

TO: Notice to Vendors DATE: May 5, 2023

FROM: Alexandre De Moraes Zanelatto, EVP Global Supply Chain  
Kerry McGinnis, Senior Legal Counsel & Privacy Officer  
Catherine Mendonsa, CISO, Director Information Systems Security

SUBJECT: **Spotting & Preventing Fraudulent RFQs & Purchase Orders**

---

Business Email Compromise (BEC) attacks are one of the most financially damaging cybercrimes and such attacks have been on the rise over the last few years. We understand that supply chain and finance departments around the world are receiving spoofed emails from fake accounts and/or websites placing fraudulent equipment orders or submitting false invoices. Finning continuously monitors for this activity and has identified that fake Finning-like domains have been created by 'bad actors' such as Finning-Inc.com, and FinningInc.com. When we are notified of new sites, we immediately report them to Domain Name Registrars and subsequently have them disabled.

In an effort to create greater supply-chain awareness and mitigate potential risk of this fraudulent activity, we remind our vendors to exercise caution and follow Finning's established purchasing guidelines when receiving and/or reviewing RFQs from the company. Finning will not be responsible for orders that are not placed in accordance with our purchasing guidelines.

#### **Tips to Identify Fraudulent RFQs**

The following are some flags to assist you with identifying fraudulent RFQs:

- **Fax Only.** Finning would not ask you to respond to our RFQs by fax only.
- **Addresses.** We have clearly set out our regions and addresses on Finning.com. We would not ask you to send goods to an address not listed on Finning.com.
- **Executive Names.** The contact names on the documents have been from Finning executive members. Our RFQ's or Purchase Orders would normally include the contact information of one of our procurement employees, not the name of or contact information for one of our executives.
- **Finning.com.** Finning's email addresses will only come from "finning.com", email addresses from any other domain (such as "finning-canada", "finninginc" or "finning-inc") are fraudulent.

#### **What You Can Do**

- **Remain Vigilant.** We urge you to remain vigilant against fraud, and to regularly review orders that you receive from Finning. If you receive any orders or delivery instructions that fall outside the normal course of dealings with Finning, please contact us as noted below.
  - **Careful Review.** We encourage you to carefully review the RFQs that you receive from us using the tips we have outlined above.
  - **Validate Contact Information.** Prior to responding to a RFQ, we would urge you to verify the contact information set out in the RFQ by checking it against your records or by contacting us.
  - **Contact the CAFC.** To report fraud, please contact the Canadian Anti-Fraud Center at <http://www.antifraudcentre-centreantifraude.ca/> or by calling 1-888-495-8501.
- Be Proactive.** We urge you to educate your employees about fraud so that they can assist you with spotting red flags.

#### **For More Information**

If you have questions or need additional information about the foregoing, please contact a member of our supplier enablement team. Contact details are set out below:

Caelan Snow, Global Director Category Management  
csnow@finning.com

Yvonne Milinkovic, Contracts Manager  
ymilinkovic@finning.com