HUNTON& WILLIAMS

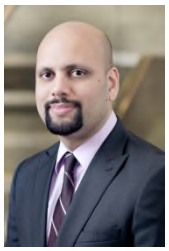
Lawyer Insights

January 11, 2018

How Retailers Can Protect Themselves Against Mobile Payments Risks

by Lorelie Masters, Syed S. Ahmad, Katherine Miller

First published in Internet Retailer on January 11, 2018.


Retailers often rely on technology providers to operate systems that enable customers to pay with their phones in stores. Without proper insurance, retailers could face unexpected financial losses.

More and more retailers are turning to smartphone-reliant technology to streamline the buying experience. In addition to contactless payment apps provided by cell phone providers, many retailers are rolling out their own contactless payment systems.

Under this approach, customers may be able to download an app to their phones, enter their payment information, and then use a contactless payment terminal to make purchases. Many retailers provide additional perks to customers just for using their apps. For example, some retailers allow customers to submit their receipts through the app and offer a credit to the customer's account if lower prices are found with local competitors.

And some retailers are exploring technology that allows customers to scan their phones at the entrance of the store, shop, and leave the store with their purchases without waiting in line or after using any contactless payment system. Items are tracked for purchase using sensors on the shelves. However, as the use of these technologies increases, it is important for retailers to identify the potential risks that arise and ensure that they have the appropriate insurance coverage.

Limits of business interruption insurance

While contactless payment systems allow for a faster checkout time, these systems work only if the network is up and running. If the network servicing the retailer's application or the network servicing the payment system goes down or is interrupted, the retailer could suffer significant loss of business and loss of profits. Typically, a retailer will have "business interruption" or "loss of business" insurance for lost profits and extra expenses if a business suffers a suspension of operations. However, this insurance typically requires that the interruption be caused by a covered risk loss, such as a water leak, a hurricane, etc., and qualifies as a "direct physical loss."

Traditional business interruption coverage would typically not cover a network outage or interruption caused by a ransomware attack or other outage not resulting from a physical loss. Thus, a retailer would likely need to secure specific cyber-related insurance coverage for this risk.

In addition, if a retailer relies on a third-party provider for the operation of its app or contactless payment system, it should consider securing contingent business interruption coverage. In general, this coverage covers a policyholder's lost profits resulting from the interruption of another business's operations that the policyholder heavily relies on, such as the policyholder's key supplier or customer.

Because contingent business interruption coverage also typically requires direct physical loss to the third party (the retailer's supplier, customer, etc.), a retailer will likely need to secure this coverage under a cyber-specific policy that specifically covers lost profits resulting from the interruption of a third-party service provider.

Similarly, a retailer will want to ensure it has cyber insurance coverage that responds to a ransomware attack if it suffers an attack on its mobile app or contactless payment system. This coverage should specifically cover the cost to hire a consultant, the cost of ransom to terminate an ongoing ransomware attack and unencrypt data, and the cost of ransom to prevent an imminent attack.

Ensuring that this coverage is in place—with the appropriate terms and conditions—is critical given that ransomware attacks are on the rise and have been widespread, as can be seen from the recent WannaCry and Petya attacks. Further, because hackers often seek payment in cryptocurrency, it is important to ensure coverage for ransom includes payment made in cryptocurrency.

In addition, as with traditional payment systems, a retailer is always at risk of liability resulting from a breach resulting in unauthorized disclosure of customer information. These breaches can easily result in multi-million-dollar losses and related reputational risks to retailers, as can be seen by some of the recent breaches suffered by retailers and other businesses. This potential liability will likely need to be addressed by a cyber insurance policy that covers breach notification costs, credit monitoring costs, and other costs resulting from a data breach or phishing attack.

Data breach exposure

And a retailer should keep in mind that, even if a third party is effectively handling all aspects of a contactless payment system, when there is a breach or other unauthorized disclosure, there is a significant risk that the retailer will be embroiled in lawsuits brought by consumers if there is a security incident or breach. Thus, if a retailer uses a contactless payment system or app that is operated by a third party, it must ensure that the third party has its own adequate insurance coverage for these losses, including liability for a privacy breach and breach notification costs.

The retailer must also ensure that it adequately transfers the risk of loss to the third party, which includes carefully drafting contracts with third parties that service these technologies to include insurance requirements, such as naming the retailer as an additional insured under the third party's own insurance and including indemnification requirements that provide that the third party is responsible for the retailer's liability that results from the third party's actions and omissions.

The European Union's Global Data Protection Regulation, which goes into effect on May 25, 2018, also raises the stakes for any company that operates in the EU, emphasizing the need for retailers to have in place well-designed data breach response plans and cyber insurance.

In sum, while the emerging payment technologies seek to streamline the buying experience, it is important for retailers to identify all potential risks arising from these technologies and to ensure their insurance coverage adequately covers the risks.

Lorelie Masters and Syed Ahmad are partners in the insurance coverage practice in Hunton & Williams LLP's Washington, DC office. Lorelie can be reached at (202) 955-1851 or lmasters@hunton.com. Syed can be reached at (202) 955-1656 or sahmad@hunton.com. Katherine Miller is an associate in the law firm's insurance coverage practice in its Miami office. She can be reached at (305) 810-2525 or kmiller@hunton.com.