Socially Engineered Shipping Scheme Hits Jewelry Industry

JUNE 27, 2017
Source: National Jeweler

New York--A group of perpetrators are calling jewelry companies and faking their identities in order to trick them into shipping out high-end items, the Jewelers Security Alliance said in a special alert issued late last week.

JSA President John J. Kennedy said that while the exact number of perpetrators is unknown, the shipping scam is the work one of one fairly large singular group believed to be operating in the United States and targeting jewelry firms in the Northeast and Southeast.

He said that both suppliers and retailers are potential victims, with the perpetrators using what's called social engineering to try to fool their victims into shipping out high-end merchandise.

Social engineering is defined as the use of deception to manipulate individuals to divulge confidential or personal information that may be used for fraudulent purposes. In May of this year, the FBI released a public service announcement about social engineering being used in business email compromise attacks, which cost businesses globally more than $5 billion between October 2013 and December 2016.

But, electronic contact is not part of the current scam that's impacting jewelers and suppliers, Kennedy said.

Instead, the perpetrators are using the phone, calling suppliers pretending to be jewelers, or targeting multi-store retail chains posing as a store manager or employee of another branch.

They will contact the retail store or supplier with a great deal of knowledge about the company, like names of employees, shipping procedures, inventory in stock and SKU numbers.

While some of the information is obtained via phone calls made prior, much is mined from the internet, including the store's website and the social media profiles of the business owner and his or her employees.

Then the perpetrator will ask for the supplier or store to ship certain high-end items--Kennedy said mainly large diamonds and high-value watches--overnight, with the goal of diverting the package en route by changing the shipping address to an address of their choice.

Sometimes when the fraud is being committed at a multi-store retail chain, the perpetrator will give an address that he or she claims belongs to a customer or salesperson and asks for the item to be sent there instead of the store.

Kennedy said while he has seen this type of fraud before, he has never seen it happening at the level it is right now.

There have been about a dozen attempts in the last two weeks alone. And those are just the ones that were reported to the JSA, he said, though he noted that only a few of the reported attempts have been successful.

"We are putting this out now because we see it as rampant," Kennedy said of the alert the JSA issued Friday.

He said that the amount of information now available on the internet is a "very large" contributor to criminals' ability to socially engineer scams today.
And while Kennedy acknowledges that businesses need to be present on the internet to market themselves today, he says jewelers should carefully consider each piece of information that goes online.

"I feel jewelers are putting far too much information out online," he said. "The more you put out there, the more you are at risk."

The JSA has five additional recommendations for jewelers and suppliers to help them avoid becoming a victim

of this shipping scheme.

1) Employees need to confirm to whom they are speaking. If someone is on the line whom the employee does not know, he or she should excuse themselves immediately and say they will have to call them back. Employees also can call back after the order or request is made to confirm that it's legitimate.

Either way, the employee should not use the number given to them by the caller and, instead, call the actual phone number of the business, obtained via Google or elsewhere.

2) Be wary of calls that come from blocked or "unknown" numbers.

3) Alert employees that they should not be fooled into giving out inappropriate information to callers asking questions about personnel or procedures. The perpetrators want to find out as much as they can about a supplier or retailer in order to sound legitimate.

4) Strictly limit the procedures that allow for a change of address on shipments. For example, some firms have only one person who can authorize a change of address or have told the shipping company that all packages on which an address change is attempted should be returned to them.

5) Kennedy also recommended Monday that jewelers or suppliers never give out tracking numbers for packages they are shipping.