>>>FAIRVIEW FLASH REPORT<<<
SEC Enforcement Action for Failure to Protect Customer Data

WHAT HAPPENED?	Last week, the Securities Exchange Commission ("SEC") responded to Morgan Stanley's failure to prevent a customer data breach. From 2011 to 2014, a then-employee transferred confidential customer information to his personal server. The employee's personal server was then hacked by a third party, who downloaded and attempted to sell the customer information.
WHAT WERE THE ISSUES?	Morgan Stanley had comprehensive policies and procedures regarding cybersecurity, including authorization modules intended to restrict access to data. However, they failed to test the proper operation of such programs. Therefore, Morgan Stanley employees were able to access data beyond their legitimate business needs. The information could then be transferred without authorization or any monitoring of portal usage.
WHAT WAS THE SETTLEMENT?	Morgan Stanley settled the charges for violation of the "Safeguards Rule" (Rule 30(a) of Regulations S-P) and agreed to: • Pay a $1 million penalty. The employee was criminally convicted and received: • 36 months of probation; and • A $600,000 restitution order.
TAKEAWAY	"Given the dangers and impact of cyber breaches, data security is a critically important aspect of investor protection. We expect SEC registrants of all sizes to have policies and procedures that are reasonably designed to protect customer information," said Andrew Ceresney, Director of the SEC Enforcement Division. The large-scale data breach of customer information indicates the need for thorough cybersecurity policies that are actively enforced. These policies should be kept up-to-date and reviewed for potential weaknesses. For advisers using Sharefile, Dropbox, and similar programs, we recommend monitoring usage periodically. We will support our registered advisers' efforts to ensure that they have implemented a formidable data security program and are regularly auditing its performance.

Sources: SEC Article; SEC Order