Three Key Credit Fraud Threats and Preventive Steps

A 2013 fraud study conducted in conjunction with LexisNexis and Javelin Strategy & Research reported that the "true cost of fraud" to victim merchants is rising, as are the types and sophisticated nature of the scams. The study noted that the true cost to a business in 2012 exceeded $2.70 for every $1 of fraud, which is up 40 cents from the previous year.

Within that framework, fraud prevention should continue to be of paramount concern to credit departments. The following are among helpful steps to prevent getting burned for a big-dollar loss:

International Dangers
Selling internationally is becoming more of a necessity as domestic demand is no longer enough to sustain many industries. However, LexisNexis and Javelin Strategy & Research noted that companies conducting international business are targeted five times more often than those that stay domestic. The success rate is four times higher as well. The FBI notes that external fraud attempts often come in the form of individuals posing as a potential customers or investors as a means to gain access to technical information that could compromise a company, and warns that weak online security is tantamount to "an invitation to hackers." Making a commitment to better online security is helpful and necessary, as is being generally more cautious with international contacts. Also of note is that the majority of fraudulent attempts originate from several areas of the world, led by West Africa and former members of the Soviet Union in Eastern Europe.

Evolution
Fraud schemes constantly evolve and are often much more complex than the email from a Nigerian prince pleading to transfer money into your account, which he would then share with you. In reality, many fraudsters have gotten significantly more proficient at avoiding prior red flags like poor language syntax in correspondence for attempts originating outside U.S. borders. Additionally, many have moved away from using email addresses unrelated to specific businesses (i.e., @hotmail.com or @att.net) because of increased awareness that they are red flags. Newer schemes involve the shipment of orders. Fraudsters use addresses that are hard to confirm as legitimate, such as near expansive government complexes, or where there is the possibility for more confusion or low security, such as college campuses where it's easy to intercept a package "mistakenly" delivered to the wrong department. One key combat strategy, aside from the usual need to be diligent, is ensuring the credit and sales staff is educated and trained on a recurring basis so they are up to date on the trends, and therefore more likely to detect a scheme.

Don't Be Fooled by a Good Website
If investigating an order from a company that is changing activity drastically, or becoming active after a long dormant period, don't be convinced by a professional-looking website. Source code copying is becoming increasingly prevalent. Present-day fraudsters readily copy legitimate business' website coding and use it to set up a visually identical website to give the appearance of legitimacy. One telltale difference might be in the URL, which may use ".us" instead of ".com." In addition, checking out the security and encryption software a site uses, as well as the incorporation date of the customer, are helpful ways to establish whether the customer's website really is legit.