Feb 19, 2015

Categories:

Publications

Authors:

Michael E. Nitardy

Will your business be financially responsible for cyber attack losses?

Businesses are becoming increasingly concerned with cybersecurity as their reliance on technology and data increases. Recent reports of cyber attack incidents underscore the importance of proactive steps to assess a business's vulnerability. Do you know how much liability your business could potentially have if it or its service provider is a victim of a cyber attack? Are the details as to who is responsible for different kinds of losses resulting from a cybersecurity incident clearly and sufficiently spelled out in your business's service provider contracts? A recent federal court decision highlights the importance of careful contract drafting and review to ensure that even time-tested contract language continues to accomplish the parties' business goals and allocates all the risks as intended, including liability for data breach losses.

Schnuck Markets v. First Data Merchant Data Services Corp. and Citicorp Payment Services, U.S.D.C. E.D. Missouri, No. 4:13-CV-2226-JAR, decided January 15, 2015, involved a well known grocery store in Missouri that was the victim of a cyber attack in late 2012 through early 2013. The companies that provided the grocery store with transaction processing services relied on the parties' credit and debit card processing services agreement as justification for withholding funds from the grocery's card transactions to cover credit card losses sustained from the data breach. The Limitation of Liability clause in the processing services agreement between the parties capped the grocery's risk exposure at $500,000, except for the processors' losses arising from the grocery's failure to comply with Payment Card Industry Data Security Standards ("PCI-DSS"), and from "… liability for chargeback, servicers' fees, third party fees, and fees, fines or penalties [sic] by" Card Associations, such as MasterCard and Visa. The Card Associations were permitted to issue assessments to processors to reimburse the Card Associations for losses relating to fraudulent charges on cards if a data breach involved data from a card's magnetic stripe. The question put to the court was twofold: (i) whether the processors

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

FBT Gibbons

improperly funded a reserve account, as purportedly permitted by the processing agreement, in an amount that exceeded the grocery's general maximum liability exposure under the Limited Liability clause and (ii) who, under the terms of the processing services agreement, was ultimately responsible for the reimbursement for fraudulent credit card charges.

The court found that the contract language that capped the grocery's liability at $500,000 did not have an exception that was applicable to this data breach so as to expand the grocery's liability; therefore, the processors were not justified in withholding more than $500,000. The court found that the concept of Data Compromise Losses, although a relatively new business risk, was known to the parties drafting the contract and could have been included in the laundry list of excepted events. The court also determined that the losses that the processors were trying to recover from the grocery could not be properly categorized as a "fee" or a "third party fee," as no intended or expected service was exchanged, nor as "fines" or "penalties," because they were not sums imposed as punishment. Finally the processors could not convince the court to shoehorn the Data Compromise Losses into either the contract's other indemnity language or the exception for non-compliance with the PCI-DSS, for the primary reason that no allegation had been pleaded in the lawsuit that the grocery was either negligent or had operated out of compliance with data security standards.

In summary, carefully drafted contract language that clearly describes the parties' expectations as to security measures, post-cybersecurity incident obligations, and allocation of liability is vital in order to avoid surprises with respect to your liability for loss in the wake of an incident. If you have questions about your potential liability with respect to data breach losses, please contact Jane Shea, Holly Powell, Michael Nitardy, Bill Repasky or any member of the Frost Brown Todd Privacy and Information Security Law team.

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

FBT Gibbons