OUR PRACTICE

Data Protection: Payment Card Industry Security

From major retailers to small businesses, all companies that accept, store, or transmit credit card data must comply with the Payment Card Industry Security Standards Council's (PCI SSC) Data Security Standards (DSS). Failure to comply with the PCI-DSS can negatively impact a company's reputation and have significant legal repercussions. As companies that are subject to PCI-DSS continue to be targets of sophisticated cyberattacks, complying with PCI-DSS remains paramount in avoiding potential data breaches and cyber incidents. As businesses collect substantial amounts of information on their customers, protecting that information has become increasingly difficult. When that data includes credit or debit card information, complying with mandatory security standards can seem even more complex. Baker Donelson has been recognized as an authorized NetDiligence Breach Coach® signifying it as a top tier law firm for Data Security, Privacy and Incident Response.

Baker Donelson's privacy professionals regularly advise clients on how to implement best practices to proactively ensure PCI-DSS compliance and minimize potential exposure. This includes working with clients to:

- Assess the level of required PCI-DSS compliance
- Evaluate relationships with vendors that may process credit card data on your company's behalf
- Identify and direct investigations into suspected data incidents involving credit card data
- Assist with regulatory reporting obligations

Whether your business has suffered a large-scale compromise, such as a ransomware attack, or is dealing with an inadvertent disclosure of an individual's credit card information, our team can help.

More than one-third of our team is credentialed with the world's largest privacy organization, the International Association of Privacy Professionals (IAPP), as well as other credentialing organizations. Our credentials include:

- Artificial Intelligence Governance Professional (AIGP)
- United States-focused Certified Information Privacy Professional (CIPP/US)
- Europe-focused Certified Information Privacy Professional (CIPP/E)
- Canadian-focused Certified Information Privacy Professional (CIPP/C)
- Privacy management-focused Certified Information Privacy Manager (CIPM)
- GIAC Law of Data Security & Investigations (GLEG)
- Privacy Law Specialist (PLS)
- Payment Card Industry Professional (PCIP)
- Certified Information Security Manager (CISM)
- Certified Information Systems Security Professional (CISSP)
- Qualified Technology Expert (QTE)
- Certified Information Privacy Technologist (CIPT)

Our Financial Services Data Protection, Privacy and Cybersecurity attorneys advise businesses on all aspects of PCI DSS compliance, including:

- Building and maintaining a secure network
- Protecting cardholder data

- Managing relationships with third-party payment processors
- Maintaining a vulnerability management program
- Implementing strong access-control measures
- Regularly monitoring and testing networks
- Maintaining an information security policy
- Maintaining an incident response plan
- Employee training
- Leading investigations and working with industry experts to assist with detection, containment and recovery in data incidents affecting cardholder data
- Assisting with assessment and drafting of any state and federal notification obligations
- Managing communications with vendors, employees, customers, and other stakeholders
- Responding to any state and federal government investigations that result from a cardholder data incident
- Providing analysis to assist in developing post-incident remediation
- Handling litigation, including class action cases, involving data incident issues

Representative Matters

- Represented national retailer managing cyber incident affecting customer credit card information, including working with forensic vendor to contain incident, conducting multi-state breach notification analysis, and notifying major credit card brands.
- Advised a leading e-commerce company that was severely impacted by a phishing attack on multiple employee e-mail accounts that required assessment of regulatory issues under the Payment Card Industry Data Security Standards (PCI-DSS) and responding to regulatory investigations by state attorneys general.
- Represented e-commerce startup company on all aspects of PCI-DSS compliance, including user terms and conditions, privacy policies, and negotiating contracts with third-party vendors.
- Counseled retailer on complying with PCI-DSS requirements.
- Assisted merchant errantly included on MATCH list.