SPONSORED BY

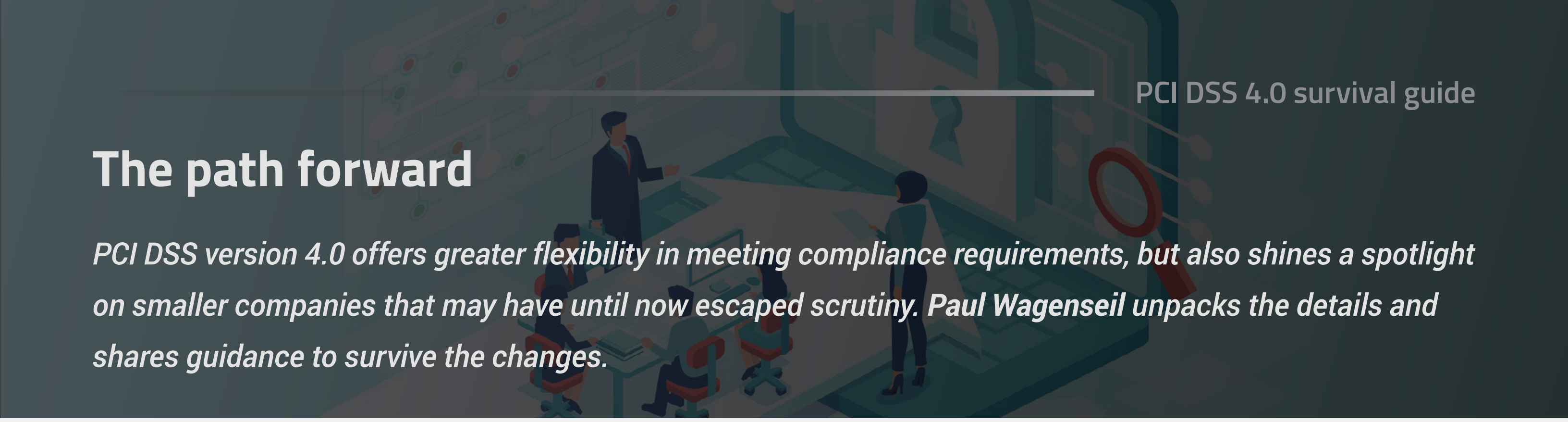
CLONE SYSTEMS®

PCI DSS 4.0 survival guide:

What you need to achieve full compliance

SC MEDIA CRA | Business Intelligence

Survival Guide
An SC Media publication



The path forward

PCI DSS version 4.0 offers greater flexibility in meeting compliance requirements, but also shines a spotlight on smaller companies that may have until now escaped scrutiny. ***Paul Wagenseil*** *unpacks the details and shares guidance to survive the changes.*

OUR EXPERTS:

Elyse Hamilton
Director, Customer Growth,
Clone Systems

Tom Nianios
Senior Security Engineer,
Clone Systems

Jorja Solomon
Senior Growth Manager,
Clone Systems

Gerald Beuchelt
CISO, Sprinklr

Norman Comstock
Managing Director,
UHY Consulting

Get ready! The new version of the Payment Card Industry Data Security Standard, PCI DSS 4.0, is about to go into effect. It applies to all merchants and service providers who accept credit and payment cards, online or off.

"PCI-DSS 4.0 is a major evolution of the standard, bringing it much closer to addressing the threats we are experiencing today," explains Gerald Beuchelt, CISO at Sprinklr, a customer-management-platform maker based in New York.

The first phase of PCI DSS 4.0 must be implemented by March 31, 2024. It includes 13 major changes from PCI DSS 3.2.1, most of which have to do with defining roles and responsibilities for teams dedicated to protecting cardholder data.

A further 51 changes, mainly technical, must be implemented as part of the second phase of PCI DSS 4.0 a year later, by March 31, 2025.

What's set to change with PCI DSS 4.0

The changes to PCI DSS are substantial. There are wider options for compliance, including the ability to create customized controls or borrow them from other compliance frameworks, and tougher requirements for password length, multi-factor authentication, encryption, and verifying the integrity of online payment pages, among other factors.

But there will also be an increased focus on compliance by smaller merchants, many of whom may have until now relied on their payment-card processors to vouch for them.

For example, restaurants, auto-repair shops and medical practices not affiliated with larger organizations may soon need to perform quarterly network vulnerability scans performed by PCI-certified approved scanning vendors (ASVs), a procedure that was not always necessary for smaller organizations.

“Many of the requirements that were implied in the past editions of PCI DSS are now explicit,” says Ciske van Oosten, Head of Global Business Intelligence, Cyber Security Consulting, Verizon, in an August webinar.

These changes may lead to confusion among merchants and assessors, similar to the confusion felt in the early days of PCI DSS nearly 20 years ago. Back then, many retailers weren't sure how to implement the new standard or verify that they were complying.

"I really feel that with [version 4.0], it's just going to go back to where PCI started out," says Elyse Hamilton, Director of Customer Growth at Clone Systems, a managed service provider and ASV in Philadelphia. "I think it's going to be very eye-opening for everyone."

Here's a breakdown of what's new in PCI DSS 4.0, why the changes are being made, how they might impact your organization and what needs to be done to comply with each phase.

History of PCI DSS

This is the first revision of PCI DSS since version 3.2.1, implemented in 2018. The last major full-point overhaul was to version 3.0 in 2014.

That was before the United States began the transition to EMV "chip" payment cards, before the bulk of credit-card theft moved online, and before many current regulations that govern online data came into effect.

The PCI DSS standard applies worldwide and is not enforced by law in most jurisdictions, but companies must comply to be able to accept payment cards.

Compliance involves meeting 12 general requirements, including using a firewall and antivirus software, encrypting data, restricting digital and physical access to cardholder data, testing network security, managing vulnerabilities and risk, and creating and adhering to an information-security policy. Those general requirements have not changed for PCI DSS 4.0, but many of their particulars — the specific "defined" requirements — have been beefed up.

The standard is governed by the Payment Card Industry Security Standards Council (PCI SSC). Merchants and other credit-card acceptors are put into four major categories, depending on the number of payment-card transactions each organization processes annually.

MasterCard and Visa define Level 1 organizations as those that process more than six million transactions per year; Level 2, between one and six million transactions; Level 3, between 20,000 and one million e-commerce transactions; and Level 4, fewer than 20,000 e-commerce transactions and up to one million offline transactions annually.

Discover follows the MasterCard and Visa definitions for Levels 1 and 2, defines Level 3 as up to one million transactions of any sort and does not use Level 4. American Express uses lower thresholds for each of the four levels, while JCB uses only Levels 1 and 2 with one million transactions as the dividing line.

Each Level 1 company must have its cardholder data environment (CDE), defined as any part of the company network that touches payment-card data, audited every year by either an external Qualified Security Assessor (QSA) or an on-staff Internal Security Assessor (ISA). Both QSAs and ISAs must be certified by the PCI SSC. Level 1 organizations must also have quarterly vulnerability scans of their CDEs done by external ASVs.

Companies at Levels 2, 3 and 4 generally do not have to be audited and can instead provide yearly Self-Assessment Questionnaires (SAQs) that document how they comply with PCI DSS. Depending on the brands of payment cards accepted (American Express, Discover, JCB, MasterCard or Visa), organizations at these levels may or may not have to do quarterly ASV scans — but it appears that more may have to for compliance with PCI DSS 4.0.

> ***"Smaller organizations now are going to have to do those PCI scans on behalf of themselves and not just rely on the processors saying that they're compliant."***
>
> — Elyse Hamilton | *Director, Customer Growth, Clone Systems*

Organizations that fail compliance won't necessarily have their ability to accept credit cards revoked right away, especially if they have shown good-faith efforts. More likely, a company will work with a QSA and the PCI SSC to get itself back up to compliance, with the stipulation that it submit to more frequent assessments and vulnerability scans for a period.

"It's not like you immediately get cut off," says Tom Nianios, Senior Security Engineer at Clone Systems. "Are you doing scans? Did you have a firewall? Did you look at the logs once a month? If you can prove stuff like that, you're adhering to the majority of the compliance requirements."

PCI DSS 4.0 puts more emphasis on compliance by smaller organizations

For the past several years, the PCI SSC has been focused on compliance among Level 1 merchants. That makes sense. As Nianios explained, a major online retailer will process tens of millions of transactions annually while a neighborhood corner store may do only a few thousand.

But with PCI DSS 4.0, the enforcement body is giving larger merchants more flexibility while expanding its attention to the smaller merchants in Levels 2 through 4, which are seeing more credit-card thefts and data breaches than they used to.

The 4.0 standard is going to focus more on the lower levels as well, says Nianios. Now, they must comply because more breaches are happening down below than they are happening up high.

Until now, many of those smaller merchants have been able to rely on their payment-card processors for PCI DSS certification. For example, a merchant that uses a third party to process credit cards may not have had to fill out an SAQ, and likely wouldn't have had to submit to an ASV scan, as its card processor would often vouch for the merchant.

"Companies were told by their payment processors, 'Hey, since you use us, you guys are PCI compliant, you're covered, you don't have to worry about doing scans,'" says Hamilton.

That will change, she says. "Those smaller organizations now are going to have to do those PCI scans on behalf of themselves and not just rely on the processor saying that they're compliant."

Because most credit-card theft now takes place online, the initial focus may be on small or medium-sized merchants who conduct e-commerce, Hamilton says, although physical stores will get their turn.

"They're probably not going to be as strict with those brick-and-mortars in the beginning," she says. "I feel like they're really going to be tackling more of the online stuff."

Even for Level 1 organizations, the PCI SSC will require more documentation and authentication for vulnerability scans and may be less receptive to self-reported scan results.

"Internal vulnerability scans will now have to be authenticated scans," says Norman Comstock, Managing Director at UHY Consulting. "Scan inventory will now be deeper and more inclusive, which will likely lead to many false positives that should be verified by both entity and assessor."

Custom controls can relieve the burden of compliance

Another significant change with PCI DSS 4.0 is the ability to create custom controls, or to borrow controls from other regulatory standards and frameworks. The only stipulations are that those substituted controls match the impact and intent of the defined PCI controls they replace, and that each substitution is documented, analyzed for risk and approved by a QSA or ISA.

PCI DSS controls are detailed, granular requirements — officially, Defined Approach Requirements — that specify what must be done to protect particular aspects of the cardholder data environment.

> ***"It's not like you immediately get cut off [if you fail an assessment]. Are you doing scans? Did you have a firewall? Did you look at the logs once a month? If you can prove stuff like that, you're adhering to the majority of the compliance requirements."***
>
> — Tom Nianios | *Senior Security Engineer, Clone Systems*

For example, a password-length requirement for staffers able to access cardholder data would be one control (PCI DSS Defined Approach Requirement 8.3.6). Mandating that those passwords change at set intervals of time would be another control (PCI DSS Defined Approach Requirement 8.3.9).

Because large organizations and enterprises often have complicated internal environments, adhering strictly to defined PCI DSS controls might mean restructuring their systems just to satisfy bureaucratic requirements. With version 4.0, the PCI SSC is recognizing that there's more than one way to reach compliance.

Furthermore, controls for other major digital-data regulations, such as the General Data Protection Regulation (GDPR), the California Consumer Privacy Act/California Privacy Rights Act (CCPA/CPRA), the Health Insurance Portability and Accountability Act (HIPAA) and the System and Organization Controls Type 2 (SOC 2), often overlap heavily with PCI DSS controls.

Version 4.0 lets organizations substitute other regulations' controls for PCI DSS ones, as long as the same goal is achieved. A HIPAA control that mandates passwords of a certain length could replace a PCI DSS one if the HIPAA control matches or exceeds the PCI DSS control's requirements.

Custom controls may not be for everyone. Smaller organizations in particular might not have the personnel or expertise to "roll their own" controls, and they would likely comply with few other regulatory frameworks whose controls could be repurposed. Those companies would do best by sticking to the PCI DSS defined controls and the compliance templates designed to work with them.

"In smaller organizations, I suggest they go with templatized stuff, just like with anything else they would do," says Clone Systems' Nianios. "Follow what's already written, what's been used all these years, because that will help you achieve the compliance level that you need to achieve."

Maintaining compliance throughout the year

Nianios points out that PCI DSS 4.0 also puts greater emphasis on continuous compliance, perhaps in an attempt to deter organizations from catching up with the standard only in the weeks leading up to a scheduled assessment.

"What does that mean? Obviously, it means educating [staffers] on a continuous basis," he says, adding that merchants will also have to be more diligent about monitoring data. "Are you reviewing log data? Yes? Now, you're going to have to be a little more precise on how you're doing it, who's doing it, what the process is, all that stuff."

As mentioned earlier, all these changes may lead to a lot of head-scratching and anxiety among merchants who find that they've suddenly got to do a lot more to achieve compliance.

"My husband and I owned a restaurant at the time" of the initial PCI rollout in 2004-2005, says Clone Systems' Hamilton. "We accepted credit cards, and we were very confused ourselves. I think we're going to see that again next year."

It doesn't help that there's a perceived lack of clarity about the upcoming changes, with some defined requirements seeming deliberately vague and classified in the PCI DSS Summary of Changes as "clarification or guidance."

Planning the transition to PCI DSS 4.0

With all this complexity and fuzziness, some organizations may be tempted to ignore the March 31, 2024, deadline and instead wait until their next assessments to reach compliance with Phase I of PCI DSS 4.0.

> ***"The biggest thing is just understanding what your responsibilities are. Do I need to do quarterly scans myself now? Can I rely on someone else to do it? Do I need to do extra testing?"***
>
> — Elyse Hamilton | *Director, Customer Growth, Clone Systems*

You might get away with that if you don't suffer any major security incident in the meantime and find yourself audited as a result. Being caught out of compliance past the deadline opens you up to fines, litigation and even revocation of your card-acceptance privileges.

Implementing Phase 1 of PCI DSS 4.0

1

Determine your compliance level and responsibilities

- "The biggest thing is just understanding what your responsibilities are, " says Hamilton, including knowing in which compliance level your organization lies.
- Questions that Hamilton suggests to ask:
    - Do I need to do quarterly scans myself now?
    - Can I rely on someone else to do it?
    - Do I need to do extra testing?

2

Determine the scope of your cardholder data environment

- The scope of those systems that PCI DSS applies to, otherwise known as your cardholder data environment (CDE), must be defined. How many parts of your network does cardholder data touch? Is it possible to segment the network to limit the scope of the CDE, and hence the impact of PCI DSS compliance upon your organization?
- "Scope is everything," says Comstock. "Under PCI DSS 4.0, both the entity and the assessor share the burden of validating scope. Furthermore, the new 12.5 [PCI DSS] requirement has formalized scoping reviews as part of the entity's annual assessment."
- If you're not sure exactly what the scope of your CDE is, consider bringing in external security consultants to perform a penetration test on your network.
- Don't limit the pen test to just those areas you know are part of the CDE. Instead, make sure that all systems, whether directly connected or not to the known CDE, are within the pen-tester's scope. Otherwise, hidden connections may escape detection.

3

Perform a gap assessment

- You'll probably next need to conduct a gap assessment, or a more thorough readiness assessment, in which you scrutinize your own CDE and measure how close it is to the PCI DSS requirements — and then map out what it would take to meet the requirements.
- "Once you understand the version 4.0 requirements, map them against your current security controls and analyze the impact the changes may have on your organization," writes PCI SSC Senior Manager of Corporate Communications Lindsay Goodspeed in a recent official blog post.

4

Enlist third parties to help

- Unless you're part of a large, well-resourced organization, you will probably need to enlist third-party cybersecurity and governance, risk and compliance (GRC) consultants to help with the transition. Don't delay in reaching out to them, as they may be booked up as the deadline for Phase I approaches. "Any organization without specialists in designing, implementation, maintaining, and documenting security controls will need to ensure that they have access to such expertise within the next few months," says Beuchelt. "Given the market for cybersecurity talent, this can become a major difficulty."
- If you decide to employ a third party to assist with long-term PCI DSS compliance, as you might with a managed service provider (MSP) or a managed security service provider (MSSP), then that entity will probably be classified by the PCI SSC as a Third-Party Service Provider (TPSP) and you will need to define the service provider's roles and responsibilities along with those of your own staffers in Phase I of the transition.

5

Set aside a budget for the PCI DSS transition

- Moving to PCI DSS 4.0 may cost more than you anticipate, especially when you factor in the potential costs of hiring outside consultants and pen testers and of having an ASV perform external vulnerability scans. "People need to do these additional tests," says Jorja Solomon, Senior Growth Manager at Clone Systems. "Find the budget and allocate the funds, because it's important. You need to invest before something happens, because there will be higher costs later down the line."
- "[Smaller merchants] just might not have that allocated towards their budget and not understand that it's going to be a need, and not just a wish, a nice-to-have," adds Hamilton.

Implementing Phase I of the PCI DSS 4.0 transition

Perhaps mercifully, PCI DSS 4.0 has only 13 new or changed defined requirements that need to be in place by March 31, 2024. The other 51 changes take effect a year later. You can get details of all 64 changes, including a chart that highlights which are in which phase, from the PCI SSC website.

Ten of those 13 Phase I defined requirements state simply that "Roles and responsibilities for performing activities in [one of the 12 general requirements] are documented, assigned, and understood."

An eleventh defined requirement, as mentioned above, mandates that a third-party service provider (TPSP), such as an MSP, MSSP, data-backup service or payment processor, "support customers' requests to provide PCI DSS compliance status and information about PCI DSS requirements that are the responsibility of the TPSP."

> ***"Any organization without specialists in designing, implementing, maintaining, and documenting security controls will need to ensure that they have access to such expertise within the next few months. Given the market for cybersecurity talent, this can become a major difficulty."***
>
> — Gerald Beuchelt | *Chief Information Security Officer, Sprinklr*

This means that specific individuals within an organization, or in an affiliated TPSP, need to be designated as having specific tasks and duties with relation to PCI DSS compliance long before there's an incident that forces them to spring into action. The PCI SSC is essentially telling companies to name their starting lineups before a game.

"I think it is an efficient manner to understand named personnel that may be interviewed by the assessor," says Comstock. "The standard formalizes many of the policies and procedures, roles and responsibilities, and other expectations an assessor will examine. Having these documented by the entity bolsters that words can be actioned by named staff who know and operate those control requirements."

The two-stage phase-in also gives companies, even small ones, a year to adopt the culture of security and compliance best practices before the more technical PCI DSS requirements take effect in March 2025.

"They did it in that order because if [the PCI] forced technical on [smaller merchants], they would have been lost on day one," says Nianios. "Whereas if they have time to educate themselves, learn about the standard, learn about their responsibilities and so forth, know the operational stuff first, then the technical stuff can follow after that and it won't be a huge surprise for them."

The last two of the initial 13 new or changed defined requirements likewise lay the groundwork for Phase II. The first has to do with documenting and confirming PCI DSS scope, which now must be done yearly. The second mandates that if custom or borrowed controls are to be substituted for defined PCI DSS ones, a risk analysis be done for each substitution every year.

"Now is the time to start implementing and validating the organizational changes necessary for this change," says Beuchelt. "It may be advisable to hire a fractional (or 'virtual') CISO during the transition time. This would ensure a more holistic approach to defining a program than hiring just for some gap remediations."

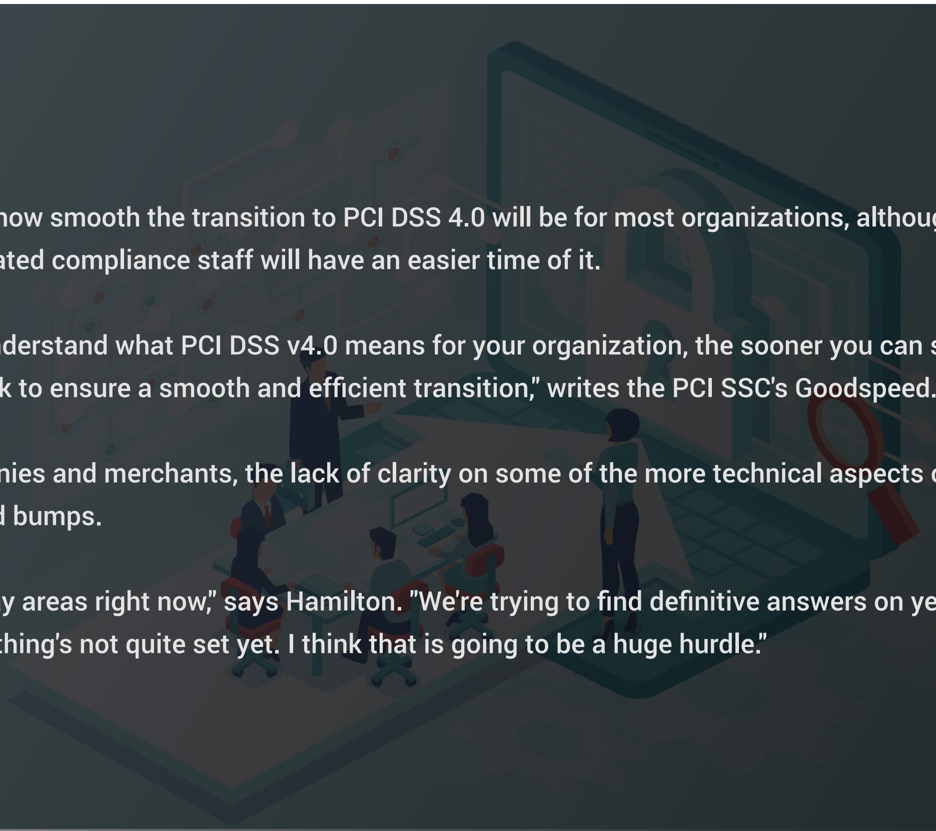
In a blog post, the PCI SSC itself recommends that the transition plan be communicated "across all departments and functions, ensuring that everyone knows their role and what to expect."

It adds that training sessions should be held to educate staffers on how to maintain compliance with the PCI DSS standard — part of the continuous education and monitoring that Nianios mentioned earlier.

Implementing Phase II of PCI DSS 4.0

The technical aspects of the second phase of the PCI DSS 4.0 transition will likely necessitate the use of external auditors for all but the largest organizations, who can use an internal ISA but will not be exempt from external vulnerability scans by an ASV every quarter.

- "QSAs will be your go-to, and definitely QSAs that have a partnership with an ASV, " says Hamilton.
- "If you have well-known QSAs with the scanning tools at their fingertips, that will help people expedite the process," she adds.
- Organizations can also use automated tools or programs to help meet Phase II requirements, as Nianios explains. "There are organizations that supply templates to everything, for every single compliance requirement out there," he says. "Smaller organizations are better off poised to utilize the templates and the information that already exists, versus having to recreate all that stuff from scratch."
- There are also new requirements for verifying the integrity of online-payment web pages. Requirement 6.4.3 states that payment-page automated scripts be authorized, verified and inventoried, along with "written justification as to why each [script] is necessary."
- Requirement 11.6.1 mandates that "change- and tamper-detection mechanism" be implemented on all payment pages to watch for unauthorized modifications of payment-page content and HTTP headers.



Conclusion

We don't yet know how smooth the transition to PCI DSS 4.0 will be for most organizations, although it's likely that larger entities with dedicated compliance staff will have an easier time of it.

"The sooner you understand what PCI DSS v4.0 means for your organization, the sooner you can start planning and prioritizing the work to ensure a smooth and efficient transition," writes the PCI SSC's Goodspeed.

For smaller companies and merchants, the lack of clarity on some of the more technical aspects of PCI DSS 4.0 may lead to some speed bumps.

"There's a lot of gray areas right now," says Hamilton. "We're trying to find definitive answers on yes-or-no questions, and it seems like everything's not quite set yet. I think that is going to be a huge hurdle."

SPONSORED BY

CLONE SYSTEMS®

Embrace Compliance. Change the World.

Compliance is a reality. If you embrace it, your company will run smoother. Clone Systems transforms red tape and constant changes into a complete offering including PCI Compliance, Penetration Testing and our proprietary SIEM and Managed SOC-as-a-Service, helping you conquer the regulatory demons with ease.

MASTHEAD

EDITORIAL

SVP OF AUDIENCE CONTENT STRATEGY

Bill Brenner | bill.brenner@cyberriskalliance.com

SALES

CHIEF REVENUE OFFICER

Dave Kaye | dave.kaye@cyberriskalliance.com

DIRECTOR, STRATEGIC ACCOUNTS

Michelle Guido | michelle.guido@cyberriskalliance.com

Don't sleep on PCI 4.0. Compliance

Take notice and get ahead with Clone Systems.

Are you ready for all of the changes looming right around the corner? PCI 4.0 is the latest version that introduces stricter requirements and advanced security measures.

We have successfully helped thousands and thousands of businesses world-wide achieve and maintain compliance, and we would welcome the opportunity to do the same for you.

Learn more now at **clone-systems.com**. It's fast and easy.

CLONE SYSTEMS®