GLOBAL SECURITY

SAFE.SURE.SECURE.

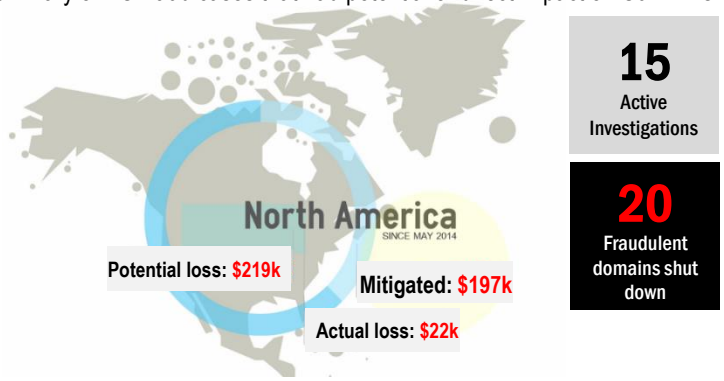
PURCHASE ORDER SCAM PREVENTION

Over the last few months, scammers have used Cummins public information, which is posted on the company's domain, to generate PO requests for various supplies. Using email as the primary method of communication, scammers will attempt to get a quote for our products. Once the quote is delivered, the scammers will either develop a PO, or forge an existing one, and request to have the products shipped to a specific location. Below is a list of unique identifiers that will help you determine if a PO request is fraudulent:

- Initial contact begins with an email claiming to be Cummins employee
- A purchase order accompanies the email
- The purchase order has a Cummins logo at the header
- Numerous spelling and grammatical errors in the email such as: incorrect phone numbers, business names and addresses
- The majority of the emails originate outside the U.S.
- The impersonator may also send a list of legitimate references who conduct business with Cummins

HAS PO FRAUD IMPACTED CUMMINS?

Over 250 companies and universities across the United States have experienced similar cases of fraud schemes go back to late 2010. Like Cummins, many of these private institutions have fraudulent domains shut down; however new variations are established. Since May 2014, Cummins has lost an estimated $22,000 to PO fraud. Although this number might seem trivial, the total amount of potential loss exceeds $219,000. The image below provides a high level summary of PO fraud cases that had potential or direct impact on Cummins.



To address this issue, Global Security partners with key stakeholders to create awareness by introducing cautionary measures and best practices to Cummins employees and suppliers. In doing so, Cummins has been able to identify and shut down more than 20 fraudulent domains and prevented $197,000 worth of PO fraud.

WHAT YOU NEED TO KNOW

- Employees and suppliers should exercise caution and report all suspicious calls or emails immediately.
- Cummins Global Security does not learn about scams until we are contacted by the company/vendor who is being targeted.
- You should educate your staff about these scams so they can alert our customers. Due diligence is the key-*Know your customer.*
- If a website is associated with the fraudulent purchase order, Global Security has the ability to shut those sites down.
- Encourage targeted companies to report the crimes to the Internet Crime Complaint Center at IC3.gov.

WHO SHOULD I CONTACT?

Report security incidents to the Cummins Response Center (CRC): If you receive or have received a call or email from an individual that you suspect is fraudulent, report the incident to the **CRC:**

- **Email:** CRC@cummins.com
- **Phone: U.S. 866-685-4313 / Intl +1 443-221-4877**

REMINDER

- Make sure all purchase orders and invoices are numbered consecutively, and regularly checked for inconsistencies.
- Match all purchase orders against your invoices before processing.
- Do not respond to suspicious or unfamiliar emails or phone calls.