Playing it safe.

Ensuring Data Security Compliance at Your School.

It's no secret that identity theft is a growing problem in today's society. According to the Federal Trade Commission (FTC), an estimated nine million Americans fall victim each year to thieves who use their information for personal gain.[1] And the costs to individuals and businesses are huge—an estimated $50 billion a year in the United States[2]—not to mention the time that is spent dealing with the issue.

In light of this, data security is a growing priority issue for businesses that handle personal and financial information on any scale. And K–12 schools are hardly immune. In fact, educational institutions are among the most commonly-targeted industries for cyber theft.[3] Storing large amounts of confidential personal data and financial records, employing multiple payment systems, and using open networks are just a few of the things that make schools vulnerable to attack. In addition, children are increasingly being seen as prime targets by identity thieves because they have clean credit records. And parents rarely—if ever—think to check their children's credit reports, so the crimes can go undetected for long periods of time.

CDW-G's 2009 School Safety Index sheds light on the issues K–12 schools face when it comes to data breaches.[4] According to the index, 55 percent of schools or school districts reported some kind of IT breach including unauthorized user access, hacking, and viruses. And while many schools are taking measures to increase security, most report that they feel unprepared to deal with the threat, stating that budgets are too tight and human resources too strained to give the issue proper attention.

With all of the rules and regulations surrounding data security, it's no wonder schools feel overwhelmed by the subject. In this guide, we will take some of the confusion out of data security and help you understand what's required to properly protect the vital information your school may handle.

1 www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html.
2 www.privacyrights.org/ar/idtheftsurveys.htm.
3 "Cards at School," AFP Exchange, March 2007.
4 "2009 School Safety Index," CDW-G, May 2009.

Understanding Data Security Standards and Regulations

There are three main data security standards and regulations that your school will need to consider when creating a data security plan—PCI, NACHA, and the Red Flags Rule.

Payment Card Industry (PCI) standards

Three PCI standards have been developed by the PCI Security Standards Council, each setting specific requirements surrounding processing and storing account users' data.

- Payment Card Industry Data Security Standard (PCI DSS) dictates the rules and regulations for protecting customer account data when handling credit and debit card information.
- Payment Application Data Security Standard (PA-DSS) requires all payment applications obtained through a vendor to be certified. In-house payment applications may fall outside of this requirement but must still adhere to PCI DSS requirements.
- PIN Transaction Security Standard (PTS) mandates that merchants use PIN entry devices that have been tested and approved by the PCI Security Standards Council.

All merchants accepting credit card payments—regardless of the number processed—must comply with these standards. For complete information on the standards and lists of PA-DSS- and PTS-compliant devices, visit pcisecuritystandards.org. If your school handles any credit card transactions at the school or on your school's Web site, you are responsible for compliance with the PCI Standards.

PCI DSS: 12 Core Principles

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.

Protect Cardholder Data

3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.

Maintain a Vulnerability Management Program

5. Protect all systems against malware and regularly update anti-virus software or programs.
6. Develop and maintain secure systems and applications.

Implement Strong Access Control Measures

7. Restrict access to cardholder data by business need to know.
8. Identify and authenticate access to system components.
9. Restrict physical access to cardholder data.

Monitor and Test Networks Regularly

10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.

Maintain an Information Security Policy

12. Maintain a policy that addresses information security for all personnel.

NACHA (The Electronic Payments Association) rules

NACHA is a private-sector organization that governs the exchange of automated clearinghouse (ACH) payments. ACH payments include:

- Internet commerce (not including credit/debit card payments).
- Electronic bill and invoice presentment and payment (EBPP, EIPP).
- E-checks.
- Financial electronic data interchange (EDI).
- International payments.
- Electronic benefit transfer (EBT).

NACHA's rules and regulations primarily focus on the security of ACH payments and require any organization that transmits these kinds of payments to adhere to encryption standards. Therefore, if your school processes ACH payments of any kind, you will need to ensure that the proper encryption methods are used.

You can find more information about NACHA, including rules and regulations, at nacha.org.

Red Flags Rule

The Red Flags Rule was developed by the Federal Trade Commission (FTC), the federal bank regulatory agencies, and the National Credit Union Administration (NCUA) as part of the Fair and Accurate Credit Transactions (FACT) Act of 2003. It requires certain businesses and organizations to develop a written program to detect the warning signs—or "red flags"—of identity theft.

Each identity theft program must include policies and procedures to address the four basic requirements:

- Identify relevant red flags.
- Detect red flags.
- Prevent and mitigate identity theft.
- Review and update the program.

Generally speaking, the rule applies to businesses and organizations that provide products or services and bill customers later. This includes any school that provides or accepts financial aid.

The FTC has developed a microsite which contains general information about the Red Flags Rule, including a guide on what kinds of businesses are affected by the rule.

You can visit the site at: ftc.gov/bcp/edu/microsites/redflagsrule/index.shtml.

Complying With Data Security Standards

Because data security ultimately affects almost all departments at your school, it needs to be more than just an IT function to be truly successful. By asking for input from staff across all areas of campus, you're more likely to secure their buy-in and support when it comes to implementing changes.

Begin by creating a data security committee, with members from each vital department such as IT, administration, educators, and health staff as well as representatives from your library, lunchroom, and even your board. The committee will be responsible for researching the issues surrounding data security at your school and implementing a plan of action to address these issues.

Centralize your payment systems

The committee's next point of business should be to determine all areas within the school that process payments of any kind—credit and debit cards, checks, and even cash. Once the list is compiled, it should make a decision about whether or not these payments should be centralized into a single system. Centralizing your payment systems is a key component to data security, making it easier to limit the number of applications that touch payment data and ensure PCI compliance.

Create a plan and assign responsibilities

The committee can now move on to creating a detailed plan for reaching full compliance with each of the necessary standards. Here are some simple steps to get started:

1. Review the complete rules and standards for each regulation.
2. Note which regulations apply to your school's current business practices.
3. Decide upon the steps needed to reach compliance for each applicable regulation.
4. Assign responsibilities.
5. Schedule regular meetings to regroup and review the regulations, making changes as necessary.

Develop an Acceptable Use Policy (AUP)

If your school doesn't already have an acceptable use policy (AUP), your committee should start by developing one. Your AUP needs to:

- Identify a strategy for promoting safe Internet use.
- Define acceptable and unacceptable usage of the Internet.
- Indicate the consequences for violating the policy.

An often overlooked part of developing an AUP is how it will be enforced and by whom, so be sure the committee covers these subjects in the planning process.

Find the Regulations Online

PCI – pcisecuritystandards.org
NACHA – nacha.org
Red Flags – ftc.gov/bcp/edu/microsites/redflagsrule/index.shtml
FERPA – ed.gov/policy/gen/guid/fpco/ferpa/index.html
HIPAA – www.hhs.gov/ocr/privacy

Offering Protection From Identity Theft

Ensuring proper data security at your school is not an easy process to be accomplished overnight. But it's imperative to protect your students, their families, your employees, and your school from attack by identity thieves.

Even as budgets remain tight, spending the time and resources to achieve compliance can be far less expensive than the potential costs of noncompliance. Suffering a single security breach can have numerous negative results such as legal costs and fines, loss of the right to accept credit and debit card payments, and—probably the most costly—a badly damaged public reputation.

With a little hard work and proper planning, your school can help deter thieves who are looking for their next identity theft victims.

FACTS Can Take the Worry Out of Your Data Security

Achieve compliance quickly and easily by centralizing your school's payment systems with FACTS Management. Our secure payment system is:

- SSAE-16 Type II Audited
- Red Flags Rule compliant.
- PCI DSS level one compliant.
- NACHA compliant

Contact FACTS today to find out how we can help.