

Borgun

通过及时且成本高效的监管报告，支持国际增长

新监管要求层出不穷且日益苛刻，在这种背景下，支付服务组织必须找到有效的方法，在不导致成本飙升的情况下遵守这些要求。为了减少合规风险敞口并为国际拓展铺平道路，Borgun 利用 IBM® Safer Payments 获得了有关发卡和收单业务的 360 度视图。

BORGUN

业务挑战

要推动国际支付服务的增长，Borgun 必须提升运营成本有效性并保证监管合规。该公司如何快速有效地应对新规则和需求？

转型

Borgun 部署了 IBM Safer Payments，这是一个可扩展的欺诈预防认知平台，可帮助减少设计和执行合规策略所需的成本、复杂性和时间。

成果

降低

合规项目的时间和成本，帮助 Borgun 快速适应法规

提升

可扩展性，支持不断增长的支付交易

实现

实时和批量监控，帮助 Borgun 保护支付和数据

业务挑战

快速做出反应，保持稳定增长

Borgun 提供全方位的电子支付服务，涵盖自身的发卡和收单业务。除了要在冰岛国内市场保持至少 50% 的份额外，该公司还致力于在欧洲扩展中小商户客户群。

Borgun 首席风险官 Steen Henriksen 表示：“支付行业瞬息万变。为了继续追求增长目标，我们必须与不断变化的监管环境保持同步，以经济高效的方式满足市场的新需求。”

过去，Borgun 利用多个系统监控并报告自己的收单业务。为了为内外部利益相关者构建报告，公司需要手动提取、整理和分析电子表格中的数据，这一过程非常耗时。

Borgun 商户监控主管 Andrea Þorlákssdóttir 解释道：“在某些情况下，我们可以使用变通方法来收集报告所需的数据，比如使用我们的商业智能系统来计算商户欺诈比率。在其他情况下，这种方法并不可行。譬如，我们无法深入到每笔交易的销售点终端标识，而这正是我们许多信用卡计划合作伙伴现在所需要的。”

她继续说道：“随着我们继续扩大国际投资组合，我们的交易量最终会超出现有监控工具的能力范围。为了获得详细完整的运营视图，以及业务增长所需的可扩展性，我们决定寻找一个新的平台。”

“随着市场竞争日益加剧，拥有像 IBM Safer Payments 这样的平台对于迅速应对新挑战至关重要。”

— Steen Henriksen, Borgun 首席风险官

转型故事

拥抱实时监控

为了支持发卡和收单业务发展，Borgun 选择采用 IBM Safer Payments，这是一款实时欺诈预防平台。

IBM Safer Payments 的 IT 实施专家兼项目经理 Sigurður Jakobsson 评论道：“选择过程包括对许多供应商进行全面评估，最终我们会将评估范围缩小到两家供应商。我们认为 IBM Safer Payments 比竞争对手产品更胜一筹，因为它具有出色的报告功能，这意味着我们可以在不部署额外模块的情况下访问所需的大部分信息。”

Jakobsson 补充道：“我们认为，IBM Safer Payments 在规则创建方面表现抢眼，我们对该平台支持我们发卡和收单业务的能力非常满意。在收单业务方面，我们获得了实时阻止可疑授权的能力，而不用再事后总结经验教训。发卡实施完成后，我们还可以使用业务规则，在系统检测到存在很高的欺诈可能性时，立即拒绝授权请求。”

为了减少部署过程中的风险，Borgun 采取了一种分步走的方法，从收单业务开始。通过并行运行 IBM Safer Payments 与遗留的监控系统，该公司在将该解决方案投入生产之前，改进了其概要文件、规则和模型的准确性。

“在整个部署过程中，我们与 IBM 团队并肩协作，事实证明这种合作非常有价值”，Jakobsson 说道。“我们的阶段性实施为我们提供了所需的时间，使我们能够掌握关于 IBM Safer Payments 的强大应用知识，这有助于我们在进入生产阶段时取得积极的成果。”

他评论道：“当我们启动该项目时，我们只打算将 IBM 平台与一个源系统集成，因为其他系统正在退役。业务中其他地方的时间线变化，意味着一些流量必须在其他系统上停留比我们预期更长的时间，为了全面了解我们的资产组合，我们还需要将这些平台与 IBM Safer Payments 集成。IBM 能够灵活地适应扩大的项目范围，因此，我们可以随时依靠 IBM 团队在需要的时候为我们提供及时的指导和支持。”

成果丰硕

减少风险，支持增长

在利用 IBM Safer Payments 来支持风险管理和欺诈监控流程之后，Borgun 可以在不增加运营成本的情况下，应对日益严格的监管环境。

“我们目前关注的焦点是满足信用卡计划合作伙伴的新需求”，Þorlákssdóttir 解释道。“除了一些策略上的例外，我们可以利用 IBM Safer Payments 获取所需的大部分数据，减少在多个系统之间来回切换以及创建大型复杂电子表格的需要。”

除了支持该公司的报告需求，该解决方案还有助于提高 Borgun 的态势感知能力。例如，该企业以前需要手动计算商户的退款率，这意味着要花费比实际所需更长的时间来生成风险报告。IBM Safer Payments 支持 Borgun 采用一种积极主动的方法来实施监控和风险管理，使用自动警报，提醒管理团队留意潜在的退款风险，以便立即进行调查。

“虽然很多商家可能并不了解我们所实施的精密监控，但是他们都能够从更强的安全性中获益”，Þorlákssdóttir 补充道。“IBM Safer Payments 还支持我们提供更多个性化服务，从而令我们能够交付更大的价值。例如，一家客户最近要求我们仅允许来自经过批准的国家或地区的信用卡交易。多亏了 IBM 解决方案，我们才能够快速创建定制规则来满足这家客户的要求。这样的灵活性将会让我们更容易从欧洲的商家手中赢得业务，并有助于在新的竞争对手出现时，仍然保持我们服务产品的优势。”

她继续说道：“我们原有监控工具与 IBM Safer Payments 的区别就像黑夜与白天：我们的用户发现新系统更易于使用。我们可以为用户帐户配置细粒度的访问权限，这令我们能够以一种安全的方式支持业务中一系列广泛的用例。”

Jakobsson 补充道：“对我们来说，平台高度稳定非常重要，我们的设置使用多个节点来确保 Borgun 所需的系统可用性。IBM Safer Payments 从一开始就提供了可靠的可用性。”

通过减少设计和执行合规策略所需的成本、复杂性和时间，Borgun 可以集中精力提升支付业务的安全水平。

Henriksen 最后说：“我们现在可以超越监管机构的最低要求，实施内部欺诈监控最佳实践，这将进一步缩小我们的风险敞口。随着市场竞争日益加剧，拥有像 IBM Safer Payments 这样的平台对于迅速应对新挑战至关重要。”

BORGUN

关于 Borgun

Borgun 创立于 1980 年，总部位于冰岛雷克雅未克，是冰岛第一家信用卡发行和收单机构。今天，该公司为冰岛和欧洲其他国家或地区的商户提供收单服务，并为信用卡和借记卡发行机构提供发卡处理服务。

解决方案组件

- Counter Fraud Management

采取下一步行动

IBM 与金融服务业的多家企业达成合作，利用 IBM Cloud、认知技术、大数据、监管科技和区块链技术来帮助他们应对业务挑战。Watson Financial Services 将 Watson 的认知能力与 Promontory Financial Group 的专业知识相结合，支持风险与合规专家做出更明智的决策，更好地管理风险与合规流程。这些流程涉及法规变更管理、特定合规流程等，如反洗钱、了解客户、行为监视和压力测试。

了解有关 IBM 金融风险与监管合规解决方案的更多信息，请访问：http://ibm.biz/cn_bank

© Copyright IBM Corporation 2018. 1 New Orchard Road, Armonk, New York 10504-1722 United States. 美国出品，2018 年 8 月。

IBM、IBM 徽标、ibm.com 和 IBM Watson 是 International Business Machines Corp. 在全球许多司法管辖区的注册商标。其他产品和服务名称可能是 IBM 或其他公司的商标。Web 站点 ibm.com/legal/copytrade.shtml 上的“Copyright and trademark information”部分中包含了 IBM 商标的最新列表。

IBM 并不一定在开展业务的所有国家或地区提供所有产品或服务。

本文引用的性能数据和客户示例仅用于说明目的。实际性能结果可能因特定配置和运行条件而异。

文档中引用或描述的所有客户示例都是为了说明某些客户使用 IBM 产品的方式以及可能取得的结果。实际环境成本和性能特征可能因不同客户的配置和条件而异。联系 IBM，了解我们可以提供哪些帮助。

评估和验证任何其他产品或程序与 IBM 产品和程序一起运行的情况，则由用户自行负责。

客户应自己负责遵守适用的法律和法规。IBM 不提供法律建议，也不表示或保证其服务或产品将确保客户遵从任何法律或法规。

良好安全实践声明：IT 系统安全性涉及通过防御、检测和响应来自企业内部和外部的不正当访问来保护系统和信息。不正当的访问可能导致信息被篡改、破坏或盗用，或者导致您的系统遭到误用而攻击别人。任何 IT 系统或产品都不应被认为是完全安全的，并且没有任何单一产品、服务或安全措施能够完全有效地防止任何不当访问。IBM 系统、产品和服务旨在成为合法、全面的安全方法的一部分，它必定涉及额外的操作程序，并且可能需要其他系统、产品或服务配合才能获得最好的效果。IBM 不保证任何系统、产品或服务免受任何一方的恶意或非法行为侵扰，或帮助您企业免受任意一方恶意或非法行为的攻击。