Why a Data Breach Makes *Fraud* Your Problem—Even if the *Breach* Isn't

A recent data breach scare at eBay is just the latest in a series of hacking incidents that are reaching epidemic proportions. Aren't you glad they don't affect you? *They can*. Just because your data security is intact doesn't mean you won't be on the receiving end of potential card fraud involving data stolen from another merchant. Stolen data could end up in a potentially fraudulent card transaction in your store. Are you ready to spot it?

It's always a good idea to revisit and sharpen up your application of best practices against such fraud, to protect both your business and your reputation. As long as you follow proper card acceptance procedures, you won't be liable for losses even if fraud does occur.

With **card present** transactions, it's critical to actually inspect the card. Look carefully to confirm the card is valid and shows no signs of tampering. The card itself can give clues: Be sure the digits are properly aligned, check to see that any hologram moves when the card does, and compare the name, number, and signature on the card with those on the transaction receipt. It's tempting for employees to skip these steps, but they're absolutely crucial. So is adherence to the authorization process and store procedures if fraud is suspected. Signed sales receipts and photo ID validation can help prevent chargeback liability.

In a **card-not-present** environment, the merchant is always at greater risk and card fraud attempts are much more common. Obtaining positive address verification and CVV numbers are critical for avoiding chargeback liability.

You can also limit your vulnerability to fraud by looking out for novel or unusual behaviors. Here are 10 transaction red flags to look for. Transactions like these might be legitimate, but they always deserve a second look:

1. A new customer, especially from out of the area
2. Multiple card entries for high-dollar orders
3. Billing and shipping information don't match
4. Multiple purchases of the same item
5. Multiple transactions from a single IP address
6. Sequences of similar account numbers
7. One card used for sending shipments to multiple addresses
8. Several cards used for shipping to a single address
9. International shipping
10. An unsolicited phone authorization for a cash advance

While these might turn out to be false alarms, if you don’t know or have an established business record with a customer, you should identify them online and vet them carefully before proceeding.

Above all, it's vital to set aside time to educate all your employees about proactive procedures. The risk of fraud is not going to decrease—nor should your efforts to defeat it.

Contact us at (**866) 944-0055** or info@veracitypayments.com to learn more about how to protect your business.