

# RISK/Factor

Volume 3, Issue 2

May 2007

## In This Issue: The Best of Risk Factor

- Electronic Product Registration
- Identity Theft: RM's Problem
- The Status of 404 Compliance

### Plus:

Conference  
Calendar

Get  
Risk Management  
News as it Happens:  
Visit the **Risk  
Factor**  
Weblog!

[ldwpublishing.com](http://ldwpublishing.com)

Risk Factor  
is a publication of  
LDW Publishing  
Valley Forge, PA  
All rights reserved.

## Electronic Product Registration: A Nintendo Case Study

By Peter Junger

In retail, there's no bigger asset than the products you sell. Every year, retailers and manufacturers lose billions of dollars due to product returns, fraud and shrinkage. For manufacturers and retailers, there's nothing more important than protecting those assets through every means possible: by better inventory management, and active loss prevention and asset recovery procedures.

Gaming giant Nintendo of America, Inc. decided to address this issue to give themselves, and their retailers, a better system to control their costs and increase their profitability.

### POS Electronic Registration – Its Origins

As the popularity of electronic gaming systems grew throughout the 1990s, Nintendo realized that its profitability was being greatly impacted by the number of product returns that retailers were accepting.

"We were concerned at the number of products being returned, and how it was affecting our bottom line," said Perrin Kaplan, Nintendo's vice president of marketing and corporate affairs. "But what was more concerning was that when we took a close look at the returns, we realized that it was not a product quality issue. It had more to do with our retailers not having the tools to enforce return guidelines and their inability to detect fraud."

So in an effort to reduce fraudulent and ineligible returns, and to create visibility to the full product logistics lifecycle, Nintendo developed a methodology that would give their retailers a foolproof system to track individual products throughout their lifecycle. This system was designed to ensure that everyone in the product chain – manufacturers, retailers, and consumers – was being treated equitably and properly.

The system developed and patented, *POS Electronic Registration*, includes proprietary methodologies, such as vendor product registration, trending and analysis, and exception reporting and alerts, which would enable the company and its retailers to track individual products by their serial number from their moment of purchase.

### How It Works

POS Electronic Registration employs the combination of a product's UPC number with its serial number to establish a unique identifier, or "fingerprint," for each individual product. When a product's unique iden-

*(Continued from page 1)*

tifier is scanned, either manually or via RFID, the information is transmitted to a central database, where it is stored with the retailer's transaction information.

To protect the privacy of the consumer, the transaction data is logged without recording any customer information. But when this product fingerprint information is established and recorded, the retailer and manufacturer have an identifiable date of purchase, from which the start of the warranty and return periods can be tracked.

When a product is returned, the retailer has only to scan the unique fingerprint on the product (currently the UPC and serial numbers) to find out if the product is eligible. If the product falls within the warranty and return policy guidelines, the clerk simply accepts the product and issues the appropriate credit or refund. If it does not meet the guidelines, the clerk can easily show the customer why it is ineligible.

The system is as flexible as the retailer wants it to be, but in all cases creating a streamlined process. Because product warranty and return policies for each product are programmed into the system, completely automating the process, clerks need little training. When the product is scanned, the system does a real-time query on the central database, which feeds back instructions based on the retailer's return policy. The system can be designed to display a list of accessories that should accompany the product being returned. If the product needs repair, the system can also be programmed to give the customer a list of local and manufacturer-approved repair facilities.

In the case of major holidays where purchasing may happen well in advance of when the gift is given, the system can be instructed at the client's request to "start the clock" for warranties and return eligibility terms on popular products on select dates rather than on the date of purchase.

In each case where a product return is attempted, the activity is recorded in the product's transaction history. All of this data can then be readily accessed and analyzed by management.

Given these tools, Nintendo's retailers were able to reduce, even eliminate, returns of ineligible products. Said Kaplan, "Taking control of this process resulted in a 72 percent reduction in return rates. That's a huge number, and it represented a significant boost to the company's bottom line."

### **Sharing The Wealth**

Knowing that these controls would be of immense

benefit to other manufacturers and retailers, but also knowing that other manufacturers, especially competitors, might not want Nintendo having access to their sales and return data, Nintendo created a separate, independent and wholly owned subsidiary company: SIRAS.com.

"Having a strong, healthy base of retailers and manufacturers is important to the overall success of our industry," said Kaplan. "Sharing these tools throughout the industry was a way we could help in that effort."

POS Electronic Registration has been implemented by many of the world's consumer brands, including Sony Computer Entertainment of America, Nintendo, Hewlett Packard, Philips, RCA, Panasonic, as well as many retailers, such as Wal-Mart, Target, K-Mart, Toys R Us, Circuit City, and Best Buy. Actual data for clients is confidential, but, on average, clients have seen a reduction in return rates of 37 percent.

The return on investment (ROI) varies depending on product prices; the higher the price point, the greater the return. But across all categories, it is common for ROI rates to exceed 10:1.

### **Unforeseen Benefits**

While the financial benefits of reducing returns is quite obvious and quantifiable, POS Electronic Registration has delivered some unintended, yet valuable benefits for retailers, customers and law enforcement officials. Note that no customer personal transaction information is ever recorded, but by being able to supply product transaction data, retailers have been able to improve their customer service ratings by increasing the efficiency with which they have helped customers who have lost their receipts, forgotten where they originally purchased the product (or had it purchased for them), and, as previously mentioned, referred customers to nearby repair centers.

Customers have also benefited by having a virtual, electronic receipt validating a product's warranty entitlement. For manufacturers, it's resulted in a valuable tool used to track warranty eligibility and manage financial reserves. But an even broader application has been the system's ability to prevent retail fraud and to help track down and catch thieves.

The patented technology and transaction information have helped retailers track down customers who have attempted to alter, forge or swap serial numbers on products or on receipts. Also, the system has been used to help track down and recover stolen items. In cases such as the shoplifting of pre-registered items, the system is able to identify those that have bypassed POS regis-

ters. To aid in the recovery process, the system can be instructed to flag any of these pre-registered products for cross-retailer return attempts, and has also helped law enforcement officials by identifying specific products.

#### **Ramp Up Time**

As you might expect, implementing POS Electronic Registration system is not an overnight process for most companies. Manufacturers and retailers who want to take advantage of this technology must allow sufficient time for planning and implementation. For manufacturers, this might involve serialization changes to comply with registration standards, such as the labeling of both the product's UPC bar code *and* its serial number bar code on the outside of the packaging. With these standards in place the products can be scanned quickly and efficiently at the point of sale.

For the retailer, it means working with SIRAS' expert IT and client services teams to encode the retailer's POS system to prompt for the serial number

scan when the UPC of a participating product is entered, and then transmit the transaction data to the central database. Each product transaction file is appended with the appropriate manufacturer warranty information for each product, as well as the retailer's return policy guidelines.

#### **Future Applications**

While its initial applications have been in the registering of popular gaming and other consumer electronics products, POS Electronic Registration is not limited to these markets. In fact, it can be applied to any industry where tracking serial numbers can help eliminate the return of products that were stolen or whose warranties have expired or are not eligible for return for other reasons.

*Peter Junger is co-inventor of SIRAS' POS Electronic Registration system and holds several patents pertaining to this loss prevention technology.*

## **Computer-Removable Media :Quantifying and Managing an Emerging Threat**

*By John Rostern*

Tom appeared to be like any other employee: punctual, efficient and friendly. But Tom had serious financial problems and needed a way out. A friend told him that the customer credit card account information he worked with every day was very valuable and offered to pay \$5,000 for copies of that information. So one day, Tom arrived at work, removed a USB flash drive from his pocket and plugged it into his computer. He typed a few commands, then unplugged and pocketed the flash drive. He would repeat this process numerous times over the following months. Meanwhile, the information was sold and resold on the black market for many times the \$5,000 Tom was paid. The information was used to commit identity theft and credit fraud against consumers and retailers around the world.

Computer Removable Media (CRM) has become ubiquitous in both the consumer electronic marketplace and the modern office. The threat of information leakage associated with these devices has become tangible and demonstrable. Devices such as USB flash drives, digital music players and digital cameras are now recognized for posing significant security threats, yet most security managers admit to not actively monitoring or preventing their use. At the same time, most information security policies do not directly address these new technologies, which are capable of storing and transporting large amounts of data in a very small physical package. Consider that when the first consumer

flash drives appeared in 1999, their capacity was around 8MB. Today, a digital camera can easily store 4GB or more and an iPod holds up to 80GB of data. On the immediate horizon are smaller, faster devices with even greater capacities.

Increased legal and regulatory requirements such as the Data Protection Act and the Payment Card Industry's (PCI) Data Security Standard require organizations to exercise due care in safeguarding certain personal information. Comprehensive security measures have already been implemented by many financial institutions—in some cases locking down the use of USBs without authorization and/or monitoring in a bid to mitigate this growing risk.

An effective overall security architecture will incorporate a combination of technical and procedural elements to provide effective countermeasures to emerging threats posed by removable media. The rapid pace of technological change demands a security strategy that is both flexible and adaptable.

The following areas should be considered as ways to mitigate the threat posed by CRM:

**Policies & Procedures:** Manage the use of removable media and communicate the policy to all staff members. Policies and procedures should be part of the organization's overall security policy and be aligned with appropriate Human Resources policies.

**Awareness:** Employees who handle sensitive in-

formation should be made aware of the security implications of removable media. Creating a security-aware workforce will improve monitoring, oversight and compliance at the grass-roots level.

**Encryption:** Consider implementing strong encryption for both data in motion and data at rest. Centrally administered schemes based on a Public Key Infrastructure and/or digital certificates provide enterprise-level key management, and integration has been proven to be effective in medium to large organizations. Smaller organizations can take advantage of a number of commercial packages to provide similar functionality.

**Device Hardening:** Implement baseline security configurations at the operating system or hardware level that restrict or prohibit the use of devices such as USB flash drives. Disabling the USB port(s) at either the physical or logical level can provide an additional layer of security.

In order to build an effective security program that considers emerging threats such as CRM, IT auditors should have a complete understanding of relevant legal and regulatory considerations affecting their industry and organization. Regulations such as HIPAA, Sarbanes-Oxley and GLBA can serve to clearly delineate risk while at the same time providing guidance as to what steps must be taken to achieve compliance.

At the same time there is a constant need to

work closely with the IT department to map out where sensitive information is processed and stored. In order to determine the existence and effectiveness of controls it is vital to have an in depth understanding of how it is processed and stored. This information provides the basis for reviewing logical and physical security in addition to supporting risk analysis of various functional areas that interact with protected and/or sensitive information.

After the risk analysis has been completed, the organization may need to develop and implement additional procedures to restrict the presence of CRM devices in these areas. Procedures should support periodic audits and/or tests to ensure that the measures are in place and are functioning as intended.

The rate of change of technology will continue to present new control challenges. In an environment of increasing regulatory constraint, organizations must carefully assess and manage technology risk. However, the basic tenets of security and risk management—people, process and technology—continue to be relevant as the foundation for managing current and future risks.

*John Rostern is the Director of Technology Risk Management for the Jefferson Wells New York office. He can be reached at 212-823-8600, or via email at [john.rostern@jeffersonwells.com](mailto:john.rostern@jeffersonwells.com).*

---

## Managing Risks Related to Identity Theft

*by Guillaume Deybach*

The odds are that every risk manager knows someone who has had his or her identity stolen. Professionally, risk managers are beginning to spend more and more time addressing identity theft-related risks as the crime continues to grow in scope and significance.

The FBI calls identity theft “a significant and growing crime problem” and an “increasingly insidious and pervasive problem” that can threaten virtually any American. As for quantified measures, the FBI says identity theft “costs American businesses and consumers a reported \$50 billion a year” and “causes untold headaches for an estimated 10 million US victims annually.”

In light of the scope of the problem, the litigious environment in the US, and existing and emerging laws concerning corporate responsibility for the protection of personal data, corporate risk managers have begun pressing commercial entities to more actively protect the data of both customers and employees. A closer look at the personal impact of identity theft reveals why it is a growing concern among risk managers.

According to a recent insurance industry study, a

typical identity theft victim can lose thousands of dollars and, more alarmingly, will spend as many as 600 hours over the course of a year or so resolving issues related to a single theft.

Because the customer service required to help consumers resolve identity theft issues is generally not offered on a 24/7 basis, victims often must take time during their workdays to resolve issues, creating a risk link between identity theft and employee productivity. Productivity losses, however, are not the only concern.

### Where the Problem Starts

Personal information can be stolen via the Internet during online transactions. Identity theft can also occur when there is some kind of personal connection between the thieves and their victims. For employers, a more critical concern is when identity theft can be tied to the action of employees, which one recent study said accounted for some 16 percent of identity theft cases.

Perhaps the best known case involved the loss of up to 26 million personal records from the US Department of Veterans Affairs due to an employee im-

*(Continued from page 4)*

properly taking the records home on a laptop computer, which was stolen. Other cases involved the US Census Bureau, the National Oceanic and Atmospheric Administration (NOAA), Bank of America, Fidelity Investments, LexisNexis, and DSW Shoe Warehouse. When employees mishandle personal data and losses occur, employers are culpable.

### **Next Step: Government Action**

A Michigan case illustrates this culpability. Last year, Michigan became the first state to require by law that every employer establish a policy for keeping employee social security numbers secure. The law was passed at nearly the same time a Michigan appeals court allowed victims of identity theft to recover financial damages from organizations that did not adequately protect personal data that were subsequently used for identity theft. In the court case, a labor union employee took home documents showing union members' names and social security numbers; the employee's daughter stole the information and used it to engage in identity theft. The union was found legally and financially liable for the actions of its employee.

A number of other data-protection initiatives have been keeping legislators busy in Washington and in state capitals around the nation.

California was the first state to pass a data security breach notification law. Similar legislation was introduced in 31 states during 2006 and has already been enacted in at least 12 states. Washington is considering federal statutes that go beyond breach notification to reducing the risk of breaches and providing harsh penalties for intentional acts of identity theft.

### **The Corporate Impact**

All three branches of government, at the state and federal levels, are focused on identity theft, leading ultimately to increased statutory, regulatory, and legal pressure on corporations to protect personal data and protect their businesses from subsequent financial and productivity losses. Common tools include audits determining what employees have access to what data and why, stricter pre-employment background checks, document destruction policies and procedures, employee education programs, and more.

In addition, companies must manage productivity losses related to employees who themselves have become identity theft victims. Remember, 10 million Americans are said to become identity theft victims every year—some four percent of the general population. But with current numbers of chil-

dren, students, and retirees, 10 percent of the full-time workforce is probably a fair number.

Assume an employee strives to minimize work time spent on such matters, keeping it to just two hours per week for a total of 100 of the typical 600 hours needed. Against a 40-hour week and across a 50-week year (allowing for two weeks of vacation), this represents a five-percent productivity loss per affected employee with the very real possibility of one in 10 employees being affected.

The potential costs of these productivity losses can be staggering, especially when considered along with related regulatory compliance costs and potential legal liabilities. The risk manager may well be the executive called upon to mitigate the kinds of productivity losses discussed here.

### **Available Assistance**

Over the past few years, the risk management industry has developed insurance products that assist corporations in minimizing certain losses related to identity theft. For example, Worldwide Assistance's Data Breach Response Service helps corporations protect themselves, their customers, and their employees from the negative impact of breached data and identity theft. Should a breach occur, affected customers and/or employees can be notified in a timely manner through the service. The related ID Theft Resolution Services, often added to a company's package of employee benefits, helps victims quickly and easily recover from identity theft. The services include assignment of a specially trained coordinator who personally assists the victim by doing the necessary paperwork, making appropriate phone calls, and completing other restoration activities, such as credit report reviews, account cancellations, disputed items removal, and more, on behalf of the victim. The work is done by a specialist trained for such cases, and the employee is freed up to focus on work instead of restoring his or her good name.

Many of the corporate risks associated with identity theft can be mitigated by the development and implementation of sound policies, systems, and procedures. Others will ultimately become matters for the courts. Risks that flow from the affected individual, however, must be managed using available tools and products that both support the individual and protect the employer. In the absence of a solid risk management plan for identity theft, the potential losses are nearly unlimited.

**Guillaume Deybach** is the President and CEO of Worldwide Assistance ([www.worldwideassistance.com](http://www.worldwideassistance.com)), part of the multinational Europ Assistance Group.

## Are We There Yet? The Current Status of Section 404 for Small Businesses

*By Gerard S. DiFiore and David T. Mittelman, Reed Smith*

Now in its fifth year, the Sarbanes-Oxley Act of 2002 continues to generate headlines daily. Praised by some as fulfilling its promise of improved accounting integrity while criticized by others as reducing U.S. capital market competitiveness, most discussion today about Sarbanes-Oxley focuses on one critical component—Section 404 governing management's assessment of internal controls. While Section 404 compliance is challenging for all companies, it is especially daunting for the 6,000 smaller public companies. These so called "small business issuers" (having less than \$25 million in revenues or non-affiliate float) bear a disproportionate burden in assessing internal controls. Even non-public companies should stay apprised of Section 404 developments because SEC standards often serve as models for corporate governance and internal controls become critical when public companies acquire smaller private companies.

### What is Section 404?

Section 404 is part of Sarbanes-Oxley's focus on enhanced financial disclosure. It directed the Securities and Exchange Commission to adopt rules requiring U.S. public companies to provide an internal control report that:

- (1) states the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and
- (2) contains an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

Section 404 also requires a public company's auditor to provide its own assessment of management's report. Together, the management and auditor reports are provided in the small business issuer's Form 10-KSB. Chief Executive Officers and Chief Financial Officers also must certify the integrity of their company's internal controls. The certification carries with it penalties of up to \$5 million in fines and 20 years imprisonment. The certification, and therefore compliance with Section 404 internal controls, is not taken lightly.

### When is the current deadline to comply with Section 404?

Due to difficulties public companies faced in formally designing and testing internal control systems, the SEC has postponed implementation of Section 404 five times, so that as of December 2006 these standards now apply:

#### *US Filer Status:*

- Large Accelerated Filer or Accelerated Filer (\$75 million or more of outstanding common equity held by non-affiliates)
- Non-accelerated Filer (less than \$75 million of outstanding common equity held by non-affiliates)

#### *Management's Report:*

- Already complying (Annual reports for fiscal years ending on or after November 15, 2004)
- Annual reports for fiscal years ending on or after December 15, 2007

#### *Auditor's Attestation:*

- Already complying (Annual reports for fiscal years ending on or after November 15, 2004)
- Annual reports for fiscal years ending on or after December 15, 2008

Importantly, for non-accelerated filers—which by definition always include small business issuers – management has a one-year head start on auditors to provide the Section 404 report. Also significantly, the SEC recently adopted rules reducing the liability a small business issuer incurs in the first year of complying with Section 404. The cumulative effect is that during the initial transition year to Section 404, management of small business issuers has more flexibility and independence to assess their own internal controls with less risk of legal action and auditor interference.

The repeated postponement of Section 404 has been both a blessing and a curse for small businesses. Generally, smaller businesses have benefited from evolving guidance on how to conduct a Section 404 assessment, without having to actually undertake the more cumbersome early models. Many small business issuers have utilized the additional time to work within the organization and with their auditors to enhance internal controls in preparation for the day when Section 404 finally will arrive.

Yet, while few persons would refuse a delay of a compliance standard as consequential as Section 404, the repeated postponements have generated uncertainty and disruption. Gearing up to conduct an internal controls assessment is not an easy task. Many smaller businesses have followed a start-and-stop approach, unsure when and how to implement Section 404. Even the current deadlines set forth in the table above are in flux. Politicians of both parties have called upon the SEC to further delay or even

exempt small business issuers from Section 404. SEC Chairman Christopher Cox and House Financial Services Committee Chairman Barney Frank (a successor to Representative Oxley), however, seem to prefer a "mend it, don't end it" approach.

#### **How do small business issuers (and the SEC) implement Section 404?**

For Section 404 ever to become palatable to small businesses, a key challenge is developing an appropriate framework for management to evaluate internal controls over financial reporting. There already exists an established framework for auditors to assess internal controls, namely Accounting Standard 2 (AS2) developed by the Public Company Accounting Oversight Board (PCAOB). But no similar framework exists for management to assess internal controls as required by Section 404. Without guidance on where it should end up in the Section 404 reporting process, some public companies are unsure where to start. The uncertainty is only exacerbated in the case of small business issuers which typically lack the financial and personnel resources of larger companies.

Recognizing the challenge faced by small business, the SEC in December 2006 proposed a "roadmap" for public companies to evaluate their internal controls. It represents perhaps the SEC's best effort to make Section 404 more "user friendly." The guidance permits management to use a risk-based, top-down assessment. Fundamentally, it emphasizes management experience in running the public company. Doing so provides more flexibility for smaller businesses. For example, a small business of only 50 employees is likely to have management actively involved in the day-to-day operations. That

level of transparency implies that management knows the strengths and weaknesses in its public company's internal controls. Therefore, the small business could rely upon fewer systems and less testing to develop effective internal controls.

The SEC has not yet adopted the proposed guidance on evaluating internal controls. The agency currently is reviewing comments on the proposal and working with the PCAOB to coordinate an AS2 update to make auditor testing and assessment more efficient. In theory, the combination of improved SEC and PCAOB guidance should translate into less burden and cost for small business. In reality, while the SEC is seeking to make it easier to implement, Section 404 compliance will never be easy. Small business issuers should expect action from the SEC before June 30, 2007. For calendar year public companies, that date marks the end of the second quarter, which is a key measuring point for determining accelerated filer status and thereby Section 404 compliance. If SEC action fails to aid small businesses at an optimum level, then political pressure probably will force further postponements of Section 404 implementation.

*Attorney Gerard S. DiFiore is partner in the New York office and Attorney David T. Mittelman is counsel in the San Francisco office for the international law firm of Reed Smith LLP. Both are former members of the Division of Corporation Finance of the Securities and Exchange Commission. You may contact Gerry at [GDiFiore@ReedSmith.com](mailto:GDiFiore@ReedSmith.com) and David at [DMittelman@ReedSmith.com](mailto:DMittelman@ReedSmith.com).*

---

#### **News Briefs**

**Judith A. Patterson** has been named president of First State Management Group (FSMG) at **The Hartford Financial Services Group**. Patterson will replace **Ralph J. Palmieri**, who is retiring after a 31-year career with FSMG and The Hartford.

Uncertainties in the financial markets could bring about an increase in business bankruptcy filings this year and major law firms are getting prepared. "There has been a pickup in Chapter 11 business and we have added personnel in our New York office as a result," says bankruptcy attorney **Rhett Campbell** of **Thompson & Knight**.

The **American College Alumni Association** announced that it will be holding its First Annual Golf Outing on Wednesday, June 6 at the DuPont Country Club in Wilmington, Delaware. The event is open to all American College alumni, family, and friends. For registration visit [www.TheAmericanCollege.OnlineCommunity.com](http://www.TheAmericanCollege.OnlineCommunity.com) or contact Adam Batchelor at (610) 526-1477.

LDW Publishing  
1465 Tullamore Lane  
Phoenixville, PA 19460  
www.ldwpublishing.com

---

### **Conference Schedule**

**May 10-11, 2007** BAI Treasury and Risk Management Conference. Renaissance Washington DC Hotel, Washington, D.C. To register, visit <http://www.bai.org/treasury/>

**May 22, 2007** BAI Treasury and Risk Management Conference. Renaissance Washington, DC Hotel, Washington, D.C. To register, visit [www.bai.org/treasury/](http://www.bai.org/treasury/)

**September 7-13, 2007** Les Rende-Vous de Septembre. Sporting d'Hiver, Place du Casino, Monte Carlo. For more information, visit [www.rvs-monte-carlo.com/index.html](http://www.rvs-monte-carlo.com/index.html)

**September 17-18, 2007** The Life Settlements Conference. Disney's Grand Floridian Resort, Orlando, Fla. For more information, visit [www.dealflowmedia.com](http://www.dealflowmedia.com)

**October 16-19, 2007** IAIS 14th Annual Conference. Harbor Beach Marriott Resort & Spa, Fort Lauderdale, Fla. For information, visit [www.iais2007.org/#](http://www.iais2007.org/#)

**RISK FACTOR** is published monthly by LDW Publishing, Valley Forge, Pa.

#### **Editorial staff:**

**Lori D. Widmer**  
Publisher

**Barbara F. Davis**  
Contributing Editor

**Kevin M. Quinley, CPCU,  
ARM**  
Contributing Writer

Mailing address:  
1465 Tullamore  
Phoenixville, Pa. 19460

Website:  
[www.ldwpublishing.com](http://www.ldwpublishing.com)

For subscription and all general information, call 610-933-7980 or email: [lwidmer@ldwpublishing.com](mailto:lwidmer@ldwpublishing.com)

*Copyright 2006 LDW Publishing. All rights reserved. Reproduction in whole or in part without written permission is prohibited.*