or when the client's business has significant volume changes. They may also reduce services if they decide to move services in-house. Further, our SMB clients may exert pricing pressure due to pricing competition or other economic needs or pressures such clients experience from their customers. On some occasions, this pricing pressure results in lower revenue from a client than we had anticipated based on our previous agreement with that client. This reduction in revenue could result in an adverse effect on our business, operating results, and financial condition.

For potential clients of our Global Business Solutions and Global Financial Solutions segments, switching from one vendor of core processing or related software and services (or from an internally-developed system) to a new vendor is a significant undertaking. As a result, potential clients often resist change. We seek to overcome this resistance through strategies such as making investments to enhance the functionality of our software. However, there can be no assurance that our strategies for overcoming potential clients' reluctance to change vendors will be successful, and this resistance may adversely affect our growth.

Security breaches or attacks on our systems may have a significant effect on our business.

In order to provide our services, we process, store, and transmit sensitive business information and personal consumer information, including, but not limited to, names, bankcard numbers, home or business addresses, Social Security numbers, driver's license numbers, and bank account numbers. Under the card network rules and various federal and state laws, we are responsible for information provided to us by merchants, ISOs, third-party service providers, and other agents. The confidentiality of such sensitive business information and personal consumer information that resides on our systems is critical to our business because we require such information to approve merchant accounts, process transactions, and protect against fraud. We cannot be certain that the security measures and procedures we have in place to protect this sensitive data will be successful or sufficient to counter all current and emerging technology threats designed to breach our systems in order to gain access to confidential information. The increasing sophistication of cyber criminals may increase the risk of a security breach of our systems. A breach of our products or systems processing or storing sensitive business information or personal consumer information could lead to claims against us, reputational damage, loss of our financial institution sponsorship, loss of clients' and their customers' confidence, as well as imposition of fines and damages, or potential restrictions imposed by card networks on our ability to process transactions, all of which could have a material adverse effect on our revenues, profitability, financial condition, and future growth. In addition, as security threats continue to evolve we may be required to invest additional resources to modify the security of our systems, which could have a material adverse effect on our results of operations.

We may experience breakdowns in our processing systems that could damage client relations and expose us to liability.

Our core business depends heavily on the reliability of our processing systems. A system outage could have a material adverse effect on our business, financial condition, and results of operations. Not only would we suffer damage to our reputation in the event of a system outage, but we may also be liable to third parties. Many of our contractual agreements with financial institutions require us to pay penalties if our systems do not meet certain operating standards. To successfully operate our business, we must be able to protect our processing and other systems from interruption, including from events that may be beyond our control. Events that could cause system interruptions include, but are not limited to, fire, natural disaster, unauthorized entry, power loss, telecommunications failure, computer viruses, terrorist acts, and war. Although we have taken steps to protect against data loss and system failures, there is still risk that we may lose critical data or experience system failures. To help protect against these events, we perform the vast majority of disaster recovery operations ourselves, but we also utilize select third parties for certain operations, particularly outside of the United States. To the extent we outsource our disaster recovery, we are at risk of the vendor's unresponsiveness or other failures in the event of breakdowns in our systems. In addition, our property and business interruption insurance may not be adequate to compensate us for all losses or failures that may occur.