

## How Many “Bombs” Are You Storing in Your File Cabinet?

*The Federal Trade Commission estimates that roughly 10 million Americans have their personal information pilfered or misused in some way every year, costing consumers \$5 billion and businesses \$48 billion annually.*

If you were asked to store a hand grenade in your house, you would refuse. If you were asked to store 250 of them, you would think the person asking was making a joke. Yet believe it or not, some charities routinely do something similar and it is no laughing matter. They store credit card numbers in hard copy, complete with expiration dates and names of the card holders. The reasoning is that the charity can have ready access to the card number should they need to modify a charge. Or make periodic charges. Each of these card numbers is a potential “bomb” if it were to fall into the hands of an identity thief. If you use a payment processing “terminal” system to check people in at your event, or ask patrons to fill out registration cards with credit card information, it is quite possible you are storing ‘hand grenades’ in your file cabinet at this very moment.

Consider this: A file folder is missing from your file cabinet. You know that inside that folder is a paper tape from your event check-in terminal containing the complete credit card number, expiration date and name of each of the attendees from your last event, or all the registration cards which contain credit card information. There are over 250 of them. In the wrong hands, each one of these credit card numbers represents a huge identity theft problem, a ‘bomb’ waiting to go off. **What is your next move?**

Of course you will launch a search for the file and hope it was just temporarily misplaced, but what if it was deliberately removed by an employee or a volunteer? At what point do you call off the search, and begin calling your patrons to advise them their credit card information has been compromised? What if the theft included not just the credit card numbers from your last event, but from all events for the last four years? Hundreds of stolen credit card numbers (or even 1 credit card number) represents a huge liability to your organization. The next time you host an event, your patrons are going to be very reluctant to trust you with their information. This will directly cost your organization, reducing your ability to sell auction items or receive donations. Further, should any of these credit card numbers fall into the hands of criminals, the liability back to your organization (and you) is enormous. Board members would also be quite nervous if they were aware you were storing so many ‘bombs’ in your file cabinet.

Until recently, it was common practice for patrons at event check-in to be asked for an imprint of their credit card. This was accomplished using carbon copy slips and a “knuckle buster” imprinter. With patrons being nervous about identity theft and having a copy of their credit card on file, several vendors have come up with a “swiped card” approach, including MaestroSoft. Some vendors use a terminal for check in, swiping the credit card and producing a paper tape for signature. Instead MaestroSoft’s system is paperless and stores credit card information in an encrypted file. Terminal approaches store credit card data within the terminal, and because printing a paper tape will expose those numbers, terminals are not secure. Many patrons may feel better about the check-in process because they see their card being swiped rather than imprinted, but from a security standpoint there is little difference. In fact, it is easier to make a paper tape print out than making photo copies of a stack of imprinted slips. In this regard, some terminals may be LESS SECURE than the old “knuckle buster” method.

Storing credit card information in any manner where that information can fall in to less than honorable hands is just bad policy. Surprisingly, not only is it easy to do, it is actually a recommended practice by some payment processors! Their advice is to "print a paper tape of all of the credit card numbers, and store in a safe place." With some credit card check-in terminals, it is simply a matter of selecting a menu choice, then pressing print. Out comes a full listing of all the stored credit card numbers, names and expiration dates for each card that had been swiped! The process takes just seconds and can be done without any password being required. Considering events use volunteers extensively at check in, it is simple to see that this sensitive information could disappear immediately. Unless someone continuously monitors the volunteers, you would never know a list of credit card numbers was even printed. Criminals could be stealing the identity of your constituents before you even process their credit card charges!

So, how can you diffuse these 'bombs?' The best way is to not build the 'bomb' in the first place. Consider the MaestroSoft system for a moment. With *qCheck* credit card processing, a swipe of a credit card puts the sensitive information into an encrypted data file immediately. There is no paper tape printer and a printout can never be made of the full, un-encrypted card number. After the event, this encrypted file is uploaded through an Internet connection to IATS/Ticketmaster, MaestroSoft's preferred credit card processing partner. Once uploaded, IATS uses their proprietary technology to decode the encrypted file and returns to the client a six digit customer ID number representing each patron's credit card. These customer ID numbers are stored (in *AuctionMaestro Pro™* software) for future use if needed, but never the credit card number of the patron. At no time does the charity ever have access to (or need) the full, unencrypted credit card number of their patrons. Corrections, additions and credits are all handled using the unique six digit customer ID number assigned to each patron.

Your patrons want to help you with your cause. They have a level of trust in your organization and assume you are looking out for their best interests as they support your event. When they trust you with their sensitive information you should repay them by protecting that information. By eliminating any risk of identity theft, you are respecting their wishes and you are eliminating a potential 'bomb' before it is ever created. This is not only a good business practice, but reduces potential liability for you, your Board members and your organization.

Jay Fiske

*Jay Fiske is the CEO of MaestroSoft and a nationally known auction consultant. He has been actively helping charities raise money through auctions since 1990, and his two companies, Northwest Benefit Auctions, Inc., and MaestroSoft, Inc. have collectively helped charities raise in excess of \$3 Billion. More information is available at [www.auctionhelp.com](http://www.auctionhelp.com) and [www.maestrosoft.com](http://www.maestrosoft.com)*