and limits debit card fees charged by certain card issuers and allows businesses and organizations to set minimum dollar amounts for the acceptance of credit cards. Specifically, under the commonly known “ Durbin Amendment ” to the Dodd- Frank Act, the interchange fees that certain issuers charge businesses and organizations for debit transactions are regulated by the Federal Reserve and must be “ reasonable and proportional ” to the cost incurred by the issuer in authorizing, clearing and settling the transactions. Rules released by the Federal Reserve in July 2011 to implement the Durbin Amendment mandate a cap on debit transaction interchange fees for card issuers with assets of \$ 10 billion or greater. Effective October 1, 2012, debit card issuers are permitted a fraud- prevention adjustment. Since October 2011, a payment network may not prohibit a card issuer from contracting with any other payment network for the processing of electronic debit transactions involving the card issuer’ s debit cards, and card issuers and payment networks may not inhibit the ability of businesses and organizations to direct the routing of debit card transactions over any payment networks that can process the transactions. Rules implementing the Dodd- Frank Act also contain certain prohibitions on payment network exclusivity and merchant routing restrictions. These restrictions could negatively affect the number of debit transactions processed, and prices charged per transaction, which would negatively affect our business. If we violate **the Family Educational Rights and Privacy Act (“ FERPA ”)** or **Protection of Pupil Rights Amendment (“ PPR ”)**, it could result in a material breach of contract with one or more of our customers in our Education **sub**-vertical and could harm our reputation. Further, if we disclose student information in violation of FERPA or PPR, our access to student information could be suspended. Our systems and solutions must also comply, in certain circumstances, with FERPA and PPR, as well as with rapidly emerging state student data privacy laws that require schools to protect student data and to adopt privacy policies which can significantly vary from one state to another. FERPA generally prohibits an educational institution from disclosing personally identifiable information from a student’ s education records without a parent’ s consent unless certain statutory exceptions apply. Our school customers and their students disclose to us, and we may store, certain information that originates from or comprises a student education record under FERPA. PPR puts limits on “ survey, analysis or evaluations ” that may come into play when schools employ internet- based educational services. Schools are required to develop policies that address, among other things, the collection, disclosure or use of personal information collected from students for the purpose of marketing or selling that information, and can place restrictions on third parties’ use of that data. As an entity that provides services to educational institutions, we are indirectly subject to FERPA’ s and PPR’ s privacy requirements, and we may not transfer or otherwise disclose or use any personally identifiable information from a student record to another party other than on a basis and in a manner permitted under the statutes. If we violate FERPA or PPR, it could result in a material breach of contract with one or more of our customers and could reduce our revenues or harm our reputation. Further, if we disclose student information in violation of FERPA or PPR, our access to student information could be suspended, thus inhibiting our business operations. Actual or perceived failures to comply with applicable privacy and security laws and regulations could result in a material breach of contract with one or more of our customers in our Healthcare vertical, harm our reputation and subject us to substantial civil and criminal penalties under laws such as HIPAA and state privacy and security laws. The data protection landscape is rapidly evolving, and we are or may become subject to numerous federal and state laws and regulations governing the collection, use, disclosure, retention, and security of health- related and other personal information. The cost of compliance with the laws and regulations is high and is likely to increase in the future. Any failure or perceived failure by us to comply with applicable data privacy and security laws or regulations, our internal policies and procedures or our contracts governing our processing of personal information could result in negative publicity, government investigations and enforcement actions, claims by third parties and damage to our reputation, any of which could have an adverse effect on our operations, financial performance and business. For example, the HIPAA privacy and security regulations extensively regulate the use and disclosure of PHI and require business associates such as our company to implement administrative, physical and technical safeguards to protect the security of such information. If we are unable to properly protect the privacy and security of PHI entrusted to us, we could be found to have breached our contracts with our customers and / or be subject to investigation by the **United States Department of Health and Human Services (“ HHS ”)** Office for Civil Rights (“ OCR ”). In the event OCR finds that we have failed to comply with applicable HIPAA privacy and security standards, we could face civil and criminal penalties. OCR has become an increasingly active regulator and has signaled its intention to continue this trend. OCR has the discretion to impose penalties without being required to attempt to resolve violations through informal means. Further, OCR may require companies to enter into resolution agreements and corrective action plans that impose ongoing compliance requirements. OCR enforcement activity can result in financial liability and reputational harm, and responses to such enforcement activity can consume significant internal resources. In addition to enforcement by OCR, state attorneys general are authorized to bring civil actions under either HIPAA or similar state laws, seeking either injunctions or damages in response to violations that threaten the privacy of state residents. Although we have implemented and maintain policies, processes and a compliance program infrastructure to assist us in complying with these laws and regulations and our contractual obligations, we cannot provide assurance regarding how these laws and regulations will be interpreted, enforced or applied to our Healthcare vertical operations. Further, the **Federal Trade Commission (“ FTC ”)** has prosecuted certain uses and disclosures of personal information and data breach cases as unfair and / or deceptive acts or practices under the Federal Trade Commission Act or

under the FTC Health Breach Notification Act. If we violate the federal **AKS**, **Anti- Kickback Statute**, the ~~CMP~~ **Civil Monetary Penalties** Law, the ~~federal FCA~~ **False Claims Act**, the Cures Act or other federal or state laws and regulations applicable to healthcare services, it could result in a material breach of contract with one or more of our customers in our Healthcare vertical, harm our reputation and subject us to substantial civil and criminal penalties. We strive to comply with healthcare laws, regulations and other requirements applicable to us directly and to our customers and contractors, but there can be no assurance that our operations will not be challenged or impacted by enforcement initiatives. We have been, and in the future may become, involved in governmental investigations, audits, reviews and assessments. Even an unsuccessful challenge by regulatory and other authorities or private whistleblowers could be expensive and time- consuming, could result in loss of business, exposure to adverse publicity and injury to our reputation and could adversely affect our ability to retain and attract customers. Healthcare laws, regulations and other requirements impacting our Healthcare vertical operations include the following: Anti- Kickback Laws. A number of federal and state laws govern patient referrals, financial relationships with physicians and other referral sources and inducements to providers and patients, including restrictions contained in amendments to the Social Security Act, commonly known as the **federal Anti- Kickback Statute (" AKS ")**. The AKS contains a limited number of exceptions, and the **Office of Inspector General for the HHS (" OIG ")** has created regulatory safe harbors to the AKS. Activities that comply with a safe harbor are deemed protected from prosecution under the AKS. Certain of our contracts and other arrangements may not meet an exception or a safe harbor. Failure to qualify for safe harbor protection does not mean the arrangement necessarily violates the AKS, but it may subject the arrangement to greater government scrutiny. We cannot provide assurance that practices outside of a safe harbor will not be found to violate the AKS. Allegations of violations of the AKS may be brought under the **federal civil Civil Monetary Penalties (" the CMP Law ")**, which requires a lower burden of proof than the AKS. The OIG has a longstanding concern that percentage- based billing arrangements may increase the risk of improper billing practices. The OIG recommends that medical billing companies develop and implement comprehensive compliance programs to mitigate this risk. In addition, certain states have adopted laws or regulations forbidding splitting of fees with non- physicians, which may be interpreted to prevent business service providers, including medical billing providers, from using a percentage- based billing arrangement. While we have developed and implemented a comprehensive billing compliance program that we believe is consistent with federal guidance, our failure to ensure compliance with controlling legal requirements, accurately anticipate the application of these laws and regulations to our business and contracting model, or ~~other failure to~~ comply with regulatory requirements, could create liability for us, result in adverse publicity and negatively affect our business. Violation of the AKS is a felony, and penalties may include imprisonment, criminal fines and substantial civil monetary penalties. In addition, submission of a claim for items or services generated in violation of the AKS may be subject to additional penalties under the federal **False Claims Act (" FCA ")** as a false or fraudulent claim. False or Fraudulent Claim Laws; Medical Billing and Coding. Medical billing, coding and collection activities are governed by numerous federal and state civil and criminal laws, regulations and sub- regulatory guidance. Our Healthcare vertical may be subject to, or contractually required to comply with, numerous federal and state laws that prohibit false or fraudulent claims including but not limited to the federal FCA, the CMP Law and state equivalents. For example, errors or the unintended consequences of data manipulations by us or our systems with respect to the entry, formatting, preparation or transmission of claims, coding, audit, eligibility and other information, may result in allegations of false or fraudulent claims. False or fraudulent claims under the FCA and other laws include, but are not limited to, billing for services not rendered, making or causing to be made or used a false record or statement that is material to a false claim, failing to report and refund known overpayments within 60 days of identifying the overpayment, misrepresenting actual services rendered, improper coding and billing for medically unnecessary items or services. Submission of a claim for an item or service generated in violation of the AKS constitutes a false or fraudulent claim. In addition, the FCA prohibits the knowing submission of false claims or statements to the federal government, including to Medicare and Medicaid programs. Although simple negligence will not give rise to liability under the FCA, " knowingly " submitting a false claim may result in liability. When an entity is determined to have violated the FCA, the government may impose substantial civil fines and penalties for each false claim, plus treble damages, and exclude the entity from participation in federal healthcare programs. Private parties are able to bring qui tam, or whistleblower, lawsuits on behalf of the government in connection with alleged false claims submitted to the government, and these private parties are entitled to share in any amounts recovered by the government. Several states, including states in which we operate, have adopted their own false claims provisions and their own whistleblower provisions whereby a private individual may file a civil lawsuit in state court. Some fraud and abuse laws, such as the CMP Law, require a lower burden of proof than other fraud, waste and abuse laws. Federal and state authorities increasingly assert liability under the CMP Law, especially where they believe they cannot meet the higher burden of proof requirements under the various criminal healthcare fraud provisions. Current penalties under the CMP Law are significant and may result in penalties of up to three times the amount claimed or received. Civil monetary penalties, including those imposed under the AKS, FCA, and CMP Law are updated annually based on changes to the consumer price index. Although we believe our processes are consistent with applicable reimbursement rules and industry practice, a court, government authority or whistleblower could challenge these processes. In addition, we cannot guarantee that federal and state authorities will regard any billing and coding errors we process or make as inadvertent or will not hold us responsible for any compliance issues related to claims, reports and other information we handle on behalf of our customers. We cannot predict the impact of any enforcement actions under the various false claims and fraud, waste and abuse laws applicable to our operations. Even an unsuccessful challenge of our practices could cause us to incur adverse publicity and significant legal and related costs. The laws and regulations in this area are both broad and vague and judicial interpretation can be inconsistent. We review our practices with regulatory experts in an effort to comply with all applicable laws and regulatory requirements. However, we are unable to predict how laws and regulations will be interpreted or the full extent of their application, particularly to services that are not directly billed to or reimbursed by federal healthcare programs, such as transaction processing services. Any determination by a federal or state

regulatory authority that any of our activities or those of our customers or vendors violate any of these laws or regulations could: ~~(i)~~ subject us to civil or criminal penalties, ~~(ii)~~ require us to enter into corporate integrity agreements or similar agreements with government regulators to meet ongoing compliance obligations, ~~(iii)~~ require us to change or terminate some portions of our business, ~~(iv)~~ require us to refund a portion of our service fees, and / or ~~(v)~~ disqualify us from providing services to customers that are, or do business with, government programs. Any of these could result in a material adverse impact on our business, results of operations or financial condition. Even an unsuccessful challenge of our activities could result in adverse publicity and could require a costly response. The Cures Act and Implementing Regulations (Information Blocking and **Health Information Technology ("HIT") Standards and Certification Requirements**). Standards regarding electronic exchange of information and interoperability are subject to regular revision and updates, and we are required to modify and enhance products and services accordingly. The Information Blocking Rule prohibits healthcare providers, **Health Information Exchange ("HIEs")**, and HIT developers, including our subsidiary that provides electronic medical records, from information blocking, which is defined as practices likely to interfere with, prevent, or materially discourage access, exchange, or use of **electronic health information ("EHI")**, except as required by law or specified by HHS as a reasonable and necessary activity. Civil monetary penalties for information blocking by HIT developers are substantial, up to \$ 1 million per violation. The HIT Standards and Certification Criteria Final Rule imposes new criteria related to EHI export and standardized APIs for patient services, and HIT developers of certified HIT need to ensure that their products and services meet the requisite technical standards by the relevant deadlines and continue to evolve as developers and other stakeholders release revised versions of these standards. Additionally, HIT developers that participate in the ONC Health IT Certification Program, like ~~is us~~, must make various certifications regarding their HIT and attest to compliance with applicable conditions of certification, including those related to information blocking. These rules apply to certain services we offer, and customers may insist that we develop additional solutions that comply with these various interoperability requirements, which could subject us to additional costs. We currently have and likely will continue to have certain solutions certified by ONC, which could further increase development costs and delay customer sales and implementations. We also may incur costs in periods prior to the corresponding recognition of revenue. To the extent current regulations are subsequently changed or supplemented, or for other reasons beyond our control, customers may postpone or cancel their decisions to purchase or implement such solutions. Exclusion from participation in government healthcare programs. The OIG may or must exclude individuals and entities involved in misconduct related to federal healthcare programs, such as Medicare and Medicaid, from participation in those programs. Federal law prohibits federal healthcare programs from paying for items or services furnished, ordered, or prescribed by an individual or entity excluded from participation. The prohibition against federal program payment extends to payment for administrative and management services not directly related to patient care. Civil penalties may be imposed against providers and entities that employ or enter into contracts with excluded individuals to provide items or services to federal healthcare program beneficiaries. We have implemented compliance policies and procedures to screen for excluded individuals. However, if we employ or contract with an excluded individual or entity, we could face significant consequences such as exclusion from participation in federal healthcare programs, civil monetary penalties, and treble damages. In addition, we could be liable under our customer contracts, if we are excluded by the OIG or employ or contract with an excluded individual or entity. Recent and future developments in the healthcare industry, particularly those related to HIT, could have a material adverse impact on our business, results of operations or financial condition. A material portion of our revenue is derived from the healthcare industry, which is highly regulated and subject to changing political, legislative, regulatory and other influences. There are numerous federal, state and private initiatives seeking to increase the use of HIT as a means of improving care and reducing costs. For example, HITECH and the Cures Act promote the use of EHR technology, interoperability and the efficient exchange of EHI. These statutes are implemented mainly through HIPAA, CMS' s Promoting Interoperability Program, and ONC' s Information Blocking Rule and HIT Standards and Certification Criteria Final Rule. These and other initiatives may result in additional legal or regulatory requirements, the cost of compliance with which may be significant; encourage more companies to enter our markets, provide advantages to our competitors; and / or result in the development of competitive technology solutions. Any such initiatives also may result in a reduction of expenditures by existing or potential customers, which could have a material adverse impact on our business, results of operations or financial condition. In addition, other general reductions in expenditures by healthcare industry constituents could result from, among other things, government regulation or private initiatives that affect the manner in which providers interact with patients, payers or other healthcare industry constituents, including changes in pricing or means of delivery of healthcare solutions. In addition, cost containment efforts at the federal and state levels may affect industry expenditures. For example, the Budget Control Act of 2011 requires automatic spending reductions to reduce the federal deficit. CMS began imposing a 2 % reduction on payments of Medicare claims in 2013. These reductions have been extended through the first six months of 2032. In addition, the American Rescue Plan Act of 2021 increased the federal budget deficit in a manner that triggered an additional statutorily mandated sequestration. As a result, an additional payment reduction of up to 4 % was required to take effect in January 2022. However, Congress has delayed implementation of this payment reduction until 2025. We anticipate that the federal deficit will continue to place pressure on government healthcare programs. Even if general expenditures by healthcare industry constituents remain the same or increase, other developments in the healthcare industry may reduce spending on healthcare IT and services or in some or all of the specific markets we serve or are planning to serve. In addition, our customers' expectations regarding pending or potential healthcare industry developments also may affect their budgeting processes and spending plans with respect to the types of solutions we provide. For example, use of our solutions could be affected by: • changes in the billing patterns of providers; • ~~changes in~~ the design of health insurance plans; and • ~~changes in~~ the contracting methods payers use in their relationships with providers. The healthcare industry has changed significantly in recent years, and we expect that significant changes will continue to occur. The timing and impact of developments in the healthcare industry are difficult to predict. We cannot be sure that the markets for our solutions will continue to exist at their current levels or will not

change in ways that adversely affect us, or that we will have adequate technical, financial and marketing resources to react to changes in those markets. We may be a party to regulatory and other proceedings that could result in unexpected adverse outcomes. From time to time, we have been, are and may in the future be, a party to legal and regulatory proceedings, including investigations, audits, and other reviews. There are an increasing number of investigations and proceedings in the healthcare industry that seek recovery under HIPAA, AKS, the FCA, the CMP, state laws and other statutes and regulations applicable to our business as described in more detail above. Such proceedings can result in verdicts, injunctive relief or other sanctions that may affect how we operate our business and / or have an adverse effect on our financial condition. Violations of applicable statutes and regulations may result in criminal penalties and ~~in~~ substantial civil penalties, including exclusion from government healthcare programs, and settlements of lawsuits involving Medicare and Medicaid issues routinely require monetary penalties and corporate integrity agreements. Assessing and predicting the outcome of these matters involves substantial uncertainties. Unexpected outcomes in these legal proceedings, or changes in management's evaluations or predictions and accompanying changes in established reserves, could have a material adverse impact on our business, results of operations or financial condition. Litigation is costly, time- consuming and disruptive to normal business operations. In addition, the defense of these matters could result in continued diversion of our management's time and attention away from business operations, which could also harm our business. Even if these matters are resolved in our favor, the uncertainty and expense associated with unresolved legal proceedings could harm our business and reputation. We must comply with laws and regulations prohibiting unfair or deceptive acts or practices, and any failure to do so could materially and adversely affect our business. We and many of our customers are subject to Section 5 of the Federal Trade Commission Act prohibiting unfair or deceptive acts or practices (**referred to as "UDAAP"**), provisions of the Dodd- Frank Act that prohibit UDAAP, the Telemarketing Sales Act, the Electronic Fund Transfer Act and other laws, rules and or regulations, which may directly impact the activities of certain of our customers. These rules may subject us, as the electronic payment processor or provider of certain services, to investigations, fees, fines and disgorgement of funds if we ~~were~~ **are** deemed to have improperly aided and abetted or otherwise provided the means and instrumentalities to facilitate the illegal or improper activities of the customer through our services. Various federal and state regulatory enforcement agencies including the Federal Trade Commission and state attorneys general have authority to take action against non- banks that engage in UDAAP, or violate other laws, rules and regulations. To the extent we are processing payments or providing products and services for a customer that may be in violation of laws, rules and regulations, we may be subject to enforcement actions and as a result may incur losses and liabilities that may adversely affect our business. Because of our international operations we could be adversely affected by violations of the US Foreign Corrupt Practices Act (the "FCPA ") and similar anti- bribery laws of other countries in which we provide services or have employees. The FCPA and similar anti- bribery laws generally prohibit companies and their intermediaries from making improper payments to government officials or other third parties for the purpose of obtaining or retaining business or gaining any business advantage. While our policies mandate compliance with these anti- bribery laws, we cannot provide assurance that our internal control policies and procedures always protect us from reckless or criminal acts committed by our employees, contractors or agents. Failure to comply with the FCPA ~~and~~ could result in the imposition of civil or criminal fines and penalties and could disrupt our business and adversely affect our results of operations, cash flows and financial condition. Numerous other federal laws affect our business, and any failure to comply with those laws could harm our business. Our payment facilitator solutions present certain regulatory challenges, principally those relating to money transmitter issues. To address these challenges we, along with our third- party service providers, use structural arrangements designed to prevent us from receiving or controlling our ~~our~~ ~~customer's~~ funds **removing** ~~and therefore remove~~ our activities from the scope of money transmitter ~~regulation~~ **regulations**. There can be no assurance that these structural arrangements will remain effective as money transmitter laws continue to evolve or that the applicable regulatory bodies, particularly state agencies, will view our payment facilitator activities as compliant. Our business may also be subject to the **Fair Credit Reporting Act ("FCRA ")**, which regulates the use and reporting of consumer credit information and imposes disclosure requirements on entities that take adverse action based on information obtained from credit reporting agencies. We could be liable if our practices under the FCRA do not comply with the FCRA or regulations under it. The Housing Assistance Tax Act of 2008 included an amendment to the Internal Revenue Code of 1986, as amended (the "Code "), that requires information returns to be made for each calendar year by payment processing entities and third- party settlement organizations with respect to payments made in settlement of electronic payment transactions and third- party payment network transactions occurring in that calendar year. Reportable transactions are also subject to backup withholding requirements. We could be liable for penalties if our information returns are not in compliance with these regulations. Depending on how our products and services evolve, we may be subject to a variety of additional laws and regulations, including those governing money transmission, gift cards and other prepaid access instruments, electronic funds transfers, anti- money laundering, counter- terrorist financing, restrictions on foreign assets, ~~gambling~~, banking and lending, U. S. Safe Harbor regulations, and import and export restrictions. Additionally, we are contractually required to comply with certain anti- money laundering regulations in connection with our payment processing activities. These regulations are generally governed by **the Financial Crimes Enforcement Network ("FinCEN ")** and **the Office of Foreign Assets Control ("OFAC ")**. Our efforts to comply with these laws and regulations could be costly and result in diversion of management time and effort and may still not guarantee compliance. Regulators continue to increase their scrutiny of compliance with these obligations, which may require us to further revise or expand our compliance program, including the procedures we use to verify the identity of our customers, and to monitor transactions. If we are found to be in violation of any such legal or regulatory requirements, we may be subject to monetary fines or other penalties such as a cease and desist order, or we may be required to make product changes, any of which could have an adverse effect on our business and financial results. We are subject to extensive tax liabilities, including federal and state and transactional taxes such as excise, sales / use, payroll, franchise, withholding, and ad valorem taxes. Changes in tax laws or their interpretations could increase our tax burden and decrease the amount of revenues we

receive, the value of any tax loss carryforwards and tax credits recorded on our balance sheet and the amount of our cash flow, and have a material adverse impact on our business, financial condition and results of operations. Some of our tax liabilities are subject to periodic audits by the respective taxing authority which could increase our tax liabilities. Furthermore, companies in the payment processing industry, including us, may become subject to incremental taxation in various tax jurisdictions. Taxing jurisdictions have not yet adopted uniform positions on this topic. If we are required to pay additional taxes and are unable to pass the tax expense through to our customers, our costs would increase and our net income would be reduced, which could have a material adverse effect on our business, financial condition and results of operations. In addition to those laws and regulations discussed previously that are imposed by the card networks and ~~NACHA~~ **Nacha**, governmental bodies in the United States have adopted, or are considering the adoption of, laws and regulations restricting the use, collection, storage, transfer and disposal of, and requiring safeguarding of, personal information. Our operations are subject to certain provisions of these laws. Relevant federal privacy laws include, in addition to FERPA ~~and~~, **PPRA and HIPAA** described above, the Gramm-Leach-Bliley Act of 1999, which applies directly to a broad range of financial institutions and indirectly, or in some instances directly, to companies that provide services to financial institutions. The U. S. Children’s Online Privacy Protection Act also regulates the collection of information by operators of websites and other electronic solutions that are directed to children under 13 years of age. These laws and regulations restrict the collection, processing, storage, use and disclosure of personal information, require notice to individuals of privacy practices and provide individuals with certain rights to prevent the use and disclosure of protected information. They also impose requirements for safeguarding and proper destruction of personal information through the issuance of data security standards or guidelines. In addition, there are state laws and regulations restricting the ability to collect and utilize certain types of information such as Social Security and driver’s license numbers. Certain states impose similar privacy obligations as well as obligations to provide notification of security breaches of computer databases that contain personal information to affected individuals, state officers and consumer reporting agencies and businesses and governmental agencies that own data. In connection with providing products and services to our customers, we are required by regulations, **applicable industry government-required** standards, and by our contracts with customers and ~~with our~~ financial institution distribution partners to provide assurances regarding the confidentiality and security of non-public consumer information. These contracts may require periodic audits by independent companies regarding our compliance with applicable standards. The compliance standards relate to the security of our infrastructure, ~~and include~~ **including** components and operational procedures designed to safeguard the confidentiality and security of individuals’ non-public personal information that our customers share with us. Our ability to maintain compliance with these standards and satisfy these audits will affect our ability to attract, grow and maintain business in the future. If we fail to comply with the laws and regulations relating to data privacy and information security, we could be exposed to legal claims and actions or to regulatory enforcement proceedings. In addition, our relationships and reputation could be harmed, which could inhibit our ability to retain existing customers and ~~distribution partners and~~ obtain new customers ~~and distribution partners~~. Legal requirements relating to the collection, storage, handling and transfer of personal data continue to evolve at both the federal and state level. For example, the CFPB ~~issued~~ **finalized** a ~~proposed~~ rule **which goes into effect January 17, 2025, that requires certain data providers to make covered data regarding covered financial products and services available to consumers and authorized third parties in an electronic form, subject to a number of requirements. Many states have introduced or passed comprehensive consumer privacy laws, including California, Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, Utah and Virginia, that may impose varying standards and requirements on our** ~~October 19, 2023, requiring depository and non-depository entities to make available to consumers data~~ **collection use** relating to consumer transactions, obligations for third accessing a consumer’s data and **processing activities** privacy protections for the data. **These** In June 2018, the State of California enacted the CCPA and subsequently enacted the CPRA. Together, the laws require companies (regardless of their location) that ~~collect~~ **process** personal information of California residents **of those states make certain disclosures** to notify consumers about **data practices, grant consumers specific rights to** their data collection, use, and **allow consumers to opt out of certain data** sharing practices, provide the ability to access and delete data to consumers and provide consumers the right to correct and limit the use and disclosure of sensitive personal information. In addition, several other states have introduced or passed similar legislation to the CCPA, including Nevada, Colorado, Virginia, Connecticut, Utah, Montana, Tennessee, Indiana, Iowa, Texas, Florida, Delaware and Oregon, that may impose varying standards and requirements on our data collection, use and processing activities. Additionally, the Federal Trade Commission and many state attorneys general are interpreting federal and state consumer protection laws to impose standards for the online collection, use, dissemination and security of data. Government regulators, industry groups and class action attorneys are increasingly scrutinizing how companies collect, process, use, store, share and transmit personal data. Regulators and courts may expand interpretations of existing laws, thereby further impacting our business. If more restrictive privacy laws or rules and / or inconsistent legal requirements are adopted by authorities in the future on the federal or state level, or regulators’ enforcement priorities shift, our compliance costs may increase and our ability to perform due diligence on, and monitor the risk of, our current and potential customers may decrease, which could create liability for us. **Many consumer privacy laws** ~~The CCPA and CPRA also~~ provide for civil penalties for violations, ~~as well as~~ **and the CCPA and CPRA provide for** a private right of action for data breaches that may increase data breach litigation. We may also be exposed to litigation, regulatory fines, penalties or other sanctions if the personal, confidential or proprietary information of our customers is mishandled or misused by any of our suppliers, counterparties or other third parties, or if such third- parties do not have appropriate controls in place to protect such personal, confidential or proprietary information. Further, many foreign data privacy regulations (including India’s Digital Personal Data Protection Act) can be more stringent than those in the United States. These laws and regulations are rapidly evolving and changing and could have an adverse effect on our operations. Our obligations and requirements under these laws and regulations

are subject to uncertainty in how they may be interpreted by government authorities and regulators. The costs of compliance with, and the other burdens imposed by, these and other laws or regulatory actions may increase our operational costs, affect our customers' willingness to permit us to use and store personal data, prevent us from selling our products or services, and / or affect our ability to invest in or jointly develop products. Failure to comply with these laws may result in governmental enforcement actions, private claims, including class action lawsuits, and damage to our reputation. We may also face audits or investigations by one or more domestic or foreign government agencies relating to our compliance with these regulations. Additionally, if we suffer a data breach, other privacy or cybersecurity regulatory compliance failures or are subject to fines, sanctions or proceedings as a result of actual or perceived compliance failures, or any similar event causing reputational harm, our opportunities for growth may be curtailed, and our potential liability for security breaches may increase, all of which could have a material adverse effect on our business, financial condition and results of operations. These laws and regulations may change rapidly, and it is frequently unclear how they apply to our business. Any failure of our products or services to comply with these laws and regulations could result in substantial civil or criminal liability and could, among other things, adversely affect demand for our services, invalidate all or portions of some of our contracts with our customers and financial institution partners, or require us to change or terminate some portions of our business. Further, reform efforts or changing healthcare regulatory requirements may also render our products or services obsolete or may block us from fully realizing or accomplishing our work or from developing new products or services. This may in turn impose additional costs upon us to adapt to the new operating environment or to further develop or modify our products and services. Such healthcare reforms may also make introduction of new products and service costlier or more time-consuming than we currently anticipate. These changes may also prevent our introduction of new products and services or make the continuation or maintenance of our existing products and services unprofitable or impossible. We no longer qualify as an "emerging growth company", and as a result, we have **been subject to** ~~comply with~~ increased disclosure and compliance requirements. We no longer qualify as an emerging growth company ("EGC") as defined in the Jumpstart Our Business Startups Act (the "JOBS Act"). As such, we are subject to certain disclosure and compliance requirements that apply to other public companies but did not previously apply to us due to our status as an EGC. These requirements include, but are not limited to: • the requirement that our independent registered public accounting firm attest to the effectiveness of our internal control over financial reporting under Section 404 (b) of the Sarbanes-Oxley Act of 2002; • compliance with any requirement that may be adopted by the PCAOB regarding mandatory audit firm rotation or a supplement to the auditor's report providing additional information about the audit and the financial statements, including critical audit matters; • the requirement that we provide full and more detailed disclosures regarding executive compensation; and • the requirement that we hold a non-binding advisory vote on executive compensation and obtain stockholder approval of any golden parachute payments not previously approved. ~~The~~ ~~We expect that the~~ ~~loss of EGC status and compliance~~ ~~will~~ ~~has increased and may continue to~~ increase our legal and financial compliance costs, and ~~may~~ cause management and other personnel to divert attention from operational and other business matters to devote substantial time to public company reporting requirements. The ~~increasing~~ **heightened** focus on environmental, social and governance ("ESG") practices could increase our costs, harm our reputation and adversely impact our financial results. There has been **heightened increasing public** focus by investors, customers, environmental activists, the media and governmental and nongovernmental organizations on a variety of ESG matters. If we are not effective in addressing ESG matters affecting our business our reputation may suffer. Moreover, we may experience increased costs in order to develop and execute upon any such ESG strategies, which could have an adverse impact on our business and financial condition. In addition, this emphasis on ESG matters has resulted and may result in the adoption of new laws and regulations, including new reporting requirements. If we fail to comply with new laws, regulations or reporting requirements, our reputation and business could be adversely impacted.

**Risks Related to Our Indebtedness** **Our indebtedness could adversely affect our financial health and competitive position.** On May 8, 2023, i3 Verticals, LLC (the "Borrower"), entered into that certain Credit Agreement (**as amended**, the "2023 Senior Secured Credit Facility") with the guarantors and lenders party thereto and JPMorgan Chase Bank, N. A., as administrative agent ("JPMorgan"). The 2023 Senior Secured Credit Facility replaces the Prior Senior Secured Credit Facility (as defined below). The 2023 Senior Secured Credit Facility provides for aggregate commitments of \$ 450 million in the form of a senior secured revolving credit facility (the "Revolver"). Borrowings under the Revolver will be made, at the Borrower's option, at the Adjusted Term SOFR rate or the base rate, plus, in each case, an applicable margin. The Adjusted Term SOFR rate will be the rate of interest per annum equal to the Term SOFR rate (based upon an interest period of one, three or six months), plus 0. 10 %, plus an applicable margin of 2. 00 % to 3. 00 % (~~3-2. 00 %~~ at September 30, ~~2023-2024~~). The Adjusted Term SOFR rate shall not be less than 0 % in any event. The base rate is a fluctuating rate of interest per annum equal to the highest of (a) the greater of the federal funds rate or the overnight bank funding rate, plus ½ of 1 %, (b) Wall Street Journal prime rate and (c) the Adjusted Term SOFR rate for an interest period of one month, plus 1 %, plus an applicable margin of 1. 00 % to 2. 00 % (2. 00 % at September 30, ~~2023-2024~~). The base rate shall not be less than 1 % in any event. As of September 30, ~~2023-2024~~, we had **no** borrowings outstanding of ~~\$ 272. 5 million~~ under the 2023 Senior Secured Credit Facility. Although we may enter into interest rate swap agreements in the future, we and our subsidiaries are exposed to interest rate increases on the floating portion of our 2023 Senior Secured Credit Facility that are not covered by interest rate swaps, to the extent we have indebtedness outstanding. For additional information about our 2023 Senior Secured Credit Facility, see "Management's Discussion and Analysis of Financial Condition and Results of Operations — Liquidity and Capital Resources" in Part II, Item 7 of this Annual Report on Form 10-K, and "Quantitative and Qualitative Disclosure About Market Risk" in Part II, Item 7A of this Annual Report on Form 10-K. On February 18, 2020, i3 Verticals, LLC issued \$ 138. 0 million aggregate principal amount of its Exchangeable Notes. The Exchangeable Notes bear interest at a fixed rate of 1. 0 % per year, payable semiannually in arrears on February 15 and August 15 of each year, beginning on August 15, 2020. ~~Prior to~~ **As of** August 15, 2024, the Exchangeable Notes **became** ~~are exchangeable only upon satisfaction of certain conditions and during certain periods~~

described in the Indenture, and thereafter, the Exchangeable Notes are exchangeable at any time until the close of business on the second scheduled trading day immediately preceding the maturity date. The Exchangeable Notes are exchangeable on the terms set forth in the Indenture into cash, shares of Class A common stock, or a combination thereof, at i3 Verticals, LLC's election, **provided that in September 2022, the Company made the irrevocable election to settle the principal portion of its Exchangeable Notes only in cash.** As of September 30, 2023-2024, \$ 117.26 . 02 million of the original aggregate principal amount of \$ 138. 0 million was outstanding. To service our debt and any additional debt we may incur in the future, we need to generate cash. Our ability to generate cash is subject, to a certain extent, to our ability to successfully execute our business strategy, including acquisition activity, as well as general economic, financial, competitive, regulatory and other factors beyond our control. Although we currently expect that our cash flow from operations, current cash and cash equivalents and available borrowing capacity under the 2023 Senior Secured Credit Facility will be sufficient to fund our operations and planned expenditures and to service our debt obligations for at least the next twelve months, there can be no assurance that our business will be able to generate sufficient cash flow from operations or that future borrowings or other financing will be available to us in an amount sufficient to enable us to service our debt and fund our other liquidity needs. To the extent we are required to use our cash flow from operations or the proceeds of any future financing to service our debt instead of funding working capital, capital expenditures, acquisition activity or other general corporate purposes, we will be less able to plan for, or react to, changes in our business, industry and in the economy generally. This will place us at a competitive disadvantage compared to our competitors that have less debt. There can be no assurance that we will be able to refinance any of our debt on commercially reasonable terms or at all, or that the terms of that debt will allow any of the above alternative measures or that these measures would satisfy our scheduled debt service obligations. If we are unable to generate sufficient cash flow to repay or refinance our debt on favorable terms, it could significantly adversely affect our financial condition and the value of our outstanding debt. Our ability to restructure or refinance our debt will depend on the condition of the capital markets and our financial condition. Any refinancing of our debt could be at higher interest rates and may require us to comply with more onerous covenants, which could further restrict our business operations. In addition, the 2023 Senior Secured Credit Facility contains, and any agreements evidencing or governing other future debt may contain, certain restrictive covenants that limit our ability, among other things, to engage in certain activities that are in our long- term best interests, including our ability to: • incur liens on property, assets or revenues; • incur or assume additional debt or amend our debt and other material agreements; • declare or make distributions and redeem or repurchase equity interests, **including making repurchases of Class A common stock pursuant to our share repurchase program,** or issue preferred stock; • prepay, redeem or repurchase debt; • make investments; • enter into any sale-and- leaseback of property; • engage in certain business activities; and • engage in mergers and asset sales. The restrictive covenants in our 2023 Senior Secured Credit Facility also require us to maintain specified financial ratios. While we have not previously breached and are not in breach of any of these covenants, there can be no guarantee that we will not breach these covenants in the future. Our ability to comply with any of these covenants and restrictions may be affected by events and factors beyond our control. Our failure to comply with any of these covenants or restrictions could result in an event of default under our 2023 Senior Secured Credit Facility. An event of default would permit the lending banks under the facility to take certain actions, including terminating all outstanding commitments and declaring all amounts outstanding under our 2023 Senior Secured Credit Facility to be immediately due and payable, including all outstanding borrowings, accrued and unpaid interest thereon, and all other amounts owing or payable with respect to such borrowings and any terminated commitments. In addition, the lenders would have the right to proceed against the collateral we granted to them, which includes substantially all of our assets. **We may not be able to secure additional financing on favorable terms, or at all, to meet our future capital needs.** In the future, we may require additional capital to respond to business opportunities, challenges, acquisitions or unforeseen circumstances, and may determine to engage in equity or debt financings or enter into credit facilities or refinance existing debt for other reasons. We may not be able to timely secure additional debt or equity financing on favorable terms, or at all. As discussed above, the 2023 Senior Secured Credit Facility contains restrictive covenants that limit our ability to incur additional debt and engage in other capital- raising activities. Any debt financing we obtain in the future could involve covenants that further restrict our capital raising activities and other financial and operational matters, which may make it more difficult for us to operate our business, obtain additional capital and pursue business opportunities, including potential acquisitions. Furthermore, if we raise additional funds by issuing equity or convertible debt or other equity- linked securities, our then- existing stockholders could suffer significant dilution. If we are unable to obtain adequate financing or financing on terms satisfactory to us, when we require it, our ability to continue to grow or support our business and to respond to business challenges could be significantly limited. **We may not have the ability to raise the funds necessary to settle exchanges of the Exchangeable Notes or to repurchase the Exchangeable Notes upon a fundamental change.** Holders of our Exchangeable Notes have the right to require us to repurchase their Exchangeable Notes upon the occurrence of a fundamental change at a repurchase price equal to 100 % of the principal amount of the Exchangeable Notes to be repurchased, plus accrued and unpaid interest, if any, to, but not including, the fundamental change repurchase date. In addition, unless we elect to deliver solely shares of Class A common stock to settle an exchange of the Exchangeable Notes, we will be required to make cash payments in respect of such Exchangeable Notes being exchanged. However, we may not have enough available cash or be able to obtain financing at the time we are required to make purchases of Exchangeable Notes surrendered therefor or Exchangeable Notes being exchanged. In addition, our ability to repurchase the Exchangeable Notes or to pay cash upon exchanges of the Exchangeable Notes is limited by the agreements governing our existing indebtedness (including the 2023 Senior Secured Credit Facility) and may also be limited by law, by regulatory authority or by agreements that will govern our future indebtedness. Our failure to repurchase Exchangeable Notes at a time when the repurchase is required by the indenture that governs the Exchangeable Notes or to pay cash payable on future exchanges of the Exchangeable Notes if and / or as required by the Indenture would constitute a default under the Indenture. A default under the Indenture or the fundamental change itself

could also lead to a default under the agreements governing our other indebtedness (including the 2023 Senior Secured Credit Facility) and agreements governing our future indebtedness. If the repayment of the related indebtedness were to be accelerated after any applicable notice or grace periods, we may not have sufficient funds to repay the indebtedness and repurchase the Exchangeable Notes or make cash payments upon exchanges thereof. ~~In the event the conditional exchange feature of the Exchangeable Notes is triggered, holders of Exchangeable Notes will be entitled to exchange the Exchangeable Notes at any time during specified periods at their option. If one or more holders elect to exchange their Exchangeable Notes, we may elect to settle all or a portion of our exchange obligation through the payment of cash, which could adversely affect our liquidity. In addition, even if holders do not elect to exchange their Exchangeable Notes, we could be required under applicable accounting rules to reclassify all or a portion of the outstanding principal of the notes as a current rather than long-term liability, which could result in a material reduction of our net working capital.~~ Risks Related to Our Organizational Structure and Our Company

We are a holding company with no operations of our own, and our principal asset is our controlling membership interest in i3 Verticals, LLC. Accordingly, we depend on distributions from i3 Verticals, LLC to pay our taxes and other expenses. We are a holding company with no operations of our own and currently have no significant assets other than our ownership of common units of i3 Verticals, LLC. We currently have no independent means of generating revenue. Consequently, our ability to obtain operating funds depends upon distributions from i3 Verticals, LLC. Furthermore, i3 Verticals, LLC is treated as a partnership for U. S. federal income tax purposes and, as such, is not itself subject to U. S. federal income tax. Instead, its net taxable income is generally allocated to its members, including us, pro rata according to the number of membership interests each member owns. Accordingly, we incur income taxes on our proportionate share of any net taxable income of i3 Verticals, LLC in addition to expenses related to our operations, and our ability to obtain funds to pay these income taxes currently depends upon distributions from i3 Verticals, LLC. We intend to cause i3 Verticals, LLC to distribute cash to us in an amount at least equal to the amount necessary to cover our respective tax liabilities, if any, with respect to our allocable share of the net income of i3 Verticals, LLC and to cover **cash dividends on our Class A common stock**, if any, we declare, **and purchases of Class A common stock pursuant to our share repurchase program**, as well as any payments due under the Tax Receivable Agreement (the “ Tax Receivable Agreement ” or “ TRA ”) by and among i3 Verticals, Inc., i3 Verticals, LLC and each of the holders, other than i3 Verticals, Inc., of common units in i3 Verticals, LLC (the “ Continuing Equity Owners ”). ~~See the detailed discussion under “ Management ’ s Discussion and Analysis of Financial Condition and Results of Operations — Liquidity and Capital Resources — 2023 Senior Secured Credit Facility ” in Part II, Item 7 of this Annual Report on Form 10-K for a discussion of the restrictive covenants, including i3 Verticals, LLC ’ s obligations to maintain specific financial ratios, that may limit its ability to make certain distributions to us.~~ To the extent that we need funds to pay our taxes or other liabilities or to fund our operations, and i3 Verticals, LLC is restricted from making distributions to us under applicable agreements under which it is bound, including its financing agreements, laws or regulations, does not have sufficient cash to make these distributions or is otherwise unable to provide such funds, we may have to borrow funds to meet these obligations and operate our business, and our liquidity and financial condition could be materially adversely affected. To the extent that we are unable to make payments under the Tax Receivable Agreement for any reason, such payments will be deferred and will accrue interest until paid. The interests of the other Continuing Equity Owners in our business may conflict with the interests of holders of shares of our Class A common stock. The Continuing Equity Owners, who collectively hold approximately 31 % of the combined voting power of our common stock as of November 21-22, 2023-2024, may receive payments from us under the Tax Receivable Agreement upon a redemption or exchange of their common units in i3 Verticals, LLC, including the issuance of shares of our Class A common stock upon any such redemption or exchange. As a result, the interests of the Continuing Equity Owners may conflict with the interests of holders of shares of our Class A common stock. For example, the Continuing Equity Owners may have different tax positions from us **in relation to** ~~which could influence their decisions regarding~~ whether and when **to we** dispose of assets, whether and when **to we** incur new or refinance existing indebtedness, and whether and when we should terminate the Tax Receivable Agreement and accelerate our obligations thereunder. ~~In addition, the structuring of future transactions may take into consideration tax or other considerations of the Continuing Equity Owners even in situations where no similar considerations are relevant to us.~~ We may not be able to realize all or a portion of the tax benefits that are expected to result from future redemptions or exchanges of common units by holders. Our organizational structure, including the Tax Receivable Agreement, confers certain benefits upon the Continuing Equity Owners that will not benefit the holders of our Class A common stock to the same extent as it will benefit the Continuing Equity Owners. Under the Tax Receivable Agreement, we are entitled to retain (a) 15 % of the U. S. federal and state income tax savings we realize as a result of increases in tax basis created by any future redemptions or exchanges of common units held by our equity holders that are parties to the Tax Receivable Agreement for shares of our Class A common stock or cash for the tax years following a redemption or exchange covered by the Tax Receivable Agreement, and (b) all of the U. S. federal and state income tax savings we realize from such redemptions or exchanges for tax periods ending after those covered by the Tax Receivable Agreement. Our ability to realize, and benefit from, these tax savings depends on several assumptions, including that we will earn sufficient taxable income each year during the period over which the deductions arising from any such basis increases and payments are available and that there are no adverse changes in applicable law or regulations. If our actual taxable income were insufficient or there were adverse changes in applicable law or regulations, we may be unable to realize all or a portion of these expected benefits, and our cash flows and stockholders’ equity could be negatively affected. The Tax Receivable Agreement provides that upon certain mergers, asset sales, other forms of business combinations or other changes of control or if, at any time, we elect an early termination of the Tax Receivable Agreement, then our obligations, or our successor’ s obligations, under the Tax Receivable Agreement to make payments thereunder would be based on certain assumptions, including an assumption that we would have sufficient taxable income to fully use all potential future tax benefits that are subject to the Tax Receivable Agreement. As a result of the foregoing, (a) we could be required to make payments under the Tax Receivable Agreement that are greater than the specified

percentage of the actual benefits we ultimately realize in respect of the tax benefits that are subject to the Tax Receivable Agreement and (b) if we elect to terminate the Tax Receivable Agreement early, we would be required to make an immediate cash payment equal to the present value of the anticipated future tax benefits that are the subject of the Tax Receivable Agreement, which payment may be made significantly in advance of the actual realization, if any, of such future tax benefits. In these situations, our obligations under the Tax Receivable Agreement could have a substantial negative impact on our liquidity and could have the effect of delaying, deferring or preventing certain mergers, asset sales, other forms of business combinations or other changes of control. There can be no assurance that we will be able to fund or finance our obligations under the Tax Receivable Agreement. In certain circumstances, i3 Verticals, LLC will be required to make distributions to us and the Continuing Equity Owners, and the distributions that i3 Verticals, LLC will be required to make may be substantial. Funds used by i3 Verticals, LLC to satisfy its tax distribution obligations ~~will~~ **may** not be available for reinvestment in our business.

**Moreover, in particular, in connection with the taxable income associated with the gain on the sale in September 2024 of our Merchant Services Business that is anticipated to be recognized for 2024 federal income tax distributions purposes by the members of i3 Verticals, LLC, a pass-through entity in which the Company held a 70.4% ownership interest as of September 30, 2024, we expect that i3 Verticals, LLC will be required under the terms of its limited liability company agreement to make ~~may be substantial, and will likely exceed (as a percentage tax distribution in the first half of 2025 to the members of i3 Verticals, LLC's net income), including i3 Verticals, Inc., the overall effective final amount of which tax distribution has not yet been determined~~ rate applicable to a similarly situated corporate taxpayer. As a result of potential differences in the amount of net taxable income allocable to us and to the Continuing Equity Owners, as well as the use of an assumed tax rate in calculating i3 Verticals, LLC's distribution obligations, we may receive distributions significantly in excess of our tax liabilities and obligations to make payments under the Tax Receivable Agreement. ~~To the extent, including in connection with the anticipated tax distribution to be made by i3 Verticals, LLC to its members, including the Company, in early 2025 as currently expected, we do not described above. Our Board of Directors will determine the appropriate uses for excess cash which is so held by the Company following tax distributions, which may include, among other uses, after giving effect to the payment of obligations under the Tax Receivable Agreement, the recontribution of such cash balances as to i3 Verticals, LLC for use in our business in exchange for common units of i3 Verticals, LLC along with an associated recapitalization of all of the outstanding common units in i3 Verticals, LLC, and / or the payment of a cash dividends- dividend on our Class A common stock. While our Board may choose to take any such actions, our Board is not required to do so, and instead to the extent, for example, hold such excess cash balances or lend continue to be held by them- the Company to i3 Verticals, LLC,~~ the Continuing Equity Owners would benefit from any value attributable to such accumulated cash balances as a result of their ownership of Class A common stock following a redemption or exchange of their common units. We are subject to a requirement, pursuant to Section 404 of the Sarbanes- Oxley Act of 2002 (the " Sarbanes- Oxley Act "), to conduct an annual review and evaluation of our internal control over financial reporting and furnish a report by management on, among other things, our assessment of the effectiveness of our internal control over financial reporting each fiscal year beginning with the year following our first annual report required to be filed with the SEC. Ensuring that we have adequate internal control over financial reporting in place so that we can produce accurate financial statements on a timely basis is a costly and time- consuming effort that must be evaluated frequently. Establishing and maintaining these internal controls is and will continue to be costly and may divert management' s attention. When evaluating our internal control over financial reporting, we may identify material weaknesses that we may not be able to remediate in time to meet the applicable deadline imposed upon us for compliance with the requirements of Section 404 of the Sarbanes- Oxley Act. In addition, if we fail to achieve and maintain the adequacy of our internal control over financial reporting, as such standards are modified, supplemented or amended from time to time, we may not be able to ensure that we can conclude, on an ongoing basis, that we have effective internal control over financial reporting in accordance with Section 404 of the Sarbanes- Oxley Act. We cannot be certain as to the timing of completion of our evaluation, testing and any remediation actions or the impact of the same on our operations. If we have not adequately implemented or complied with the requirements of Section 404 of the Sarbanes- Oxley Act, we may be subject to sanctions or investigation by regulatory authorities, such as the SEC, or suffer other adverse regulatory consequences, including penalties for violation of Nasdaq rules. As a result, there could be a negative reaction in the financial markets due to a loss of confidence in the reliability of our financial statements. A loss of confidence in the reliability of our financial statements also could occur if we or our independent registered public accounting firm were to report one or more material weaknesses in our internal control over financial reporting. In addition, we may be required to incur costs in improving our internal control system, including the costs of the hiring of additional personnel. Any such action could negatively affect our business, financial condition, results of operations and cash flows and could also lead to a decline in the price of our Class A common stock. Certain provisions of Delaware law and our amended and restated certificate of incorporation and amended and restated bylaws may have an anti- takeover effect and may delay, defer, or prevent a merger, acquisition, tender offer, takeover attempt, or other change of control transaction that a stockholder might consider in its best interest, including those attempts that might result in a premium over the market price for the shares held by our stockholders. These provisions provide for, among other things: • prohibiting the use of cumulative voting for the election of directors; • advance notice for nominations of directors by stockholders and for stockholders to include matters to be considered at our annual meetings; and • certain limitations on convening special stockholder meetings. In addition, while we have opted out of Section 203 of the Delaware General Corporation Law, or the " DGCL, " our amended and restated certificate of incorporation contains similar provisions providing that we may not engage in certain " business combinations " with any " interested stockholder " for a three- year period following the time that the stockholder became an interested stockholder, unless: • prior to such time, our board of directors ( " Board of Directors " ) approved either the business combination or the transaction that resulted in the stockholder becoming an interested stockholder; • upon consummation of the transaction that resulted in the stockholder becoming an interested**

stockholder, the interested stockholder owned at least 85 % of the votes of our voting stock outstanding at the time the transaction commenced, excluding certain shares; or • at or subsequent to that time, the business combination is approved by our Board of Directors and by the affirmative vote of holders of at least 66 2 / 3 % of the votes of our outstanding voting stock that is not owned by the interested stockholder. Generally, a “ business combination ” includes a merger, asset or stock sale or other transaction resulting in a financial benefit to the interested stockholder. Subject to certain exceptions, an “ interested stockholder ” is a person who, together with that person’ s affiliates and associates, owns, or within the previous three years owned, 15 % or more of the votes of our outstanding voting stock. For purposes of this provision, “ voting stock ” means any class or series of stock entitled to vote generally in the election of directors. Under certain circumstances, this provision will make it more difficult for a person who would be an “ interested stockholder ” to effect various business combinations with our company for a three- year period. This provision may encourage companies interested in acquiring our company to negotiate in advance with our Board of Directors because the stockholder approval requirement would be avoided if our Board of Directors approves either the business combination or the transaction that results in the stockholder becoming an interested stockholder. These provisions also may have the effect of preventing changes in our Board of Directors and may make it more difficult to accomplish transactions that stockholders may otherwise deem to be in their best interests. These provisions in our amended and restated certificate of incorporation and amended and restated bylaws may discourage, delay or prevent a transaction involving a change in control of our company that is in the best interest of our minority stockholders. Even in the absence of a takeover attempt, the existence of these provisions may adversely affect the prevailing market price of our Class A common stock if they are viewed as discouraging future takeover attempts. These provisions could also make it more difficult for stockholders to nominate directors for election to our Board of Directors and take other corporate actions. We may issue shares of preferred stock in the future, which could make it difficult for another company to acquire us or could otherwise adversely affect holders of our Class A common stock, which could depress the price of our Class A common stock. Our amended and restated certificate of incorporation authorizes us to issue one or more series of preferred stock. Our Board of Directors has the authority to determine the preferences, limitations and relative rights of the shares of preferred stock and to fix the number of shares constituting any series and the designation of such series, without any further vote or action by our stockholders. Our preferred stock can be issued with voting, liquidation, dividend and other rights superior to the rights of our Class A common stock. The potential issuance of preferred stock may delay or prevent a change in control of us, discourage bids for our Class A common stock at a premium to the market price, and materially and adversely affect the market price and the voting and other rights of the holders of our Class A common stock.

#### Risks Related to Ownership of Our Class A Common Stock

The Continuing Equity Owners own common units in i3 Verticals, LLC, and the Continuing Equity Owners have the right to redeem their common units in i3 Verticals, LLC pursuant to the terms of the limited liability company agreement of i3 Verticals, LLC (the " LLC Agreement") for shares of Class A common stock or cash. As of September 30, 2023-2024, we have an aggregate of 126, 746 117, 728-965 shares of Class A common stock authorized but unissued, including 10, 093-032, 394-676 shares of Class A common stock issuable, at our election, upon redemption of common units of i3 Verticals, LLC that are held by the Continuing Equity Owners. Subject to certain restrictions contained in the LLC Agreement, the Continuing Equity Owners are entitled to have their common units redeemed from time to time at each of their options (subject in certain circumstances to time- based and service- based vesting requirements and other limitations) for newly- issued shares of our Class A common stock on a one- for- one basis or a cash payment equal to a volume weighted average market price of one share of Class A common stock for each Common Unit redeemed, in each case, in accordance with the terms of the LLC Agreement. At our election, however, we may effect a direct exchange by i3 Verticals, Inc. of such Class A common stock or such cash, as applicable, for such common units in lieu of redemption. The Continuing Equity Owners may exercise such redemption right for as long as their common units remain outstanding. We have also entered into a Registration Rights Agreement pursuant to which the shares of Class A common stock issued to certain Continuing Equity Owners upon such redemption and the shares of Class A common stock issued to certain Continuing Equity Owners in connection with the Reorganization Transactions will be eligible for resale registration, subject to certain limitations set forth in the Registration Rights Agreement. We cannot predict the size of future issuances of our Class A common stock or the effect, if any, that future issuances and sales of shares of our Class A common stock may have on the market price of our Class A common stock. Sales or distributions of substantial amounts of our Class A common stock, including shares issued in connection with an acquisition, or the perception that such sales or distributions could occur, may cause the market price of our Class A common stock to decline. Holders of our Class A common stock may be diluted by future issuances of preferred stock or additional Class A common stock or common units in connection with our incentive plans, acquisitions or otherwise; future sales of such shares in the public market, or the expectations that such sales may occur, could lower our stock price. Our amended and restated certificate of incorporation authorizes us to issue shares of our Class A common stock and options, rights, warrants and appreciation rights relating to our Class A common stock for the consideration and on the terms and conditions established by our Board of Directors in its sole discretion. We could issue a significant number of shares of Class A common stock in the future in connection with investments or acquisitions. Any of these issuances could dilute our existing stockholders, and such dilution could be significant. Moreover, such dilution could have a material adverse effect on the market price for the shares of our Class A common stock. The future issuance of shares of preferred stock with voting rights may adversely affect the voting power of the holders of shares of our Class A common stock, either by diluting the voting power of our Class A common stock if the preferred stock votes together with the common stock as a single class, or by giving the holders of any such preferred stock the right to block an action on which they have a separate class vote, even if the action were approved by the holders of our shares of our Class A common stock. The future issuance of shares of preferred stock with dividend or conversion rights, liquidation preferences or other economic terms favorable to the holders of preferred stock could adversely affect the market price for our Class A common stock by making an investment in the Class A common stock less attractive. For example, investors in the Class A common stock may not wish to purchase Class A

common stock at a price above the conversion price of a series of convertible preferred stock because the holders of the preferred stock would effectively be entitled to purchase Class A common stock at the lower conversion price, causing economic dilution to the holders of Class A common stock. Sales of shares of our Class A common stock in connection with the Registration Rights Agreement, or the prospect of any such sales, could materially affect the market price of our Class A common stock and could impair our ability to raise capital through future sales of equity securities. In connection with the completion of our IPO, we entered into a Registration Rights Agreement with certain Continuing Equity Owners. Any sales in connection with the Registration Rights Agreement, or the prospect of any such sales, could materially and adversely impact the market price of our Class A common stock and could impair our ability to raise capital through future sales of equity securities. In the future, we may also issue additional securities if we need to raise capital, including, but not limited to, in connection with acquisitions, which could constitute a material portion of our then- outstanding shares of Class A common stock.