Financial Institutions & IT Asset Disposition

How financial institutions can meet compliance requirements by contracting for secure IT asset disposal with Cascade

The twentieth century U.S. criminal Willie Sutton was said to rob banks because "that's where the money is." The same motivation in our digital age makes merchants and financial institutions the new target for financial fraud. It's a serious problem – the Privacy Rights Clearinghouse reported 64 data breach cases at financial institutions impacting more than 1.4 million consumers from 2016 through June 2017.

Merchant-based vulnerabilities may appear almost anywhere in the card-processing ecosystem including point-of-sale devices; personal computers or servers; wireless hotspots or Web shopping applications; in paper-based storage systems; and unsecured transmission of cardholder data to service providers. The threat is exacerbated when companies rely on legacy IT systems. When any of these data storage medium is disposed, it is imperative to effectively clear or destroy all data on these devices to protect consumer data.

Compliance with the Payment Card Industry (PCI) Data Security Standard (DSS) helps to alleviate these vulnerabilities and protect cardholder data. Cascade provides a simple and secure means to ensure firms meet this standard when disposing of their IT assets.

> *Threats from cybercrime have increased and legacy IT systems are increasingly becoming a risk factor, especially in the financial industry. Many financial organizations rely on legacy IT systems that are expensive to maintain, prone to more unpatched vulnerabilities and the general challenges of software integration and architecture upgrading compound when mergers and acquisitions are in place.*
>
> *- 2016 Financial Industry Cybersecurity Report by* SecurityScorecard

PCI DSS is controlled by the PCI Security Standards Council which was founded by credit card brands to ensure that consumers are protected from data breaches by establishing minimum standards for companies who process credit cards. Creation of the standard was largely in response to high profile data breaches such as the one experienced by T.J. Maxx and others that were attributed to poor security measures and shook consumer confidence. Every company in the United States that processes credit cards as a form of payment must comply with this standard. Compliance was required by the year 2010.

Large firms that process over 80,000 credit cards per year must by certified by a Qualified Security Assessor. For smaller firms, the standard is different depending on how they actually process transactions. It could be as simple as completing a self-assessment questionnaire to certify the company has practices in place to meet the requirements of this standard.

Cascade itself is considered a merchant because it accepts credit cards for payment of products and services. Cascade meets the requirements of the PCI DSS standard and has completed a self-assessment questionnaire to certify we are compliant.

The PCI Security Standards Council maintains a website with a host of resources to help organizations comply with this law: www.pcisecuritystandards.org

Cascade can help firms meet their obligation to follow required security protocols to manage and ensure the destruction of all consumer financial data on disposed IT assets. To help regulated firms understand how Cascade's services can be aligned to meet the firm's PCI compliance requirements, we put together a table listing all the sections of the PCI DSS standard relevant to IT asset disposition.

Madison, WI * Indianapolis, IN
608-222-4800 * 888-222-8399
info@cascade-assets.com * www.cascade-assets.com

How Cascade helps financial firms meet relevent PCI DSS standard requirements

and protect their risk from maintaining legacy systems – version 3.2, April 2016

Item	Description	Interpretation	How Cascade helps you comply
9.8	Destroy media when it is no longer needed for business or legal reasons.	Firms need to perform media destruction themselves or contract with a suitable processor.	Cascade provides destruction services for electronic data storage media for our customers consistent with the PCI DSS requirements. We can also assist with document destruction services through the use of subcontractors.
9.8.1	Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed.	Paper materials must be completely destroyed. Examine storage containers used for materials that contain information to be destroyed.	Cascade outsources all paper destruction to NAID AAA certified companies who exceed this standard. Shredding is accomplished on site and a certificate of destruction is issued based on the weight of paper shredded. Cascade can also provide locking data bins to secure media in storage and transit.
9.8.2	Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	Method of destruction must prevent recovery. Examples of methods for securely destroying electronic media include secure wiping, degaussing, or physical destruction (such as grinding or shredding hard disks.)	Cascade will electronically overwrite data storage devices to NIST 800-88 Guidelines for Media Sanitization or physically destroy by shredding at the customer's option. We can also perform on-site hard drive, SSD and tape crushing, degaussing and shredding. Cascade's asset level disposition reporting allows firms to document the process used to render data unrecoverable. This report is available in paper and electronic formats.
9.10	Ensure that the security policy and operational procedures for restricting physical access to cardholder data are documented, in use and known.	All employees and partners must be aware of the risks presented by loss of data and employers must have a means to train personnel.	Each Cascade employee is trained at hire and annually on Cascade's security policy and program to protect customer data. Each employee signs an acknowledgment form upon completion of the training and receipt of our security policy which details Cascade's expectations regarding security.
12.7	Screen potential personnel prior to hire to minimize the risk of attacks from internal sources.	All employees and partners must pass a relevant background check if they will have access to cardholder data or the data environment.	Cascade performs background checks on all employees as a condition of employment. These checks review the previous 7 years and any crimes related to financial, fraud, or computer hacking, as well as employment history. In addition, all personnel are re-checked every three years.
12.8	If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers.	Firms need to execute a written agreement with service providers performing their IT asset disposition services and verify the service provider has appropriate policies and procedures in place via an audit or 3rd party verification.	Cascade recommends the execution of a service agreement with all regulated entities. Cascade's standard Master Service Agreement specifies Cascade's roles and responsibilities, and it is consistent with the contracting requirements of PCI DSS. In addition, Cascade performs at least annual 3rd party security audits as part of its e-Stewards certification. Customers are also welcome to visit and audit Cascade's facilities themselves.
12.10	Implement an incident response plan. Be prepared to respond immediately to a system breach.	Firms need to ensure service providers handling cardholder data have a method to coordinate breach incidents with the appropriate firm representative.	Cascade's ISO 9001 certified quality management system includes an incident response plan to identify and communicate any potential breach of customer data on equipment. Since Cascade's founding in 1999, there have been no incidents of an actual data breach, though anomalies were reported to customers when identified and all issues were resolved without incident.

Madison, WI * Indianapolis, IN
608-222-4800 * 888-222-8399
info@cascade-assets.com * www.cascade-assets.com