

Analytics

|

🕒 6 MIN READ

📰 NEWS

Many Retailers Will Not Make PCI Compliance Deadline

Problems with applications, access management leave credit card processors facing fines - and vulnerabilities



Tim Wilson, Editor in Chief, Dark Reading
[Contributor](#)

September 26, 2007



With the compliance deadline just four days away, many retail merchants are still trying to climb over high hurdles in the Payment Card Industry (PCI) security requirements -- and figuring out what will happen if they can't make it in time.

The PCI Data Security Standard (PCI DSS), a set of security requirements for retailers and other businesses that process credit cards, is mandated by the major credit card companies, including Visa and MasterCard. If companies don't comply, they may be subject to fines, or they may even have their ability to process credit cards revoked.

Despite the threats of fines and penalties, however, it looks as though many retailers are about to miss yet another PCI compliance deadline. Experts estimate that more than a third of Level 1 merchants -- the largest retailers -- will fall short. Smaller retailers generally are even further away.

"Sixty percent of the respondents in the U.S. and the U.K. will plan to be fully compliant in the next year, while 51 percent of companies in Germany and 40 percent of companies in Spain and France are planning to take more than one year to comply with PCI," says Forrester Research in an RSA-sponsored [study](#) of the largest merchants published earlier this week. "Twenty-two percent of the global respondents plan to take at least two years or more before becoming fully PCI compliant."

In a separate study of 60 recent PCI audits at 50 major companies, security vendor VeriSign found that some 53 percent of organizations failed at least one of PCI's 230 requirements. That's an improvement over last year's study, in which 73 percent of companies failed the audit, VeriSign says.

If they don't make it by Sept. 30, it will be the third time the stragglers will have missed a PCI compliance deadline. The credit card companies had originally mandated compliance by June 2005. The deadline was stretched to 2006, and then the deadline for the revised PCI 1.1 was extended to Sept. 30 of this year. (See [Retailers Lag on Security Standard](#).)

So what's taking so long? Experts differ on which is the largest obstacle, but three elements consistently come up in all of the conversations: access management, application security, and encryption.

More than a quarter of companies are still struggling with the process of classifying credit card data and finding a secure place to store it, which means they still have a lot of work to do on access control, Forrester observes. Another 25 percent said developing effective policies and procedures for access control is their biggest sticking point. Twenty percent said implementing proper access control technologies is a chief hurdle.

But application security was one of the chief topics discussed last week at a meeting of the PCI Security Standards Council, which attracted more than 300 IT and compliance officers at major companies to Toronto.

"One of the biggest questions was whether companies should do detailed code review or put in an application firewall," said Joe Lindstrom, senior director of compliance consulting at Symantec, who was a panelist at the meeting. "The standard says you must do either one, but it doesn't require you to do both, so a lot of companies are struggling with what to do there."

Computer forensics experts at the Council meeting testified that as many as 60 percent of the breaches they have investigated in PCI environments can be traced to flaws in five or six retail applications, Lindstrom reported. "They didn't want to give out the names of those apps, but they are mostly payment processing applications that are specific to the retail environment."

Encryption, cited often last year, also continues to be among the most difficult technical obstacles to PCI. Twenty-seven percent of respondents to the Forrester survey said data encryption is the most challenging area of PCI compliance -- approximately the same number of respondents that cited identity and access management. A key element here is the wireless environment, where WEP continues to be the dominant technology despite its proven hackability, experts observe.

But while many large U.S. merchants and payment processors struggle with these technical issues, credit card companies are likely more worried about smaller retailers and non-U.S. regions that are not nearly as far along as their Level 1 counterparts. For many of these companies, the problem is not technology, but resources.

"The forensics people we heard from said that more than 80 percent of the [credit card] compromises they see are coming from merchants who are at Level 4 -- the smallest retailers," said Lindstrom. "This is where the least [PCI compliance] work has been done."

The forensics experts also confirmed the RSA study's suggestion that other regions are falling behind the U.S. in PCI compliance. "The reports are that there is actually a dropoff in compromises in North America, but that's being offset by growth in Europe and Asia," Lindstrom said. The data is becoming more difficult to track because criminals are now using anti-forensics tools and other methods to better cover their tracks, he said.

With so many companies struggling to meet the PCI requirements, vendors are turning out in droves to launch PCI compliance management tools and PCI-compliant products. ArcSight, Astaro, Shavlik Technologies, and many other companies have launched PCI tools in the last few weeks, and the PCI Security Vendor Alliance has released a free [tool](#) that aids with PCI risk assessment.

Despite all these tools, however, many companies will not achieve PCI compliance in time for Sept. 30. So what will happen to them? Experts observe that many Level 1 merchants already are paying fines -- and, in some cases, paying higher processing fees -- as a result of missing previous deadlines. In other cases, the fines are being absorbed by banks or financial institutions who want to keep their best credit card merchants online.

"Some merchants have looked at it and determined that the cost of coming into compliance would be higher than the cost of the fines, so they've elected not to do anything," Lindstrom observes. "Those are the ones that likely will begin to see fines being leveled against them." In those cases, financial institutions may decide to pass the costs of the fines on to the retail merchants who aren't compliant, he says.

But such punitive actions don't help improve overall credit card security, which remains at risk despite three years of PCI deadlines.

"Merchants typically keep too much [credit card] data," the Forrester report says. Eighty-one percent retain credit card data. Seventy-three percent store expiration dates, and 71 percent store verification codes. Fifty-seven percent store magnetic card stripe data. Many companies store the data in order to help identify customers or do business analysis, but under PCI, they are not supposed to be storing any of this data for more than a few weeks.

If retailers don't toe the PCI line more carefully in the future, however, the law may step in, experts say. The state of Minnesota already has passed legislation outlawing the storage of credit card data. (See [Cyber Law Cuts Two Ways](#).)

Have a comment on this story? Please click "Discuss" below. If you'd like to contact Dark Reading's editors directly, [send us a message](#).

- [ArcSight Inc.](#)
- [Astaro Corp.](#)
- [RSA Security Inc.](#) (Nasdaq: EMC)
- [Shavlik Technologies](#)
- [Symantec Corp.](#) (Nasdaq: SYMC)

[Vulnerabilities/Threats](#) [Risk](#) [Attacks/Breaches](#) [Application Security](#) [Compliance](#)

Keep up with the latest cybersecurity threats, newly-discovered vulnerabilities, data breach information, and emerging trends. Delivered daily or weekly right to your email inbox.

[Subscribe](#)

Editors' Choice

Rackspace Sunsets Email Service Downed in Ransomware Attack

Kelly Jackson Higgins 2, Editor-in-Chief, Dark Reading

Five Guys Data Breach Puts HR Data Under a Heat Lamp

Tara Seals, Managing Editor, News, Dark Reading

Beyond the Obvious: The Boldest Cybersecurity Predictions for 2023

Tara Seals, Managing Editor, News, Dark Reading

API Security Is the New Black

Jonathan Care, Contributing Writer, Dark Reading

Webinars

-  Zero Trust Security 101: What You Need to Know Before Getting Started
-  Detecting, Analyzing, and Mitigating Targeted Attacks
-  The Craziest Cyberattacks Seen In the Wild and How You Can Avoid Them
-  A Roadmap to Zero Trust: Steps for Meaningful Progress Amongst the Hype
-  Every DDoS Resilience and Response Playbook Should Include These Things

More Webinars

Reports

-  10 Hot Talks From Black Hat USA 2022
-  The Promise and Reality of Cloud Security
-  How Machine Learning, AI & Deep Learning Improve Cybersecurity
-  Enterprise Cybersecurity Plans in a Post-Pandemic World
-  Increased Cooperation Between Access Brokers, Ransomware Operators Reviewed

More Reports

White Papers

-  How Machine Learning, AI & Deep Learning Improve Cybersecurity
-  Ransomware Resilience and Response: The Next-Generation
-  Ransomware Is On The Rise
-  State of Ransomware Readiness: Facing the Reality Gap
-  How Hybrid Work Fuels Ransomware Attacks

More White Papers

Events

-  Black Hat USA - August 5-10 - Learn More

 [Black Hat Asia - May 9-12 - Learn More](#)

 [\[FREE Virtual Event\] The Identity Crisis](#)

[More Events](#)

More Insights

White Papers

- [How Machine Learning, AI & Deep Learning Improve Cybersecurity](#)
- [Ransomware Resilience and Response: The Next-Generation](#)

[More White Papers](#)

Webinars

- [Zero Trust Security 101: What You Need to Know Before Getting Started](#)
- [Detecting, Analyzing, and Mitigating Targeted Attacks](#)

[More Webinars](#)

Reports

- [10 Hot Talks From Black Hat USA 2022](#)
- [The Promise and Reality of Cloud Security](#)

[More Reports](#)

Discover More From Informa Tech

[Interop](#)

[InformationWeek](#)

[Network Computing](#)

[ITPro Today](#)

[Data Center Knowledge](#)

[Black Hat](#)

[Omdia](#)

Working With Us

[About Us](#)

[Advertise](#)

[Reprints](#)

Follow Dark Reading On Social

[!\[\]\(850829aa965caa4dea435b1dbd2b01c2_img.jpg\)](#) [!\[\]\(3344821a4a4db2b1bf08ab78880bd4b9_img.jpg\)](#) [!\[\]\(c55f79df16a3f273c8c7bf3e80113e52_img.jpg\)](#) [!\[\]\(bd42759b50f88bd068b0963f68dd8750_img.jpg\)](#) [!\[\]\(cbc7908f1ae0bf9d5ef78c8d1cdefcc5_img.jpg\)](#)