COSMOS
Navigate the Compliance Universe

Report on Supply Chain Compliance Volume 2, Number 15. August 15, 2019
Recent data breaches have compliance professionals asking, 'What can I do better?'

By Sascha Matuszak

The recently reported Capital One Financial Corporation data breach involves similar cloud computing vulnerabilities discussed in *RSCC's* July 18 article, "The risk of a data breach to your supply chain is real … and so are the solutions," namely "S3 buckets," components of Amazon Web Services (AWS). The Capital One data breach was carried out by a former insider, who had also worked for AWS systems in the past and, according to court documents, was able to take advantage of a misconfiguration of Capital One's cloud database to gain credentials that allowed access to the personal data of more than 100 million individuals.

Capital One released a statement, including the following:

> We encrypt our data as a standard. In addition, it is our practice to tokenize select sensitive data fields, most notably Social Insurance Numbers and credit card account numbers. Tokenization involves the substitution of the sensitive field with a cryptographically generated replacement. The method and keys to unlock the tokenized fields are different from those used to encrypt the data. Due to the particular circumstances of this incident, the unauthorized access also enabled the decrypting of the data.

According to Mark Lanterman, chief technology officer of Computer Forensic Services, the breach had little to do with encryption issues: