

Risk Factors Comparison 2023-08-24 to 2022-08-25 Form: 10-K

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

The Company's business and the results of its operations are affected by numerous factors and uncertainties, some of which are beyond our control. The following is a description of some of the important risks and uncertainties that may cause our actual results of operations in future periods to differ materially from those expected or desired. Business and Operating Risks Data security breaches, failures, or other incidents could damage our reputation and business. Our business relies upon receiving, processing, storing, and transmitting sensitive information relating to our operations, employees, and customers. If we fail to maintain a sufficient digital security infrastructure, address security vulnerabilities and new threats, or deploy adequate technologies to secure our systems against attack, we may be subject to security breaches that compromise confidential information, adversely affect our ability to operate our business, damage our reputation and business, adversely affect our results of operations and financial condition, and expose us to liability. We rely on ~~industry-standard encryption, network, and Internet security systems, most of which we license from third parties~~ **for various business purposes, and to provide the these third parties face similar** security risks and authentication necessary to effect secure transmission of data and to prevent ~~unauthorized access to our computer networks, systems, and data~~. A security failure by one of these third parties could expose our **data or subject our** information systems to interruption of operations and security vulnerabilities. ~~We also use third-party vendors to store and process data for us and they face similar risks~~. Our services and infrastructure are increasingly reliant on the ~~Internet~~ **internet**. Computer networks and the Internet are vulnerable to ~~unauthorized access, computer viruses and other~~ disruptive problems such as denial of service attacks or other cyber-attacks carried out by cyber criminals or state-sponsored actors. Other potential attacks include attempts to obtain unauthorized access to confidential information or destroy data, often through the introduction of computer viruses, ransomware or malware, cyber-attacks, and other means, which are constantly evolving and **at times** difficult to detect. ~~Although none of these types of attacks have had a material effect on our business or operations to date, we anticipate that attempts to attack our systems, services, and infrastructure, and those of our customers and vendors, may grow in frequency and sophistication~~. Those same parties may also attempt to fraudulently induce employees, customers, vendors, or other users of our systems through phishing schemes or other **social engineering** methods to disclose sensitive information in order to gain access to our data or that of our customers ~~or clients~~. We are also subject to the risk that our employees may intercept and transmit unauthorized confidential or proprietary information or that employee corporate-owned computers are stolen, or customer data media is lost in shipment. An interception, misuse or mishandling of personal, confidential, or proprietary information being sent to or received from a customer or third party could result in legal liability, remediation costs, regulatory action, and reputational harm, any of which could adversely affect our results of operations and financial condition. **We anticipate that attempts** Under state, federal, and foreign laws requiring consumer notification of security breaches, the costs to **attack** remediate security breaches can be substantial. ~~Although we believe our security controls systems, services, and infrastructure are adequate to protect our systems and data, we~~ **and those of our customers and vendors, may grow in frequency and sophistication. We** cannot be certain that ~~these our security controls and infrastructure will be adequate to continue to protect our systems and data and our~~ **efforts will may not** be sufficient to combat all current and future technological risks and threats. Advances in computer capabilities, new discoveries in the field of cryptography, or other events or developments may render our security measures inadequate. Security risks may result in liability to our customers or other third parties, damage to our reputation, and may deter financial institutions from purchasing our products. The significant amount of capital and other resources we currently expend to protect against the threat of security breaches may prove insufficient to prevent a breach. We cannot ensure that any limitation-of-liability provisions in our customer and user agreements, contracts with third-party vendors, or other contracts are sufficient to protect us from liabilities or damages with respect to claims relating to a security breach or similar matters. The insurance coverage we maintain to address data security risks may be insufficient to cover all types of claims or losses that may arise, and there is no assurance that such insurance coverage will continue to be available to us on economically reasonable terms, or at all. In the event of a security breach, we may need to spend substantial additional capital and resources alleviating problems caused by such breach. **Under state, federal, and foreign laws requiring consumer notification of security breaches, the costs to remediate security breaches can be substantial.** Addressing security problems may result in interruptions, delays, or cessation of service to users, any of which could harm our business. Failure to maintain sufficient technological infrastructure or an operational failure in our outsourcing facilities could expose us to damage claims, increase regulatory scrutiny, and cause us to lose customers. Our products and services require substantial investments in technological infrastructure, and we have experienced significant growth in the number of users, transactions, and data that our technological infrastructure supports. If we fail to adequately invest in and support our technological infrastructure and processing capacity, we may not be able to support our customers' processing needs and may be more susceptible to interruptions and delays in services. Damage or destruction that interrupts our outsourcing operations could cause delays and failures in customer processing which could hurt our relationship with customers, damage our reputation, expose us to damage claims, and cause us to incur substantial additional expense to relocate operations and repair or replace damaged equipment. Events that could cause operational failures include, but are not limited to, hardware and software defects, breakdowns or malfunctions, cybersecurity incidents, human error, power losses, disruptions in telecommunications services, computer viruses or other malware, or other events. Our facilities are also subject to physical risks related to natural disasters or severe weather events, such as tornados, flooding, hurricanes, and heat waves. Climate change may increase the likelihood and severity of such events. Our back-up systems and procedures may prove insufficient or otherwise fail to prevent

disruption, such as a prolonged interruption of our transaction processing services. If an interruption extends for more than several hours, we may experience data loss or a reduction in revenues by reason of such interruption. Any significant interruption of service could reduce revenue, have a negative impact on our reputation, result in damage claims, lead our present and potential customers to choose other service providers, and lead to increased regulatory scrutiny of the critical services we provide to financial institutions, with resulting increases in compliance burdens and costs. Implementing modifications and upgrades to our technological infrastructure subject us to inherent costs and risks associated with changing systems, policies, procedures, and monitoring tools. Failures associated with payment transactions could result in financial loss. The volume and dollar amount of payment transactions that we process is significant and continues to grow. We direct the settlement of funds on behalf of financial institutions, other businesses, and consumers, and receive funds from clients, card issuers, payment networks, and consumers on a daily basis for a variety of transaction types. Transactions facilitated by us include debit card, credit card, electronic bill payment transactions, Automated Clearing House (“ACH”) payments, real-time payments through faster payment networks (such as Zelle, RTP, and FedNow), and check clearing that support consumers, financial institutions, and other businesses. If the continuity of operations, integrity of processing, or ability to detect or prevent fraudulent payments were compromised in connection with payments transactions, we could suffer financial as well as reputational loss. In addition, we rely on various third parties to process transactions and provide services in support of the processing of transactions and funds settlement for certain of our products and services that we cannot provide ourselves. If we are unable to obtain such services in the future or if the price of such services becomes unsustainable, our business, financial position, and results of operations could be materially and adversely affected. In addition, we may issue short-term credit to consumers, financial institutions, or other businesses as part of the funds settlement process. A default on this credit by a counterparty could result in a financial loss to us. Failures of third-party service providers we rely upon could lead to financial loss. We rely on third-party service providers to support key portions of our operations. We also rely on third-party service providers to provide part, or all of, certain services we deliver to customers. As we continue to move more computing, storage, and processing services out of our data centers and facilities and into third-party hosting environments, our reliance on these providers and their systems will increase. **This reliance is further concentrated as we use certain third-party vendors to provide large portions of our hosting needs.** While we have selected these third-party vendors carefully, we do not control their actions. A failure of these services by a third party could have a material impact upon our delivery of services to our customers. Such a failure could lead to damage claims, loss of customers, and reputational harm, depending on the duration and severity of the failure. Third parties perform significant operational services on our behalf. These third-party vendors are subject to similar risks as us including, but not limited to, compliance with applicable laws and regulations, hardware and software defects, breakdowns or malfunctions, cybersecurity incidents, human error, **failures in internal controls,** power losses, disruptions in telecommunications services, computer viruses or other malware, natural disasters or severe weather events, or other events. One or more of our vendors may experience a cybersecurity event or operational disruption and, if any such event does occur, it may not be adequately addressed, either operationally or financially, by the third-party vendor. Certain of our vendors may have limited indemnification obligations or may not have the financial capacity to satisfy their indemnification obligations. If a critical vendor is unable to meet our needs in a timely manner or if the services or products provided by such a vendor are terminated or otherwise delayed and if we are not able to develop alternative sources for these services and products quickly and cost-effectively, our customers could be negatively impacted, and it could have a material adverse effect on our business. Competition may result in decreased demand or require price reductions or other concessions to customers, which could result in lower margins and reduce income. We vigorously compete with a variety of software vendors and service providers in all of our major product lines. We compete on the basis of product quality, reliability, performance, ease of use, quality of support and services, integration with other products, and pricing. Some of our competitors may have advantages over us due to their size, product lines, greater marketing resources, or exclusive intellectual property rights. New competitors regularly appear with new products, services, and technology for financial institutions. If competitors offer more favorable pricing, payment or other contractual terms, warranties, or functionality, or otherwise attract our customers or prevent us from capturing new customers, we may need to lower prices or offer other terms that negatively impact our results of operations in order to successfully compete. Failure to achieve favorable renewals of service contracts could negatively affect our business. Our contracts with our customers for outsourced data processing and electronic payment transaction processing services generally run for a period of seven or more years. We will continue to experience a significant number of these contracts coming up for renewal each year. Renewal time presents our customers with the opportunity to consider other providers or to renegotiate their contracts with us, including reducing the services we provide or negotiating the prices paid for our services. If we are not successful in achieving high renewal rates upon favorable terms, revenues and profit margins will suffer. We may experience increased costs for services from our third-party vendors due to inflation or other cost expansion, but because our customer contracts typically have longer terms than our vendor contracts, our ability to pass on those higher costs to customers may be limited. If inflation or costs outpace our contractual ability to adjust pricing during the contractual terms of our customer contracts, our revenues and profit margins could be negatively impacted. If we fail to adapt our products and services to changes in technology and the markets we serve, we could lose existing customers and be unable to attract new business. The markets for our products and services are characterized by changing customer and regulatory requirements and rapid technological changes. These factors and new product introductions by our existing competitors or by new market entrants could reduce the demand for our existing products and services, and we may be required to develop or acquire new products and services. Our future success is dependent on our ability to enhance our existing products and services in a timely manner and to develop or acquire new products and services. If we are unable to develop or acquire new products and services as planned, or if we fail to sell our new or enhanced products and services, we may incur unanticipated expenses or fail to achieve anticipated revenues, as well as lose prospective sales. Software defects or problems with installations may harm our business and reputation and expose us to potential liability. Our software products are

complex and may contain undetected defects, especially in connection with newly released products and software updates. Software defects may cause interruptions or delays to our services as we attempt to correct the problem. We may also experience difficulties in installing or integrating our products on systems used by our customers. Defects in our software, installation problems or delays, or other difficulties could result in negative publicity, loss of revenues, loss of competitive position, or claims against us by customers. In addition, we rely on technologies and software supplied by third parties that may also contain undetected errors or defects that could have a negative effect on our business and results of operations. Expansion of services to non-traditional customers could expose us to new risks. We have expanded our services to business lines that are marketed outside our traditional, regulated, and litigation-averse base of financial institution customers. These non-regulated customers may entail greater operational, credit, and litigation risks than we have faced before and could result in increases in bad debts and litigation costs.

Regulatory and Compliance Risks The software and services we provide to our customers are subject to government regulation that could hinder the development of our business, increase costs, or impose constraints on the way we conduct our operations. The financial services industry is subject to extensive and complex federal and state regulation. As a supplier of software and services to financial institutions, portions of our operations are examined by the Office of the Comptroller of the Currency, the Federal Reserve Board, the Federal Deposit Insurance Corporation, the Consumer Financial Protection Bureau, and the National Credit Union Association, among other regulatory agencies. These agencies regulate services we provide and the way we operate, and we are required to comply with a broad range of applicable federal and state laws and regulations. If we, or third parties with whom we contract or partner, fail to comply with applicable regulations or guidelines, we could be subject to regulatory actions and suffer harm to our customer relationships and reputation. Such failures could require significant expenditures to correct and could negatively affect our ability to retain customers and obtain new customers. In addition, existing laws, regulations, and policies could be amended or interpreted differently by regulators in a manner that imposes additional costs and has a negative impact on our existing operations or that limits our future growth or expansion. New regulations could require additional programming or other costly changes in our processes or personnel. Our customers are also regulated entities, and actions by regulatory authorities could influence both the decisions they make concerning the purchase of data processing and other services and the timing and implementation of these decisions. We will be required to apply substantial research and development and other corporate resources to adapt our products to this evolving, complex, and often unpredictable regulatory environment. Our failure to provide compliant solutions could result in significant fines or consumer liability on our customers, for which we may bear ultimate liability. Compliance with new and existing privacy laws, regulations, and rules may adversely impact our expenses, development, and strategy. We are subject to complex laws, rules, and regulations related to data privacy and cybersecurity. If we fail to comply with such requirements, we could be subject to reputational harm, regulatory enforcement, and litigation. The use, confidentiality, and security of private customer information is under increased scrutiny. Regulatory agencies, Congress, and state legislatures are considering numerous regulatory and statutory proposals to protect the interests of consumers and to require compliance with standards and policies that have not been defined.

The number of state privacy and cybersecurity laws and regulations has grown tremendously over the past several years, creating an increasingly complex patchwork of data privacy and security requirements. This includes industry-specific rules such as those enacted by the New York Department of Financial Services that require covered financial institutions to have a cybersecurity program along with other compliance requirements and as well as comprehensive consumer data privacy rules such as the California Consumer Privacy Act, the Iowa Consumer Data Protection Act, and the Virginia Consumer Data Protection Act. **Though several privacy concepts are common across the laws, each state requires compliance with standards and policies that are not cohesive with other laws and are often further amended by regulatory action.** The unique data protection regulations issued by multiple agencies have created a fragmented series of requirements that makes it increasingly complex to comply with all the mandates in an efficient manner and may increase costs to deliver affected products and services as those requirements are established. Failure to comply or readily address compliance and regulatory rule changes made by payment card networks could adversely affect our business. We are subject to card association and network compliance rules governing the payment networks we serve, including Visa, MasterCard, Zelle, FedNow, and The Clearing House's RTP network, and all rules governing the Payment Card Data Security Standards. If we fail to comply with these rules and standards, we could be fined or our certifications could be suspended or terminated, which could limit our ability to service our customers and result in reductions in revenues and increased costs of operations. Changes made by the networks, even when complied with, may result in reduction in revenues and increased costs of operations.

Economic Conditions Risks **A natural disasters, public health crises, wars, acts of terrorism, other armed conflict, and workforce shortages could adversely affect our results of operations. The occurrence of, or threat of, natural disasters,** widespread public health ~~erisis~~ ~~crises~~ could adversely affect our results of operations. ~~The widespread outbreak of a communicable illness or disease,~~ **political unrest such as the COVID-19 outbreak, or war, acts of terrorism, other public health crises armed conflicts involving the United States or foreign countries, or general workforce shortages including government mandates in response to such events,** can result in significant economic disruptions and uncertainties and could adversely affect our business, results of operation, and financial condition. The conditions caused by such events may affect the rate of spending by our customers and their ability to pay for our products and services, delay prospective customers' purchasing decisions, interfere with our employees' ability to support our business function, disrupt the ability of third-party providers we rely upon to deliver services, adversely impact our ability to provide on-site services or installations to our customers, or reduce the number of transactions we process, all of which could adversely affect our results of operation and financial position. We are unable to accurately predict the impact of such events on our business due to a number of uncertainties, including the duration, severity, geographic reach and governmental responses to such events, the impact on our customers' and vendors' operations, and our ability to provide products and services, including the impact of our employees working remotely. If we are not able to respond to and manage the impact of such events effectively, our business will be harmed. Our business may be adversely impacted by

general U. S. and global market and economic conditions or specific conditions in the financial services industry. We derive most of our revenue from products and services we provide to the financial services industry. If the general economic environment worsens, **including if inflation or interest rates continue to increase or remain at higher than recent historical levels**, or if conditions or regulatory requirements within the financial services industry change, such as if financial institutions are required to increase reserve amounts **or become subject to new regulatory assessments**, customers may be less willing or able to pay the cost of our products and services, and we could face a reduction in demand from current and potential clients for our products and services, which could have a material adverse effect on our business, results of operations, and financial condition. In addition, a growing portion of our revenue is derived from transaction processing fees, which depend heavily on levels of consumer and business spending. Deterioration in general economic conditions could negatively impact consumer confidence and spending, resulting in reduced transaction volumes and our related revenues. Consolidation and failures of financial institutions will continue to reduce the number of our customers and potential customers. Our primary market consists of approximately 4, **790-660** commercial and savings banks and more than **5-4, 000-850** credit unions. The number of commercial banks and credit unions in the United States has experienced a steady decrease over recent decades due to mergers and acquisitions and financial failures and we expect this trend to continue as more consolidation occurs. Such events may reduce the number of our current and potential customers, which could negatively impact our results of operations.

Acquisition Risks Our growth may be affected if we are unable to find or complete suitable acquisitions. We have augmented the growth of our business with a number of acquisitions and we plan to continue to acquire appropriate businesses, products, and services. This strategy depends on our ability to identify, negotiate, and finance suitable acquisitions. Merger and acquisition activity in our industry has affected the availability and pricing of such acquisitions. If we are unable to acquire suitable acquisition candidates, we may experience slower growth. Acquisitions subject us to risks and may be costly and difficult to integrate. **On August 5, 2022, we entered into an Agreement and Plan of Merger to acquire 100% of the equity interests of Payrailz, LLC, which offers digital payment capabilities, including real-time person-to-person ("P2P") payments. The acquisition is anticipated to close on August 31, 2022, subject to the satisfaction of customary closing conditions.** Acquisitions, ~~including the Payrailz acquisition,~~ are difficult to evaluate, and our due diligence may not identify all potential liabilities or valuation issues. We may also be subject to risks related to cybersecurity incidents or vulnerabilities of the acquired company and the acquired systems. We may not be able to successfully integrate ~~Payrailz or any other~~ acquired companies. We may encounter problems with the integration of new businesses, including: financial control and computer system compatibility; unanticipated costs and liabilities; unanticipated quality or customer problems with acquired products or services; differing regulatory and industry standards; diversion of management's attention; adverse effects on existing business relationships with suppliers and customers; loss of key employees; and significant depreciation and amortization expenses related to acquired assets. To finance ~~the Payrailz acquisition or other~~ future acquisitions, we may have to increase our borrowing or sell equity or debt securities to the public. If we fail to integrate our acquisitions, our business, financial condition, and results of operations could be materially and adversely affected. Failed acquisitions could also produce material and unpredictable impairment charges as we review our acquired assets.

Intellectual Property Risks If others claim that we have infringed their intellectual property rights, we could be liable for significant damages or could be required to change our processes. We have agreed to indemnify many of our customers against claims that our products and services infringe on the proprietary rights of others. We also use certain open source software in our products, which may subject us to suits by persons claiming ownership of what we believe to be open source software. Infringement claims have been and will in the future be asserted with regard to our software solutions and services. Such claims, whether with or without merit, are time-consuming, may result in costly litigation and may not be resolved on terms favorable to us. If our defense of such claims is not successful, we could be forced to pay damages or could be subject to injunctions that would cause us to cease making or selling certain applications or force us to redesign applications. Our failure to protect our intellectual property and proprietary rights may adversely affect our competitive position. Our success and ability to compete depend in part upon protecting our proprietary systems and technology. Unauthorized parties may attempt to copy or access systems or technology that we consider proprietary. We actively take steps to protect our intellectual property and proprietary rights, including entering into agreements with users of our services for that purpose and maintaining security measures. However, these steps may be inadequate to prevent misappropriation. Policing unauthorized use of our proprietary rights is difficult and misappropriation or litigation relating to such matters could have a material negative effect on our results of operation.

General Risk Factors A material weakness in our internal controls could have a material adverse effect on us. Effective internal controls are necessary for us to provide reasonable assurance with respect to our financial reports and to mitigate risk of fraud. If material weaknesses in our internal controls are discovered or occur in the future, our consolidated financial statements may contain material misstatements and we could be required to restate our financial results, which could materially and adversely affect our business and results of operations or financial condition, restrict our ability to access the capital markets, require us to expend significant resources to correct the weaknesses or deficiencies, subject us to fines, penalties or judgments, harm our reputation, or otherwise cause a decline in investor confidence. The loss of key employees and difficulties in hiring and retaining employees could adversely affect our business. We depend on the contributions and abilities of our senior management and other key employees. Our Company has grown significantly in recent years and our management remains concentrated in a small number of highly qualified individuals. If we lose one or more of our key employees, we could suffer a loss of managerial experience, and management resources would have to be diverted from other activities to compensate for this loss. We do not have employment agreements with any of our executive officers. Further, we **are facing an increasingly continue to face a** competitive market for hiring and retaining skilled employees, ~~which is exacerbated by the effects of the COVID-19 pandemic and increased acceptance of hiring remote working employees by our competitors and other companies.~~ Difficulties in hiring and retaining skilled employees may restrict our ability to adequately support our business needs and / or result in increased personnel costs. There is no assurance that we will be able to attract and

retain the personnel necessary to maintain the Company' s strategic direction . **Unfavorable future tax law changes could adversely affect our tax expense. Our income tax positions result in a significant net deferred income tax liability on our consolidated balance sheet. Unfavorable future tax law changes, including increasing U. S. corporate tax rates, could increase this net liability and negatively impact our provision for income taxes and net income** . The impairment of a significant portion of our goodwill and intangible assets would adversely affect our results of operations. Our balance sheet includes goodwill and intangible assets that represent a significant portion of our total assets ~~at as of~~ June 30, ~~2022~~ **2023** . On an annual basis, and whenever circumstances require, we review our goodwill and intangible assets for impairment. If the carrying value of a material asset is determined to be impaired, it will be written down to fair value by a charge to operating earnings. An impairment of a significant portion of our goodwill or intangible assets could have a material negative effect on our operating results. An increase in interest rates could increase our borrowing costs. Although our debt borrowing levels have historically been low, we may require additional or increased borrowings in the future under existing or new debt facilities to support operations, finance acquisitions, or fund stock repurchases. Our current ~~revolving credit facility facilities~~ **bears bear** interest at ~~a~~ **variable rate rates** . Increases in interest rates on variable- rate debt would increase our interest expense, which could negatively impact our results of operations. **19**