6 Quick Lessons from Jimmy John's POS Data Breach

According to public releases by Jimmy John's (the sandwich shop franchisor) and Signature Systems (the point of sale (POS) system provider for 216 Jimmy John's locations), malware was installed on those POS systems through use of a user name and password used for purposes of remote administration. This type of remote access has been an ongoing source of unauthorized access to POS systems for some time and has affected other franchised retail businesses. Here are **six quick lessons** franchisors should learn from these attacks:

1. Know Your Vendor.

The breach at Jimmy John's has been traced to the "PDQ" POS system sold by Signature Systems. As noted above, access to the PDQ POS system was gained as a result of a user name and password used to remotely administer the systems. As of October 2013, the PCI Security Standards Council had removed approval of the PDQ system for new deployments (see Validated Payment Applications). A check of approved systems would have shown that this system should not have been installed at new locations after the date the approval was removed.

2. Do Your Due Diligence and Periodically Verify.

Vendor due diligence cannot be over-emphasized. Merchants are responsible for choosing and implementing systems that are PCI compliant. Franchisors should independently verify the PCI validation of a POS system prior to purchase. Further, you should incorporate periodic verification of ongoing approval of the system into your data security policies. You should also evaluate whether to implement a broader search to identify reported or known security vulnerabilities in the specific POS system. In particular, ask your POS vendor what it has done to address remote access vulnerabilities—and check up on your vendor periodically to assess its ongoing compliance and updating of security.

3. Update Your Systems.

You should regularly check for and install security patches and other updates for your POS system. Franchisees should be required to promptly update their systems when new patches are available. Franchisors should implement a system to notify franchisees of available system updates.

4. Use of Unapproved Systems May Be Hazardous to Your Wallet.

The use of systems that are not PCI approved and compliant will expose users to liability for unauthorized card transactions. Card processing rules impose liability on merchants in situations where the merchant is not PCI compliant and card data is compromised. This dollars and cents liability should be communicated to your franchisees.

5. Monitor Developing Card and Data Security Threats.

Payment card security is not a static world. Security threats are continually evolving and the sophistication of attacks is continuing to grow. The effectiveness of your security program is dependent on understanding how these threats are evolving and making adjustments to respond to the new threats. Regular review of the threat landscape should be an integral part of your security program.

6. Communications Are Important.

In most cases, the card issuers are the first to detect a pattern of fraudulent transactions and will then notify the affected merchant, typically the individual franchisee. That means that your franchisees may receive notice of a breach, but you do not. Being able to react quickly to a breach is important for your brand. You want to be able to react to the incident and to deliver notice to other franchisees that may be affected. In order to help in promptly responding to a breach, you should adopt a policy requiring that franchisees immediately notify you when they receive information about a potential breach. Without effective communications from your franchisees, the first you hear of a breach may be from a reporter.

Although certainly not exhaustive, taking the steps mentioned above will improve your data security risk management. Reliance on the assurances of others is no substitute for your own knowledge and due diligence.

* * * * *

For further information regarding cyber security, data breaches, and taking proactive measures to protect your franchise system, please contact Mark Kirsch (mark.kirsch@gpmlaw.com or 202.295.2229) or George Meinz (george.meinz@gpmlaw.com or 320.202.5358), visit the Payment Systems page on our website, or view our franchisor guidance regarding cyber security and protecting franchise system customer data.