sellers' businesses. We also obtain sensitive information regarding our sellers' customers, including their contact information, payment card numbers and expiration dates, and purchase histories. We

have administrative, technical, and physical security measures in place, and have policies and procedures in place to contractually require third parties to whom we transfer data to implement and maintain appropriate security measures. However, if our security measures or those of the previously mentioned third parties are inadequate or are breached as a result of third-party action, employee error, malfeasance, malware, phishing, hacking attacks, system error, trickery, or otherwise, and, as a result, someone obtains unauthorized access to sensitive information, including personally identifiable information, on our systems or our partners' systems, our reputation and business could be damaged. If the sensitive information is lost or improperly disclosed or threatened to be disclosed, we could incur significant liability and be subject to regulatory scrutiny and penalties, including costs associated with remediating the breach. Under payment card rules and our contracts with our card processors, if there is a breach of payment card information that we store or that is stored by our sellers or other third parties with which we do business, we could be liable to the payment card issuing banks for their cost of issuing new cards and other related expenses. Additionally, if our own confidential business information were improperly disclosed, our business could be materially and adversely affected. A core aspect of our business is the reliability and security of our payments platform. Any perceived or actual breach of security could have a significant impact on our reputation as a trusted brand, cause us to lose existing sellers, prevent us from obtaining new sellers, require us to expend significant funds to remedy problems caused by breaches and to implement measures to prevent further breaches, and expose us to legal risk and potential liability. Any security breach at a company providing services to us, our sellers, or other users of our services could have similar effects.

Our risk management efforts may not be effective, which could expose us to losses and liability and otherwise harm our business.

We offer payments services and other products and services to a large number of customers, and we are responsible for vetting and monitoring these customers and determining whether the transactions we process for them are legitimate. When our products and services are used to process illegitimate transactions, and we settle those funds to sellers and are unable to recover them, we suffer losses and liability. These types of illegitimate transactions can also expose us to governmental and regulatory sanctions. The highly automated nature of, and liquidity offered by, our payments services make us a target for illegal or improper uses, including fraudulent or illegal sales of goods or services, money laundering, and terrorist financing. Identity thieves and those committing fraud using stolen or fabricated credit card or bank account numbers, or other deceptive or malicious practices, potentially can steal significant amounts of money from businesses like ours. In configuring our payments services, we face an inherent trade-off between security and customer convenience. Our risk management policies, procedures, techniques, and processes may not be sufficient to identify all of the risks to which we are exposed, to enable us to mitigate the risks we have identified, or to identify additional risks to which we may become subject in the future. As a greater number of larger sellers use our services, our exposure to material risk losses from a single seller, or from a small number of sellers, will increase. For example, in the three months ended March 31, 2015, we recorded a loss of approximately $5.7 million related to fraud by a single seller using our payments services. In addition, when we introduce new services, focus on new business types, or begin to operate in markets where we have a limited history of fraud loss, we may be less able to forecast and reserve accurately for those losses. Furthermore, if our risk management policies and processes contain errors or are otherwise ineffective, we may suffer large financial losses, we may be subject to civil and criminal liability, and our business may be materially and adversely affected.

We are currently, and will continue to be, exposed to risks associated with chargebacks and refunds in connection with payment card fraud or relating to the goods or services provided by our sellers. In the event that a billing dispute between a cardholder and a seller is not resolved in favor of the seller, including in situations where the seller engaged in

fraud, the transaction is typically "charged back" to the seller and the purchase price is credited or otherwise refunded to the cardholder. If we are unable to collect chargeback or refunds from the seller's account, or if the seller refuses to or is unable to reimburse us for a chargeback or refunds due to closure, bankruptcy, or other reasons, we may bear the loss for the amounts paid to the cardholder. Beginning October 2015, businesses that cannot process EMV chip cards are held financially responsible for