PCI DSS: A [Non-]Law Every Kentucky Lawyer Should Understand
BY: PROFESSOR ED ZUGER

INTRODUCTION
The Payment Card Industry Data Security Standard (PCI DSS) is the “global data security standard adopted by the payment card brands for all entities that process, store or transmit cardholder data and/or sensitive authentication data.” The standard consists of six organizational security goals further split into a dozen requirements, each of which being comprised of multiple sub-requirements. In a nutshell, the standard reflects the best practices toward maintaining the confidentiality, integrity, and availability of an organization’s cache of payment card information. It is critical for every payment card stakeholder to understand the requirements that govern an organization’s use and custody of payment card data.

THIS MEANS YOU
We are all most likely stakeholders in the system that relates to payment cards. “Payment cards” may also be known as bank cards, ATM cards or another form of payment device, though the payment cards that are the subject of this writing, and of the PCI DSS, relate to credit cards or debit cards. We carry them. Many of us accept them as payment. Surely many of our business clients, if not all, carry, use, and process payment cards. According to PrivacyRights.org, since 2005 there have been over 9,000 publicly reported data breaches that, when combined, total 11 billion compromised records containing sensitive information. Information derived from a payment card gets bought and sold in underground marketplaces found on the dark web. While it is impossible to fully vet marketplace data, recent estimates for the value of just one credit card including a full set of card data extends up to $40 per card. Payment card information represents some of the most sought after data available to opportunistic criminals and fraudsters. Cardholder data, in one sense, is the key not only to our bank accounts, but also to our credit allowances, which regrettably in too many modern cases balloon much larger than the bank accounts to which they’re tied. Custody of payment card data, therefore, requires care and effort in order to protect the value that it bears.

This brief article intends to edify the reader about one mechanism in place to help buttress the information security surrounding payment card data. For readers who process payment cards, or whose clients do the same, the piece will illuminate the main goals of compliance that the PCI DSS requires, lest you or your clients lose the privilege of accepting cards for payment. Said another way, unless you want to go back to cash or barter, you’ll want to comply with the PCI DSS requirements. First, we get some context about why the payment card industry determined a need to create a standard. Then comes a quick rundown of the standard, and its goals and requirements. Finally, there will be consequences demonstrated. What could happen after failing to uphold the standard? The answer regrettably involves litigation and money damages. Recall from the title, this is not a law. These aren’t regulations. The state has no interest in the fight. These are governing principles for your organization nonetheless, and their voluntary nature is the merchant’s or vendor’s Hobson’s choice. Thus, you and your clients either comply with the PCI DSS requirements, or do not and limit your transactions to cash, or do not and risk what could cost you much more than the business that you might lose by being a cash-basis concern.

INDUSTRY DEEMED THE LAWS AS LAX
We can skip over the transactional days of barter and fast-forward to the early 1900s when the first payment cards were not
bank-issued, such as Visa or MasterCard, but rather were issued by gas stations, retailers, and hotels. Back then, a mere piece of plastic (the early varieties, however, were coins) and your good name was enough to trade for goods and services. The utility of payment cards has not changed much over the decades. As payment card users, we tend to operate as one of two types. Some of us use them for their convenience, including their security vis-à-vis cash, and others use them as “revolvers,” those who rely on the related line of credit to finance a purchase.

You need not be an information security expert to understand that criminals historically and continually see new technologies as new opportunities for fraud and crime. No different was the payment card. Whether you are a convenience user or a revolver, the threat has become evident.

There are various studies about the impacts of payment card fraud and crime. The Association of Certified Fraud Examiners put the 2016 costs at over $28 billion. As a portion of that, the Aite Group posited that 2018 gave way to nearly $1 billion in losses specifically associated with synthetic credit card fraud—i.e., when fraudsters create identities out of thin air to obtain credit. No matter how you stack the cards, the problem costs us all, and has done so as long as the cards have been in existence.

As attorneys, we are aware of many laws and regulations that have been implemented to thwart payment card fraud. The Consumer Credit Protection Act of 1968, commonly called the Truth in Lending Act, was an early entry that protected consumers from unfair credit card practices. The federal government set forth penalties for the fraudulent use of payment cards at 15 U.S.C. § 1644. The Credit CARD Act of 2009, sometimes known as the Credit Cardholders Bill of Rights, amended the Truth in Lending Act, and others, toward minimizing unfair and deceptive credit card practices. In Kentucky, we look to KRS Chapter 434, et seq, for protections against payment card crimes such as their unauthorized reproduction. However, if you ask the payment card industry companies, the government’s intervention failed to be effective enough in the massive fight against fraud.

**INDUSTRY RESPONSE TO INEFFECTIVE LAWS**

Enter the Payment Card Industry Security Standards Council (PCI SSC). The industry group was founded in 2006 by American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc. It identifies as “a global forum for the industry to come together to develop, enhance, disseminate and assist with the understanding of security standards for payment account security.” Organizations, obviously including law firms, that desire to accept payment cards for payment must comply with the standards set forth by the PCI SSC. The banks that process payment card information enforce said compliance.

Compliance is not to be taken lightly, as will be shown, but let us first look at an overview of the PCI DSS. According to version 3.2.1, the newest iteration of the standard released last May, there are six main goals of the PCI DSS, and 12 requirements that must be adhered to in order to uphold those goals:

<table>
<thead>
<tr>
<th>Goals</th>
<th>PCI DSS Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Build and Maintain a Secure Network and Systems</strong></td>
<td>1. Install and maintain a firewall configuration to protect cardholder data</td>
</tr>
<tr>
<td></td>
<td>2. Do not use vendor-supplied defaults for system passwords and other security parameters</td>
</tr>
<tr>
<td><strong>Protect Cardholder Data</strong></td>
<td>3. Protect stored cardholder data</td>
</tr>
<tr>
<td></td>
<td>4. Encrypt transmission of cardholder data across open, public networks</td>
</tr>
<tr>
<td><strong>Maintain a Vulnerability Management Program</strong></td>
<td>5. Protect all systems against malware and regularly update antivirus software or programs</td>
</tr>
<tr>
<td></td>
<td>6. Develop and maintain secure systems and applications</td>
</tr>
<tr>
<td><strong>Implement Strong Access Control Measures</strong></td>
<td>7. Restrict access to cardholder data by business need to know</td>
</tr>
<tr>
<td></td>
<td>8. Identify and authenticate access to system components</td>
</tr>
<tr>
<td></td>
<td>9. Restrict physical access to cardholder data</td>
</tr>
<tr>
<td><strong>Regularly Monitor and Test Networks</strong></td>
<td>10. Track and monitor all access to network resources and cardholder data</td>
</tr>
<tr>
<td></td>
<td>11. Regularly test security systems and processes</td>
</tr>
<tr>
<td><strong>Maintain an Information Security Policy</strong></td>
<td>12. Maintain a policy that addresses information security for all personnel</td>
</tr>
</tbody>
</table>
For each of the 12 requirements, the PCI SSC set forth many subrequirements, 80 altogether. Thus, your careful analysis will be better facilitated by visiting its website and poring over the 39-page PCI DSS Quick Reference Guide. Suffice it to say, particularly for the uninitiated payment card stakeholder, that even envisioning compliance with the 12 requirements may give them pause.

When you contemplate the 12 requirements, think in the most personal and basic terms about whether you, yourself, abide. For instance, the last time you bought a WiFi router, did you change the default password before setting it up? Do you use antivirus software? Do you regularly update your antivirus software? How restricted is your cardholder data? Not very if you are in the habit of allowing assistants or office mates to use the card, or if you are not in the habit of shredding paper statements. Those questions point at you, the individual. Now, think about the standard from the perspective of your entire firm or, importantly, your business clients who process payment cards. It can be daunting. When daunting evolves to noncompliance, then there is a real problem.

THE COSTS OF NONCOMPLIANCE
The Nashville firm Genesco, a publicly traded footwear powerhouse with thousands of retail outlets, faced a cyber attack in 2009 and 2010 that culminated in Visa, Inc., levying over $13 million in noncompliance fines, which were fought in federal court. To be clear, Visa fined Wells Fargo and Fifth Third under their respective contracts that included a requirement that the banks ensure that Genesco and other merchants, comply with the PCI DSS. The banks, of course, were indemnified against Visa’s fines under their agreements with Genesco.

Based on the requirements of the PCI DSS, Visa looked to reports provided by the standard’s mandated Qualified Security Assessor and PCI Forensic Investigator, supportive functions you should be aware of, particularly when (not “if”) faced with a security incident. The reports illuminated three areas of noncompliance based on Genesco’s security incident, to wit the PCI DSS Requirements 1., 8., and 11. From a security perspective, the glaring issue was that Genesco’s cardholder data was left unencrypted. Don’t do that. The case in the main surrounded discovery and the FRE, which are 1., 8., and 11.

We can agree, especially on behalf of our small business clients, or your own practice if it processes payment cards, that compliance with the PCI DSS is not inconsequential. You likely already understand that the payment card industry initially takes some percentage from every transaction, the so-called interchange fee. The costs to comply with the standard add to that fee. Some put that number in the tens of thousands of dollars.

CONCLUSION
Genesco truly represents one of the PCI SSC’s largest fines levied for noncompliance. Nevertheless, if you assume that such a result would never apply to you or your clients, do not forget that when a data breach or hack occurs perhaps the PCI SSC is the least of your worries considering the relevant laws and regulations that go into force upon such an incident. One that should come to mind is Kentucky’s data breach notification statute (plus, you or your clients may be subject to multiple jurisdictional laws, related).

We can forestall the lesson about that challenging and potentially costly law. For now, among the numerous additional governance rules and costs for noncompliance within this edition and beyond, heed the warning that ignorance of or noncompliance with the PCI DSS will not spare you or your clients from the pains inherent to information security incidents. Rather, look at an investment in its understanding as exactly that, and more importantly activate your newfound understanding of it for your firm, its clients, and their customers. The payment card system is complex, and the old adage about the power of the weakest link applies. Billions of stolen records should demonstrate that in spades.

ENDNOTES
acl=15134870826847.
15. Id. at 564.
17. KRS 365.732.