CYBER RISKS IN INTERNATIONAL BUSINESS:
Tips and Pointers for International Sales

1. Act quickly when you notice or are alerted to any suspect activity (reports of scraped website, reports of spoofed internal emails, or spoofed emails from your customers or distributors). This includes but is not limited to notifying your insurer and determining whether coverage exists.

2. If you stop an initial fraud attempt it usually does not deter the fraudulent actors. You should assume and act as though you are now under attack. Depending on the circumstances, your communications (especially email) may be monitored by the perpetrators.

3. In light of the nature of international trade, it may be weeks before you learn that you or your customers/distributors have been defrauded.

4. First order of priority is to ensure that the fraud is stopped. Alert your customers (and/or your internal team) and contain damage. Contact IT specialists and/or law enforcement as necessary. Due to 3. above, the fraudsters have a running start.

5. Moving swiftly is to your advantage so you can alert customers to advise their banks (or advise your bank) the payment was fraudulent and identify and track movement of funds. It is possible to recover funds if customers alert their banks (or you alert your bank) quickly and act quickly to follow/track where your funds went and attempt to stop further transfers.

6. You are likely to be sued by a customer who received fraudulent diverted payment instructions, so as you follow the steps above keep in mind you are also building evidence for a court/arbitrator. Involve an outside IT consultant and legal counsel early to build your case as you follow the above steps.

7. Document and retain all notices to customers and communications from and to them regarding suspicious activity or cyber risks. Legal counsel should review your correspondence before it is sent.

8. Review your internal payment and payment instruction procedures and your Terms and Conditions of Sale to ensure appropriate checks and confirmations are required. Seek a company strategy that attempts to maintain a customer relationship while putting the company in the best position to defend against claims.

9. Carefully vet and perform vigorous due diligence on foreign business partners/customers/distributors/agents.

10. Educate yourself on advance payment schemes. They are on the rise from purported foreign customers and purported foreign agents or distributors wishing to represent your company and sell your product overseas. See https://www.fbi.gov/scams-and-safety/common-fraud-schemes/advance-fee-schemes. More information on types of business email compromise schemes can be found in the FBI Public Service Announcements. See https://www.ic3.gov/media/2016/160602.aspx

FOSTER SWIFT
FOSTER SWIFT COLLINS & SMITH PC | ATTORNEYS

LANSING | SOUTHFIELD | GRAND RAPIDS | DETROIT | HOLLAND | ST. JOSEPH

Contact Information for International Trade Practice

Jean G. Schtokal	**John W. Mashni**	**Zachary W. Behler**	**Taylor A. Gast**
517.371.8276	517.371.8257	517.371.8323	517.371.8238
jschtokal@fosterswift.com	jmashni@fosterswift.com	zbehler@fosterswift.com	tgast@fosterswift.com

For more information visit: **fosterswift.com**