Shining a light on the shady dealings of con artists

by Julie Maager

From high tech to low tech, from simple to sophisticated, from misleading you into overspending on products to outright stealing your money, scammers are out there and your restaurant could be a target.

Wisconsin Restaurant Association frequently warns its members when a new scam rears its head or an old one resurfaces. Staying ahead of the swindlers requires staying on your toes and there is no better way to do that than with information.

High tech theft

Con artistry is nothing new, but the tools scammers use are constantly evolving. Exploiting delays in banking transactions is one way scammers have devised of separating people from their money faster than a three-card Monte operator.

Two forms of this scam have been hitting the restaurant industry lately: the foreign reservation scam and the relay operator scam.

Reservation scam: One frequently attempted scam involves approaching restaurants and hotels via e-mail to request a reservation for a large group of people from a foreign country. The scammer will pre-pay to hold the reservation and then cancel, asking for their money to be refunded. The hitch is that their pre-payment to you has been made with forged checks or stolen credit cards; while that transaction is pending (and you believe you have the money in your account), you issue the refund. A short time later, the initial payment to your business is refused and you are out the money you sent as a “refund.”

How to spot the scam: Have reservations about large, foreign reservations! Often the initial e-mail will appear legitimate, but be wary. Tip offs that you are being targeted by a scam artist: the e-mail has poor or strange grammar or random capitalization; the writer tries to impress you with a fancy title; the sender is overly eager to assure you that the payment method is legitimate; or your business is not referred to by name, only as “your restaurant” or “establishment.”

Relay operator scam: The relay operator scam works in a similar way—the scammer makes a fraudulent prepayment for a reservation, large catering order, or to-go order and then asks for a refund—but there is an additional twist: it exploits the telephone relay service used by people who are hearing impaired.

Relay service—which has been around for decades—allows deaf and hard of hearing callers to type messages to an operator who then reads it to the hearing person on the other end of the

continued on page 22
call. In the past, users needed a special text telephone to use the service. Now the internet and text messaging devices make it easy for anyone to use the service—including con artists.

Joanne Palzkill, owner of Draganteeti’s Ristorante in Altoona and the new Taverna Grill in Eau Claire, was immediately suspicious when a very odd catering order came into Draganteeti’s from a “customer” using relay service.

“My sister took the call. She was gone awhile and came back saying, ‘You won’t believe the phone call I just got,’” Palzkill recalled. The order was for 300 sandwiches, potato salad and coleslaw—not, as Palzkill said, “food you’d order from a typical Italian restaurant.” Even odder was the caller’s apparent disinterest in the food itself: “People do not order for 300 and not care what they’re getting,” Palzkill said.

Although suspicious, Palzkill responded the next day to the email address that was given to her sister. She got an immediate reply to her email saying an “intermediary” would come pick up the food. The immediacy of the response, the odd phrasing of the reply and the disinterest in the food itself sealed it for Palzkill and she dismissed the whole order as a scam attempt.

Previous to receiving the relay call, Palzkill had heard about the scam from the Wisconsin Restaurant Association and had printed out copies of the WRA Alert and put them at both of her restaurant’s phones. However, it still took her by surprise, she said, as she thought big metro areas would be the target of the scammers. “I couldn’t believe it—right here in Wisconsin!” she said.

How to spot the scam: Be wary of callers ordering very large to-go orders, customers who show little interest in the food being ordered, people who want to use a third party delivery service, or callers who want to split orders between several credit cards. Like the reservation scam, many of these ploys also originate in foreign countries and odd or overly formal phrasing is typical. All of these may be signs you are the target of a scam.

**Capitalizing on current events**

While technology has proven a fruitful tool for con artists, capitalizing on current events has been another rich resource for scrammers. Two scams that have recently targeted restaurant owners play off the H1N1 flu (sometimes incorrectly called swine flu) scare and the Economic Stimulus Act for credibility.

**H1N1 flu (swine flu) kit:** The National Restaurant Association has passed on reports of restaurant operators targeted by companies selling “swine flu kits.” A restaurant employee in Indiana took a call from someone who said the kit was required to meet Department of Homeland Security requirements. However, the caller couldn’t give specifics on the kit that he wanted to sell for nearly $400.

How to spot the scam: Much like the workplace poster and OSHA first aid kit scams covered later in this article, this scam relies on scaring business owners with regulation requirements that are distorted or—in this case, outright phony—in order to sell a product. No such “swine flu kit” requirement exists. Check with WRA or another reliable source before spending money on a product you may not need.

**SBA scam:** In February, the U.S. Small Business Administration issued a scam alert regarding letters being

---

**Extreme scam: One restaurant’s experience**

While no business owner wants to get “taken” on any level, Bob Doller surely would have preferred to pay for some overpriced handwashing posters instead of the experience he and his wife, Jessica, suffered in 2008: a stomach-turning case of food tampering, an extortion attempt, and publicity that reached national levels.

In April 2008, a professionally-dressed woman came to the Dollers’ upscale Appleton restaurant, The Seasons, for lunch. After eating three quarters of her dish, the woman called over her server, Doller said. On her fork was a portion of a cooked rat.

“She got up and made a scene and went to the bathroom as if she were sick,” Doller said. “It was like time had stopped. I’m thinking, ‘Did it come in the tomatoes? Did it come in the pasta?’” he said.

Thoroughly shaken, the Dollers exchanged phone numbers with the woman and told her to go to the hospital. On the advice of WRA, they also called in the health department for an exhaustive inspection, trying to find how a rat could have possibly gotten into their food. Meanwhile, visions of losing their livelihood ran through both their minds.

“My wife freaked out,” Doller said. “She said ‘She’s going to the media. We’re going out of business.’”

Over the next few days, the Dollers exchanged phone calls with the woman who told stories of a two-day hospital stay and blood transfusions. The Dollers called in their attorney and insurance company. When the woman refused to release her medical records to the insurance company, suspicions grew. Finally, after a number of exchanges, the woman called and left a message with the insurance agent demanding $500,000 or she would go to the press with her story.

While the insurance company continued their investigation, Doller and his wife watched their business drop off and answered hushed questions from friends and customers who had heard the rumors around town. Eventually, after about three months, the full story came out: the insurance company determined the rat was actually a white lab rat that had been cooked in a microwave (The Seasons doesn’t use microwaves in its cooking) and the woman was charged with criminal extortion.

The last chapter of this story isn’t written, as the woman has been in mental evaluations and has yet to go to trial. Doller says their business has never completely recovered. The whole experience has been stressful and eye opening, he says.

“There are some people out there—very, very few I’m sure—but they will do anything,” he said.
sent out on what appeared to be SBA letterhead. The letters told business owners that they may be eligible for a tax rebate under the Economic Stimulus Act and the SBA was assessing their eligibility. The letter asked the business to provide the name of its bank and account number.

How to spot the scam: Be very suspicious of any unsolicited correspondence—via mail or e-mail—that asks for your bank account information. This is what is known as “phishing” when it is done via e-mail; it’s an attempt by criminals, posing as a legitimate business/organization, to obtain your financial or personal information. In the case of this scam, there is no such “rebate program” being administered by the SBA.

Misleading advertising, overpriced products

While some scammers are taking advantage of current events, other ploys targeting the restaurant industry could almost be termed “perennial favorites,” they have come up so often. Many of these involve misleading restaurant owners into buying overpriced posters or other items in order to comply with regulations that have been distorted by the company selling the product.

Kate Reiser, WRA’s Member Communications Coordinator, has taken numerous WRA hotline calls from members on these products over the years. The scam operators “apparently think business owners are so busy that any time they see the word ‘compliance’ they’ll write a check,” Reiser said.

Handwashing posters: Companies selling grossly overpriced handwashing posters have sent direct mail ads to restaurant operators implying business owners could suffer steep fines or even jail time if they do not post the specific signs they are selling. Over the years, some of the ad language has been toned down a bit, Reiser said, but there is no reason a restaurant has to pay for any company’s specific signs, especially ones being sold for $19.95 each. Any sign—from the $1 versions sold by WRA, to the free versions that can be downloaded from the Department of Health Services and WRA web sites, to a handmade sign—will satisfy the regulatory requirement, according to Reiser.

The company most recently marketing these signs used an official-looking eagle logo, a Madison address and references the Wisconsin Department of Health Services to further the impression of a government endorsement. In reality, the Madison address is only a P.O. Box (the company is based in Michigan) and the ads have been referred by DHS to their legal counsel and the Consumer Protection Office at the Department of Agriculture, Trade and Consumer Protection for investigation.

Medical kits: Another intimidate-and-sell scheme that has come up more than once is the “OSHA” medical kit. A company calls saying your restaurant must have an approved medical kit required by OSHA or they could face stiff fines. While OSHA does require businesses to have first aid supplies, Reiser explained, the supplies must only be “commensurate with the hazards of the workplace.” In other words—despite what a company may want you to think—no specific kit is required.

Vanity publications: These aren’t scare-and-sell products, but more like flatter-and-sell products. A company will call and tell you that you have won an award or that they want to include you in a prestigious sounding directory. Then they want you to buy the directory, which will probably cost you hundreds of dollars. You may get the directory, but don’t feel too flattered; they will undoubtedly bestow this “honor” on anyone willing to write the check.

I’ve been targeted—now what?

If you feel you’ve been targeted by a con artist or an unscrupulous company trying to pull a fast one on your business, let the WRA Hotline know. They can refer you to any government agencies tracking such scams and they can let your fellow restaurateurs know what is out there by sending an alert to the WRA members. If restaurateurs all watch each others’ backs, hopefully fewer people will be taken in by the scammers. WR