Brought to you by the publishers of COMPLIANCE WEEK

Top TPRM priorities in 2023

An e-Book publication sponsored by dun & bradstreet

About Us

COMPLIANCE WEEK

Compliance Week, published by Wilmington plc, is a business intelligence and information service on corporate governance, risk, and compliance that features a daily e-mail newsletter, a quarterly print magazine, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has become the go-to resource for chief compliance officers and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance practitioners. www.complianceweek.com

dun & bradstreet

Dun & Bradstreet, a leading global provider of business decisioning data and analytics, enables companies around the world to improve their business performance. Dun & Bradstreet's Data Cloud fuels solutions and delivers insights that empower customers to accelerate revenue, lower cost, mitigate risk, and transform their businesses. Since 1841, companies of every size have relied on Dun & Bradstreet to help them manage risk and reveal opportunity. For more information on Dun & Bradstreet, please visit www.dnb.com.

Cybersecurity, regulatory risks lead TPRM priorities in 2023

Respondents to a survey from Compliance Week and Dun & Bradstreet overwhelmingly indicated cybersecurity to be the most important compliance-related area affecting third-party risk management in the new year, though fraud and other risks should still be on their radar.

BY AARON NICODEMUS

Compliance professionals will be most focused on addressing cybersecurity and regulatory compliance risks contained within their third-party relationships this year, according to the results of a new survey from Compliance Week and Dun & Bradstreet.

Out of 179 total respondents to the "State of Third-Party Risk Management in 2023" survey conducted online between October and November, 41 percent said cybersecurity was their top risk management priority. Second was regulatory compliance at 27 percent, followed by supplier risk at 15 percent; environmental, social, and governance (ESG) at 9 percent; and combating business fraud at 8 percent.

Approximately 37 percent of respondents said ESG was the least of their concerns of those five issues, followed by combating business fraud at 29 percent.

Another question asked which compliance-related area would be most important in 2023. Cybersecurity was the clear favorite among options provided at 65 percent, followed by anti-bribery/anti-money laundering (13 percent), climate-related risk disclosures (12 percent), and ISO frameworks (6 percent).

Survey respondents represented industries including financial services (19 percent); healthcare (8 percent); manufacturing (6 percent); real estate, education, and technology (all 5 percent); and automotive, food and beverage, retail, pharmaceuticals, construction, and government (all 3 percent).

That cybersecurity is the top concern in assessing third-party relationships does not come as a surprise, said Paul Westcott, Dun & Bradstreet's product director for know your customer/know your business (KYC/KYB).

"Cybersecurity can become a large reputational risk," he said. "The results of a cyberattack can appear in the media much more quickly than many other types of risks."

Regulatory compliance in 2022 was increasingly complicated by Russia's war against Ukraine, a trend likely to continue in 2023. Many countries are continually adding companies and individuals to sanctions watchlists, creating a regular stream of potentially problematic new connections to third parties.

The key with assessing the risks these events pose is to determine ahead of time whether certain changes in your firm's relationships with particular third parties are material to your operations, Westcott said.

"Fraud peaks under times of economic stress. That's when good people do bad things. From my point of view, it's going to be a tough year for fraud."

– Brian Farley, VP, Business Segment Manager, Third-Party Risk and Compliance, Dun & Bradstreet

Survey respondents, when asked which third-party data they are most reliant on to assess their business relationships, said financial (55 percent), company principals/employees (52 percent), legal (50 percent), watchlists and sanctions (40 percent), and corporate linkage (31 percent). Respondents could choose more than one type of data. Less popular answers included firmographic/corporate entity and ultimate beneficial ownership, which both came in at 22 percent.

Some firms are moving away from only using data to drive decision-making about their partners and vendors, which can track patterns that are not material to the business relationship, Westcott said. Instead, they are transitioning to an event-based model, in which a change of ownership or significant shift in business model are more relevant, he said.

"It's determining how material that risk is to my organization, in context to all of the other risks," he said.

ESG being ranked so low by survey respondents is likely because of multiple factors in the market, said Brian Farley, Dun & Bradstreet's vice president, business segment manager, third-party risk and compliance.

The first factor is companies are bracing for a recession, and efforts to measure, for example, the greenhouse gas emissions of suppliers, are being pushed off.

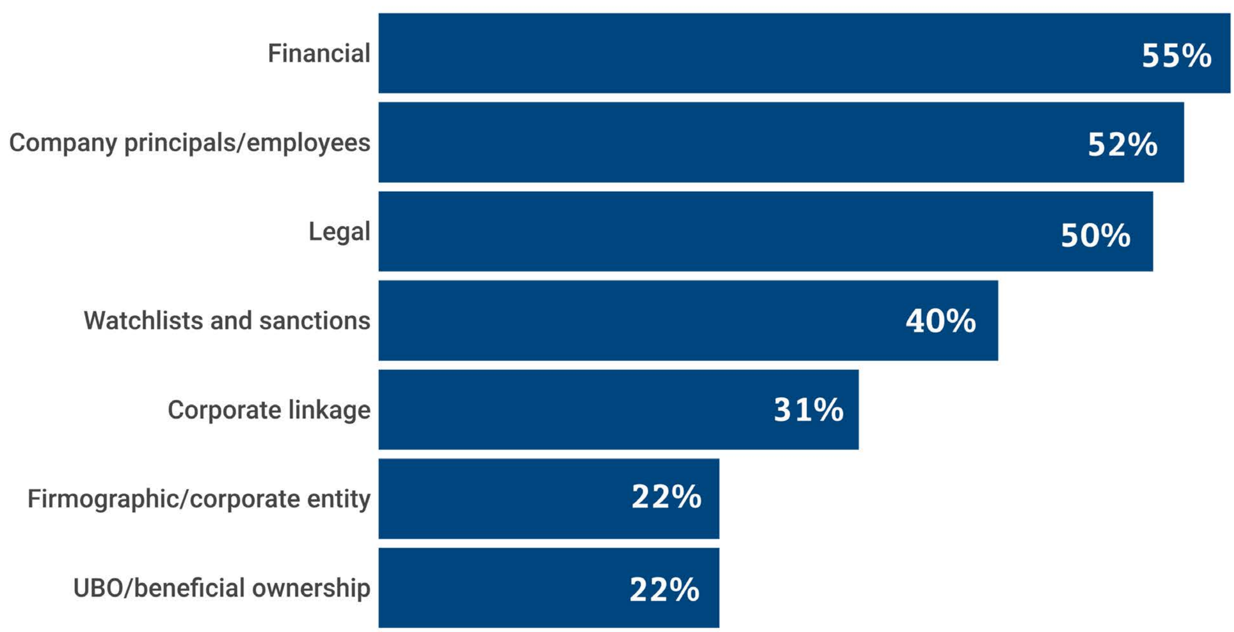
Another factor is while regulators in Europe have begun requiring ESG-related disclosures, the climate-related disclosure rule proposed by the U.S. Securities and Exchange Commission has not been finalized.

"The regulatory framework isn't baked yet. People don't want to invest in something, then learn they need a totally different solution," Farley said.

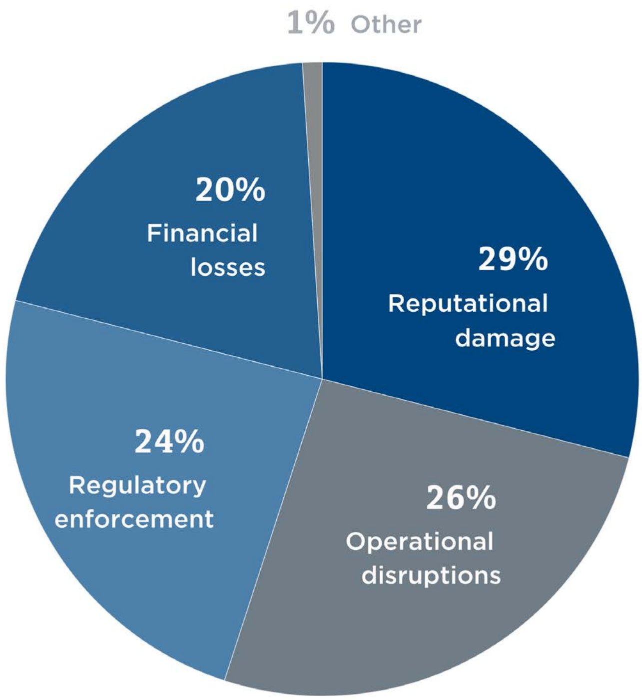
Survey respondents said reputational damage is the most important consequence for not managing third-party risk

> "Cybersecurity can become a large reputational risk. The results of a cyberattack can appear in the media much more quickly than many other types of risks."
>
> Paul Westcott, Product Director for KYC/KYB,
> Dun & Bradstreet

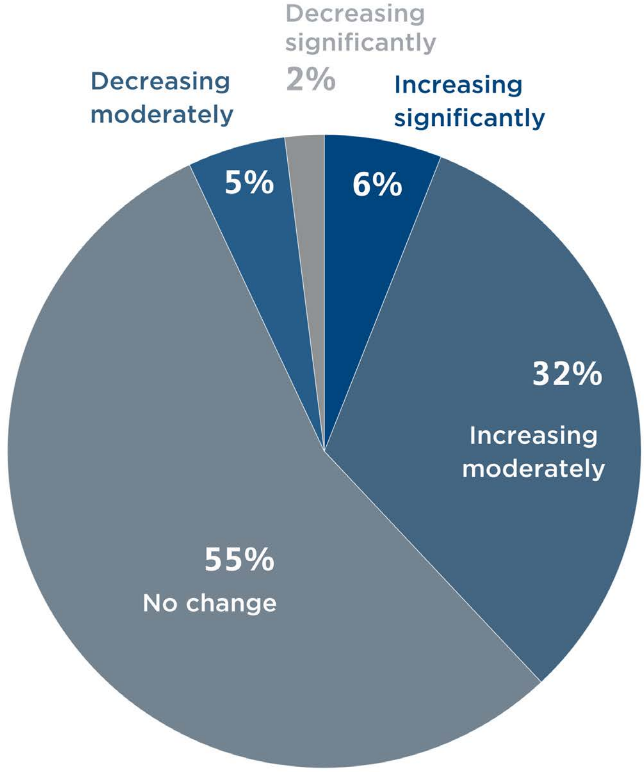
What types of data will you be most reliant on to perform customer and third-party due diligence? Choose all that apply.



What are you most concerned about if your compliance team is not effectively managing risk?



Have you observed B2B fraud increasing or decreasing in the past year?



(29 percent), followed closely by operational disruptions (26 percent), regulatory enforcement (24 percent), and financial losses (20 percent).

More than half of survey respondents (54 percent) reported increasing vendor/third-party due diligence in response to global disruption, while 45 percent reported increasing their ongoing monitoring of their third parties. Respondents could choose as many responses as applied. Nearly two in five (39 percent) reported an increased reliance on risk data and analytics to drive decision-making. Only 18 percent reported no change to their third-party risk management priorities because of global disruptions.

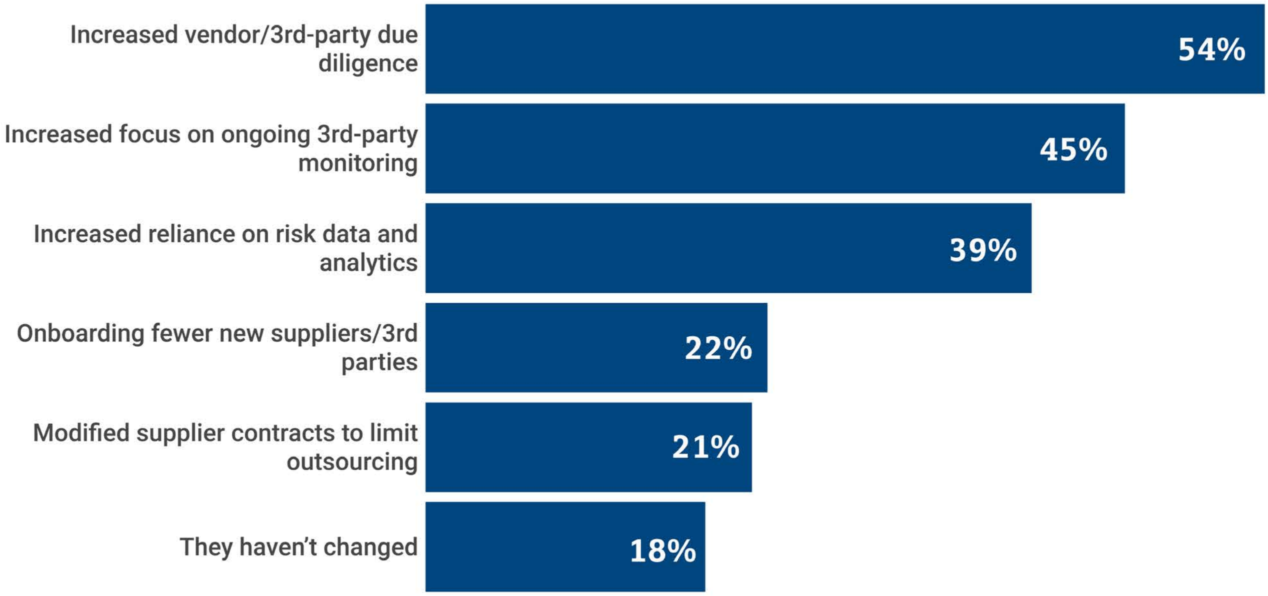
When asked to choose all the ways their firm has reacted to increased scrutiny of sanctions compliance, one in three respondents said they invested or planned to invest in more standardized/actively monitored data. Nearly as many respondents (30 percent) reported their firms had enhanced screening technology or implemented new sanctions compliance programs. Other responses included increasing sanctions screening frequency (29 percent) and ending high-risk relationships (22 percent).

Nearly a third (29 percent) of respondents said their business had not been impacted by sanctions.

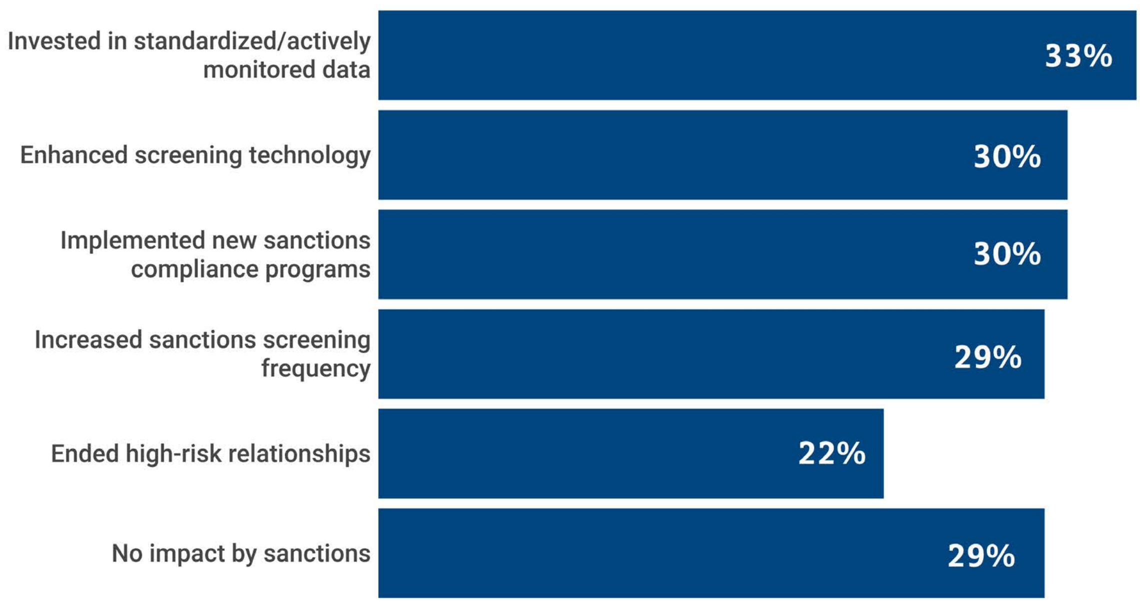
One question asked respondents if they have seen an increase or decrease in business-to-business fraud in the past year. More than half (55 percent) said they experienced no change. Nearly a third (32 percent) said it increased moderately. Six percent said such fraud increased significantly, while 7 percent said it was decreasing.

"This surprised me a little bit," Farley said, particularly since there are signs of a recession coming in 2023. "Fraud peaks under times of economic stress. That's when good people do bad things. From my point of view, it's going to be a tough year for fraud." ■

How have your TPRM priorities changed considering global disruption/instability? Choose all that apply.



How has your team responded to increased scrutiny of sanctions compliance? Choose all that apply.



dun & bradstreet

In today's climate of elevated business risk, you need timely third-party risk and compliance insights.

That's where we can help.

Manage compliance and monitor emerging risks with the most *comprehensive* data available.

Identify entities associated with sanctions, watchlists, and adverse media.

Get corporate linkage and UBO data to verify third parties and accelerate due diligence.

Streamline compliance to be more efficient and avoid regulatory penalties.

Learn how we can help protect *your* business from third-party risk.

WWW.DNB.COM/COMPLIANCE

© Dun & Bradstreet, Inc. 2023.
All rights reserved. (CR-1203792219440615 01/23

dun & bradstreet

WHITE PAPER

Integrating Finance and Risk Intelligence

Getting the Right Data into the Right Systems

Introduction

Record inflation, cyberattacks, supply chain disruption: Finance and risk leaders are grappling with a constant barrage of threats to the continuity and resilience of their businesses.

Most of these leaders know that if they're going to successfully confront and deflect these threats, they need data. There are, of course, many types of data — financial, supply chain, firmographic, and ESG are just a few. And it's not that enterprises lack for this data; in a recent risk management survey conducted by a leading global research and advisory firm, 74% of respondents, on average, said that their companies had access to a broad range of risk data and used it regularly or consistently.[1]

[1] "Change the Culture of Risk Management to Increase Business Resilience" (a commissioned study conducted by Forrester Consulting on behalf of Dun & Bradstreet), August 2022.

The challenge and the barrier to more effective risk management, then, seems not to be the quantity of available data. Data is in abundance, and it's only growing. It can be overwhelming for decision makers and data managers alike to use data effectively if it's ingested uncontrollably — or if it's not accessible by those who urgently need to derive insights from it. This means that data itself is just one key requirement for a data strategy that provides real value to finance and risk organizations. The other requirement is integration — consolidating and connecting risk intelligence across functions to maximize accessibility, usability, and risk visibility.

Data integration is achieved through surrounding technology that enables processes to move and insights to flow, and ultimately fuels decision-making. But technical design and infrastructure should only be assessed after qualifying some prerequisite steps that are crucial to data integration.

Let's dive in.

Create a Vision Aligned to Your Business Goals

Enterprise data integration initiatives begin with a business need — such as, the need to ensure that there are no business transactions with sanctioned or watchlisted third parties. If any members of the cross-functional team cannot articulate accurately the business issues that need to be solved or goals that have been set, pause. This vision and direction should answer: "What does success look like?" Be focused and deliberate. For example, when involved in a sourcing/purchasing data initiative, ensure that you are informed with the sourcing plan that is attached to the needs of the business.

"Build. Measure. Iterate" is what Program Manager Ashley Thompson of the Beeck Center at Georgetown University noted when she discussed the importance of agile rapid prototyping — a method of mitigating natural challenges that come with problem-solving.

Begin with the end in mind

Integration initiatives present the risk of getting lost in the minutia of process design. Always keep that business goal close. When building/designing steps or phases of the project, ensure that they have direct impact on specific finance and risk goals.

Think big, but start small

Plan on scaling. Why is this important? Goals might seem lofty at times and may be deemed unreachable. Creating smaller prototypes helps you to know if this is the case. In moving forward, proofing in scale becomes critical to test the viability of goals. Find those small wins that are pertinent to the business needs at hand.

Define stages and success metrics

And don't overlook the timing required for each stage until you can get to the finish line. Make sure the effort is quantifiable; this is the difference between a dream and a goal.

Understand the Landscape

To properly scale enterprise data integration initiatives, it's pertinent to know how, where, when, and what data is being created, edited, deleted, and accessed. It pays to know both the data landscape and the market landscape of finance and risk management to understand your starting point and where you want to progress in your data journey.

Data landscape

Beyond the technical information of data storage and connectivity, knowing the engagement of your data stakeholders will influence the architecture of the eventual data landscape. Is it distributed, siloed, or centralized? For example, keep tabs on your vendor master. It may be in a supported instance like a master data management (MDM) system, or it could be cobbled from various data sources — or worse, from unsanctioned spreadsheets. Guide the behavior of data users by instituting a sustainable system with scalable methods to edit, enrich, and relate supplier/vendor data.

Market landscape

In the current post-COVID economy, it's necessary to manage volatility in KYC/KYTP/KYB processes. Inform your criteria on potential customers, vendors, or third parties with trusted data to reduce risk and reduce disruptions. This can be achieved by:

- Employing a trusted source of external global data
- Building robust and complete customer/supplier/third-party profiles that let you avoid exposure and maximize efficiency
- Validating your records against a reliable third-party source to ensure you are adhering to compliance and reporting requirements

Right-Size Your Data

Moving to become data-driven does not stop with data quality and data completeness. Widen the aperture by going beyond internal data and bringing in external referential data to help you align data strategy with business need.

Enrich your files to expand your view of risk and opportunity

Employ consistent data services that ensure you have high-quality data when and where you need it. If you want reliability in your supplier or customer base, you also need it in your supplier or customer data.

Choose a data provider that can match your data to its own repository of business records and standardize, cleanse and de-duplicate it. Refresh your data frequently to maintain its accuracy and completeness; this is key for proactive mitigation of customer and third-party risk in a dynamic global marketplace.

Elevate scalability through ESG data

This is the new data superpower to help mitigate potential business risk and volatility, particularly for KYB and KYTP purposes. Knowing the environmental, social, and governance (ESG) factors associated with potential vendors and third parties enables companies to assess reliability and viability. Incorporate an intelligent third-party sustainability analytics solution that will allow your company to assess and track vendor and supplier ESG performance and activities. Here's how to accomplish this:

- Assess suppliers and third parties on ESG criteria throughout the procurement and compliance processes
- Maintain ESG performance visibility throughout your supplier and third-party portfolios by identifying ESG risks in specific industries and geographies
- Actively monitor high-risk suppliers and third parties; identify areas for supplier engagement by monitoring ESG risk over the course of the business relationship

Expand to a 360° View

One of the key outcomes of data integration across finance, procurement, compliance, and other risk-focused functions is to be able to provide that complete view of your customers and vendors. This means mastering your data in a scalable environment.

Master your internal data with third-party data

To gain this holistic view of your data, you'll need to optimize by establishing frameworks, stewardship, and data governance. Keep in mind that this is not a once-and-done task. Data practices, operations, and actions need to be ongoing and guided by policies instituted to meet agreed-on business goals. This may seem like an enormous undertaking, but third-party data contributes greatly to its ultimate success by resolving data attributes to achieve a single source of truth. Clean, updated firmographic data, public and private financial data, and risk scores are examples of third-party data that help you conserve time and resources while boosting confidence in the data integration initiative.

Assess through corporate linkage/ownership relationships

The organizational hierarchy plays the role of a central nervous system for master data. These hierarchies connect all supplier, customer, and third-party master data. Understanding the organizational hierarchy (or corporate family tree) is one of the core principles of a sound master data strategy. Organizational hierarchy is the foundation, and parent-subsidiary relationships are the cornerstones of the intelligence needed for reporting and aggregating finance and risk data, whether at the companywide or individual account level.

Conclusion

The end in mind

Collectively, data is often cited as the missing element that will help finance and risk teams — including procurement and compliance — to "reimagine" risk management and achieve the upper hand in this climate of volatility and unpredictability. But more data isn't necessarily good enough; the focus needs to be having the right data in the right places. When you start by defining the outcomes your data-driven organization requires, you've taken a critical first step that will serve as the north star, a directive, of your data strategy. This will clear the way for the necessary interrogation of processes and data completeness that will expand data value and eliminate the blind spots in your risk management efforts.

Learn more about why and how businesses can become more resilient and *future-ready* through better integration of finance and risk data.

READ THE STUDY ›

ABOUT DUN & BRADSTREET®

Dun & Bradstreet, a leading global provider of B2B data, insights and AI-driven platforms, helps organizations around the world grow and thrive. Dun & Bradstreet's Data Cloud fuels solutions and delivers insights that empower customers to grow revenue, increase margins, manage risk, and help stay compliant—even in changing times. Since 1841, companies of every size have relied on Dun & Bradstreet. Dun & Bradstreet is publicly traded on the New York Stock Exchange (NYSE: DNB). Twitter: @DunBradstreet

© Dun & Bradstreet, Inc. 2023. All rights reserved. (CR-1203792219440615 01/23)

dnb.com