ransom demands to not expose security vulnerabilities in our systems or the systems of third parties, or other security breaches, and could result in the destruction or exfiltration of data and systems. As cyber threats continue to evolve, we may be required to expend significant additional resources to continue to modify or enhance its protective measures or to investigate and remediate any information security vulnerabilities or incidents. Despite efforts to ensure the integrity of our systems and implement controls, processes, policies and other protective measures, we may not be able to anticipate all security breaches, nor may we be able to implement guaranteed preventive measures against such security breaches. Cyber threats are rapidly evolving and we may not be able to anticipate or prevent all such attacks and could be held liable for any security breach or loss.

Although we have programs in place related to business continuity, disaster recovery and information security to maintain the confidentiality, integrity, and availability of our systems, business applications and customer information, we, like other financial services firms, have been and continue to be the subject of cyberattacks. Such cyberattacks may result in interruptions in service to customers and loss or liability to us, including losses related to misuse of customer data that has been the subject of unauthorized disclosure. Although we do not believe any of such events have resulted in any material losses or other material consequences to date, there can be no guarantee that such losses or consequences will not occur in the future. In addition, future cyberattacks could be more disruptive and damaging, and we may not be able to anticipate or prevent all such attacks. Further, future cyberattacks may not be detected in a timely manner.

Cyberattacks or other information or security breaches, whether directed at us or third parties, may result in a material loss or have material consequences. In the event of cyberattacks impacting our transportation payments business (i.e., Factoring and TriumphPay), such attacks may result in payment diversions or other events that could cause us financial loss, which could be material given the payment volumes of such businesses. Furthermore, the public perception that a cyberattack on our systems has been successful, whether or not this perception is correct, may damage our reputation with customers and third parties with whom it does business. Hacking of personal information and identity theft risks, in particular, could cause serious reputational harm. A successful penetration or circumvention of system security could cause us serious negative consequences, including loss of customers and business opportunities, costs associated with maintaining business relationships after an attack or breach; significant business disruption to our operations and business, misappropriation, exposure, or destruction of its confidential information, intellectual property, funds, and/or those of its customers; or damage to our, our customers' and/or third parties' computers or systems, and could result in a violation of applicable privacy laws and other laws, litigation exposure, regulatory fines, penalties or intervention, loss of confidence in our security measures, reputational damage, reimbursement or other compensatory costs, additional compliance costs, and could adversely impact our results of operations, liquidity and financial condition. In addition, we may not have adequate insurance coverage to compensate for losses from a cybersecurity event.

We primarily rely on Amazon Web Services to deliver our services to customers on our Payments and Factoring platforms, and any disruption of or interference with our use of Amazon Web Services could adversely affect our business, financial condition, and results of operations.

We currently host our Payments and Factoring platforms and support our operations in multiple data centers provided by Amazon Web Services, or AWS, a third-party provider of cloud infrastructure services. We do not have control over the operations of the facilities of AWS that we use. AWS' facilities could be subject to damage or interruption from natural disasters, cybersecurity attacks, terrorist attacks, power outages, and similar events or acts of misconduct. The occurrence of any of the above circumstances or events and the resulting impact on our platform may harm our reputation and brand, reduce the availability or usage of our platform, lead to a significant short-term loss of revenue, increase our costs, and impair our ability to retain existing customers or attract new customers, any of which could adversely affect our business, financial condition, and results of operations.