The Powerful Economic-Loss Rule

Defending the Business-to-Business Data-Breach Lawsuit

By Alex M. Pearce

Hardly a day goes by without a headline announcing that a prominent company has fallen victim to a data breach. These headlines are followed, almost inevitably, by reports of class action lawsuits filed by consumers whose data was compromised.

In the typical data-breach case, these consumers sue the breached company before thieves have misused their data. The alleged injury, then, is usually an increased risk of *future* fraud or identity theft.

Future harm, however, is often not enough to establish Article III standing in a federal court. Thus consumers have had only limited success in these data-breach lawsuits.

When a data breach affects a company's business partners, on the other hand, they're much more likely to suffer direct financial loses that can be readily identified. Business plaintiffs in data-breach lawsuits thus have little trouble alleging an "injury in fact" sufficient to establish standing.

With standing-based arguments foreclosed, how else can a company defend against data-breach lawsuits brought by its business partners?

According to a recent decision from a federal court in Colorado, one potentially powerful defense is the economic-loss rule, which prevents plaintiffs who suffer economic losses stemming from a contract from trying to recover those losses through non-contract claims.

This column examines that decision and its implications for defendants in business-to-business data-breach lawsuits.

A Cyberattack Compromises Diners' Payment-Card Data

SELCO Community Credit Union v Noodles & Company, No. 16-CV-02247-RBJ, 2017 WL 3116335 (D. Colo. Jul. 21, 2017), concerned a cyberattack on the Noodles & Company restaurant chain that compromised customers' credit and debit card information. The plaintiffs were credit unions whose cardholders dined at Noodles and whose information was compromised.

According to the credit unions, Noodles breached a common law duty to protect its customers' payment-card information by failing to implement industry-standard data-security measures. The credit unions alleged that this breach caused them damages, including the costs to cancel and reissue affected cards and to refund cardholders for unauthorized charges.

The credit unions brought tort claims—all based on theories of negligence—against Noodles. Noodles filed a motion to dismiss based on the economic-loss rule, pointing to agreements that it and the credit unions had entered as participants in the payment-card-processing ecosystem.

The Payment-Card Ecosystem: A Chain of Interrelated Contracts

In its motion, Noodles observed that each actor in this ecosystem signed an agreement with at least one other actor in which it agreed to follow rules issued by bank-card associations such as Visa and Mastercard. Importantly, the agreements required merchants such as Noodles to maintain a certain level of security for payment-card data—including compliance with a set of detailed best practices for data security in the payment-card industry called the Payment Card Industry Data Security Standard (PCI DSS).

Noodles argued that these agreements also allocated the parties' rights and responsibilities in the event of a cyberattack. Specifically, the agreements called for the credit unions to guarantee cardholders zero liability for fraudulent transactions. The credit unions, in turn, could partially recover their losses from breached merchants through a loss-shifting scheme managed by the bank-card associations.

Noodles accused the credit unions of trying to undermine this risk-allocation scheme—and violating the economic-loss rule—by bringing tort claims.

An Independent Duty?

The credit unions had two main arguments in response. First, seeking to avail themselves of the "independent-

■ Alex M. Pearce is of counsel at Ellis & Winters LLP in Raleigh, North Carolina. His practice focuses on privacy and data-security law. He provides guidance to clients on matters that implicate domestic and international privacy and data-security considerations. His experience includes counseling on state and federal privacy, consumer protection, and breach notification laws; designing and implementing global data-protection compliance strategies; negotiating cloud-computing, data license, and data-sharing agreements; and representing clients in disputes that involve privacy and data-security issues.

duty" exception to the economic-loss rule, they argued that Noodles owed them a common law duty to secure payment-card data and to prevent foreseeable harm to cardholders. This duty, they urged, was separate and distinct from any contract-based duty to comply with PCI DSS and could support their tort claim. Second, the credit unions argued that the economic-loss rule should not apply because the credit unions had no direct contract with Noodles. Thus, the credit unions argued, they never had the chance to "reliably allocate risks and costs" with Noodles.

The Court's Decision

The court sided with Noodles.

On the independent-duty argument, the court concluded that each duty that Noodles allegedly breached was bound up in the agreements to comply with the bank-card association rules and PCI DSS. Even if Noodles might *also* have had a common law duty to protect payment-card data from a cyberattack, that duty could not be considered "independent of a contract that memorialize[d] it." *SELCO,* 2017 WL 3116335, at *4.

The fact that the credit unions never contracted directly with Noodles had no analytical influence. In the court's view, the economic-loss rule does not mandate a one-to-one contract relationship. Instead, the court reasoned, the rule asks whether plaintiffs had "the opportunity to bargain and define their rights and remedies, or to decline to enter into the contractual relationship." *Id*. at *5. The credit unions, concluded the court, had that chance here.

Lessons for Litigants

SELCO confirms that the economic-loss rule can provide a powerful shield against attempts—including and especially by businesses—to make end-runs around negotiated limitations and allocations of liability for cyberattacks.

Defendants, however, must be ready to show that the contract on which they rely imposes relevant data-security obligations. Doing so requires that the obligations be clearly defined—well before litigation arises—in any contracts that involve the receipt or handling of sensitive information.

Clearly defining data-security obligations in contracts is already a recognized best practice for information-security risk management. But as *SELCO* demonstrates, this type of clarity can also lay the groundwork for deploying the economic-loss rule against business-to-business lawsuits arising from a successful cyberattack. FD