ECKERT SEAMANS ATTORNEYS AT LAW

December 20, 2022

Data Security& Privacy Update

Joint Cybersecurity Advisory issued by FBI, FDA OCI, and USDA Warns Food & Agriculture Sector About Increase in Business Email Compromise Scams to Divert Shipments of Food Products

By Matthew H. Meade, Esq. and Emma M. Lombard, Esq.

On December 16, 2022, the Federal Bureau of Investigation (FBI), the Food and Drug Administration Office of Criminal Investigations (FDA OCI), and the U.S. Department of Agriculture (USDA) released a Joint Cybersecurity Advisory to warn the Food & Agriculture sector about recently observed incidents of criminal actors using business email compromise (BEC) scams to divert shipments of food products and ingredients in order to steal them. The advisory highlights several incidents this year involving shipments of sugar, powdered milk, and non-fat dry milk, in which the cyber criminals posed as individuals or organizations to scam the sector.

BEC scams or attacks are one of many ways that cyber criminals exploit businesses to effectuate fraudulent money transfers, to purchase products, or to acquire data held by the company and exchanged through email. To do this, criminals may gain access to an employee's business email account through fraudulent means or may use an email address that closely resembles a valid employee email address. They then impersonate the employee while sending fraudulent emails to banks, vendors, or other employees. Unfortunately, these emails often appear to recipients as valid, authorized requests. In this instance, the Joint Cybersecurity Advisory warns that criminals are using BEC scams to fraudulently order food products, which are fulfilled by the victim company and shipped to the criminals without payment. Often, businesses may not realize they have been the victim of a BEC until the company that shipped the goods reaches out for payment.

To protect against BECs, businesses should implement multi-factor authentication (MFA) on all business email accounts, increase password complexity requirements, and require employees to frequently update their passwords. In addition, it is important to train employees on how to identify fraudulent email addresses and domains and how to guard against phishing emails. Businesses should also conduct web searches for their company name to identify whether any fraudulent websites exist that may be used by criminals to impersonate the company through a scam. The Joint Cybersecurity Advisory highly recommends independent verification of contact information provided by vendors or customers through reputable online sources like associations or business directories as well as to pay close attention to the verified company name and branding. For example, a scammer's email may reference "Acme Baking, Inc." instead of "The Acme Baking Company" and contain an off-color or pixelated logo which mimics the original.

ECKERT SEAMANS ATTORNEYS AT LAW

This Data Security & Privacy Alert is intended to keep readers current on developments in the law, and is not intended to be legal advice. If you have any questions, please contact Matthew H. Meade at 412.566.6983 or mmeade@eckertseamans.com, Emma M. Lombard at 609.989.5024 or elombard@eckertseamans.com, or any other attorney at Eckert Seamans with whom you have been working.