Five Actions on Payments and Fraud Protection You Need to Take Now

Payments processing and fraud protection aren't "set it and forget it" activities. Find out what you should be doing today to transform payments and fraud management to improve customer experience and revenue creation.

Radial
a bpost company

Taking a Hard Look at Payments and Fraud

Most consumers have no idea what happens behind the scenes after they click Buy Now. They simply want to purchase their merchandise – using the fastest, most convenient means possible.

Until recently, merchants took a similarly dispassionate approach to payments and fraud. Sure, payments processing was key to keeping the dollars rolling in. Fraud protection was essential for avoiding losses. But those were mundane activities largely handled by external vendors – not strategic processes that can create differentiation and drive profitability.

No longer. Merchants are waking up to the fact that payments and fraud management have grown unrecognizably complex. Smart companies are taking a hard look at payments and fraud to achieve important goals:

- Leverage payments and fraud management to simultaneously improve both customer experience and revenue creation.
- Understand how payments and fraud affect the business.
- Identify ways to optimize payments and fraud-management processes.

Shifting Payments and Fraud Sands

The payments and fraud landscape has changed significantly over the past couple of years. And it will continue to evolve quickly, on several fronts:

Processor consolidation – Established payments processors have been merging. In January 2018, Vantiv completed its acquisition of Worldpay. Then in July 2019, FIS Global acquired the combined companies. That followed the January 2019 announcement that Fiserv would acquire First Data.

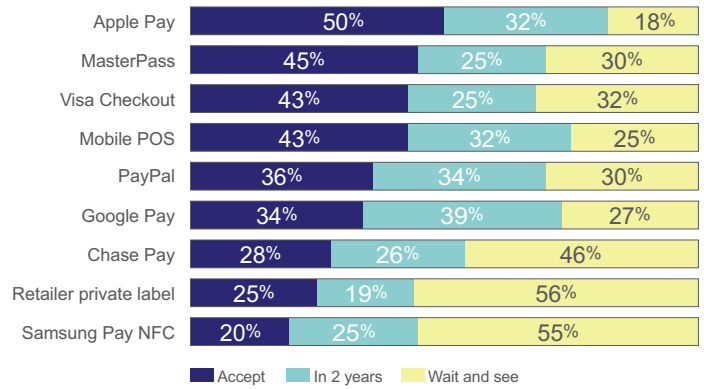
This industry consolidation seems like it should simplify payments, but it doesn't. For one thing, some legacy processors use outmoded technology that's difficult for merchants to work with. As they consolidate, they often retain disparate systems, gaining scale but not simplicity.

Payments startups – New rivals have entered the market with simpler offerings. These disruptors try to differentiate themselves by allowing merchants to get up and running with a piece of code instead of an established payments service. But their simplicity comes at a cost, because they lack global reach, a choice of payments methods and pricing transparency.

Tender proliferation – Until recently, ecommerce mostly involved credit-card payments. Merchants just needed to pass the credit-card data to the bank through the payments processor. It wasn't complicated, and there was no need for creativity.

Today's consumers have far more choices – from PayPal to Apple Pay to Visa Checkout. (See Figure 1.) That creates confusion for consumer and merchant alike. How many payments options should you offer in your ecommerce checkout? You want to give customers the tender options they expect, while avoiding a complex checkout and a poor customer experience.

Figure 1: Digital Payments Methods Accepted by North American Retailers [1]



Cybercrime – Merchants are well aware of the increase in cybercrime. More than 1,200 documented data breaches exposed some 440 million records in 2018 – an incredible 14 records per second. And the number of records with personally identifiable information (PII) increased 126%.[2] That means there's an enormous number of stolen credentials available for fraudsters to use in your retail channels.

In addition, EMV chip cards have reduced card-present (CP) fraud for in-store retail sales. In fact, EMV-enabled merchants saw CP fraud plummet 80% between 2015 and 2018.[3] But in response, fraudsters have turned their attention to card-not-present (CNP) ecommerce transactions. CNP fraud is expected to balloon at a compound annual rate of 14% through 2023 – costing retailers $130 billion.[4]

But if you can master these new payments-and-fraud realities, you can position your brand to compete and win in an increasingly complex and competitive marketplace. With that objective in mind, here are five payments-and-fraud actions that should be on every retailer's to-do list.

1. Approach Fraud Protection and Payments Processing Strategically

Many merchants start with payments processing and then consider fraud protection as an add-on. For example, they might use one vendor for payments processing and a separate vendor for fraud protection. Or they might simply tack on the fraud services of their payments processor, even if those services are limited in functionality and effectiveness.

That's a mistake. Applying fraud protection as an afterthought, or treating these two closely related processes individually, can result in greater friction for your customers and higher fraud levels for you.

A much more effective strategy is to begin with fraud protection and then integrate payments processing in a holistic way. Such a fraud-focused, integrated approach can deliver tangible business advantages.

Starting with fraud protection makes sense, because this is where your service provider can have the greatest impact on your customers and your business. An effective fraud-management solution is fast and precise, it minimizes fraudulent orders while maximizing order conversions, and it completely indemnifies you against fraud and chargebacks.

Once you've implemented such a state-of-the-art fraud solution, it's wise to use the same vendor for payments processing. If that isn't feasible, given your specific needs, at least find a provider that has experience with both payments and fraud protection.

There's a logical reason for this: Separate vendors will be at cross-purposes. One will be concerned with preventing bad transactions from happening. The other will be focused on making sure transactions go through. The result can be friction in the checkout process, a less-than-optimal customer experience, lower sales conversions and unacceptably high chargebacks. Choosing a vendor that understands both payments and fraud will help you avoid these pitfalls.

Of course, chargebacks are something every merchant wants to avoid. And you may believe that because your fraud-protection vendor offers indemnification, there's no need to change the way you manage fraud. But chargeback indemnification that occurs separate from payments processing can lead to unexpected – and far more significant – costs.

> Approaching payments and fraud management strategically can deliver tangible business advantages.

If your business is associated with a high number of chargebacks – typically 1% of transactions, though that threshold will likely soon be lowered – a merchant-processing bank could add you to the Terminated Merchant File (TMF) or Member Alert to Control High Risk (MATCH) list. Once that happens, you could find it very difficult to obtain a new merchant account from another bank. And your entire business could be placed in serious jeopardy.

With separate vendors, you may have no idea that fraud is about to affect payments processing. But with effective fraud protection integrated with payments processing, your provider is incentivized to share information and optimize both processes in your favor.

Just as important, this fraud-and-payments approach makes chargeback processing faster and easier. With separate vendors, first you're alerted by your payments processor of a chargeback. Then you need to challenge the chargeback to avoid unnecessary outlays, and file a claim to be reimbursed for the chargeback losses. But if fraud protection and payments are handled by the same provider, the process is seamless and conflict-free. In fact, you don't even need to get involved.

Another advantage of combined services is the ability to assess fraud risk both before and after payments authorization. Running a quick check before authorization can lower authorization costs and increase authorization rates. If your fraud provider has already determined the transaction is fraudulent, why send it on for authorization? And if the pre-authorization check is successful, you can feel better about paying the authorization fee.

Finally, a single provider can perform analytics on both fraud and payments to optimize both processes. That can especially have a positive impact on fraud protection.

When a payments processor handles a credit card, it converts the number into a cyber-protected token, which is then difficult to analyze from a fraud perspective. Because a combined fraud-protection and payments provider has access to the universal consumer profile, analysis and understanding of fraud patterns and trends become easier and can be leveraged across the provider's ecosystem. So if a credit-card number was used to commit fraud on one site, it doesn't need to be decrypted to detect fraud on another site.

Such analytics cross-pollination extends to your business. An effective provider should be able to deliver a single report that shows all fraud and payments activity, so you get a single point of visibility into your own operations.

2. Protect Data Shared Across Channels

Retail sales today occur across store, online and mobile channels – often all three for a single customer in a single buying journey. (See Figure 2.) And among high-income Millennials in particular – those earning $70,000 or more a year – payments can take place via credit card, mobile device or even wearable. (See Figure 3.)

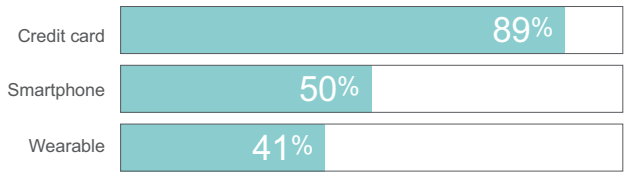
What's more, more merchants will soon follow the lead of Amazon with its touch-free Go checkout, in which sensors record items that shoppers remove from the shelf and place in their bag. Other viable scenarios include smart fitting rooms where shoppers can virtually try on items and tap photos on digital displays to make ecommerce purchases that are then shipped to their home.

All this omnichannel shopping activity means merchants need to manage fraud across a growing number of touchpoints: store, ecommerce website, mobile app and mobile payments made at a physical point of sale. It's no wonder 55% of retailers say fraud is their top payments-related issue. (See Figure 4).

The challenge, of course, is that stolen credentials can also extend across channels. Once fraudsters are authenticated in one channel, they have the possibility of making fraudulent purchases in your other channels. And that means more chargebacks and greater losses for your business.

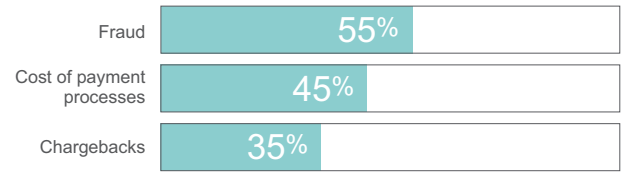
Figure 2: 2018 Holiday Season Shopping [5]

Figure 3: High-Income* Millennial Smart Payments [6]



*>$70,000/year

Figure 4: Top 3 Payments-Related Challenges [7]



The solution would seem to be a more aggressive approach to denials. But just as fraud can extend across channels, so can false positives. And that can lead to poor customer experiences. If a customer is inaccurately flagged for potentially fraudulent activity on your ecommerce website, you don't want to compound the problem with a high-friction checkout in your retail store. That could result in not only lost sales but also lost customer relationships.

As a consequence, you need robust yet flexible fraud protection wherever sales transactions take place. You want to minimize cross-channel fraud and chargebacks while simultaneously avoiding checkout friction and rejected orders.

The good news is that you can leverage cross-channel data from your fraud-protection provider to better understand fraudulent activity, safeguard your revenue streams and deliver positive customer experiences in every channel.

But not every fraud-protection vendor has the sophistication to understand and protect data across channels. Look for a provider with capabilities in these areas:

PCI Level 1 compliance – The Payments Card Industry (PCI) sets standards for security and best practices. A Level 1 service provider must submit to an annual review of compliance by a qualified security assessor. It must also undergo a quarterly network scan by an approved scanning vendor, as well penetration tests and internal scans. Not every vendor achieves Level 1 compliance, and the capabilities that lead to compliance are very difficult for merchants to achieve on their own.

Machine learning (ML) – Your provider should employ sophisticated ML algorithms that quickly understand the unique behavior profile of your customers and rapidly adapt to changes in that behavior over time.

Comprehensive fraud protection – Look for a provider that leverages a full suite of tools, including anomaly detection and both automated and manual transaction reviews. Your provider should regularly capture data from clients and relevant third parties. And all that knowledge and capability should be baked into a comprehensive fraud-detection system.

Business intelligence and reporting – An effective fraud-protection provider should track trends in retail fraud and understand how they affect your business. It should also maintain a history of your customer behavior. The provider should then deliver business intelligence that gives you a picture of the channels that shoppers are using overall, as well as the channels your customers in particular are using to interact with your brand.

Leverage cross-channel data from your fraud-protection provider to deliver positive customer experiences.

Ultimately, you want to provide customers with friction-free checkout, optimize sales conversions and drive down your chargeback rate to less than 1% – or, as standards will likely soon change, even lower. And you need to achieve those goals in every one of your growing number of channels.

3. Strike the Right Balance Between Automated and Manual Fraud Protection

Whether in-store, on an ecommerce website or through a mobile app, you want fraud protection to occur quickly and accurately. Automation can help, and in the past few years, advances in artificial intelligence (AI) capabilities such as ML have enabled sophisticated fraud review to take place in milliseconds. That development has led some fraud-protection vendors to relegate all fraud processes to automated tools.

But even the best ML today still generates an unacceptable number of false-positive declines. For that reason, some vendors cling to manual fraud review – a time-consuming and potentially high-cost process.

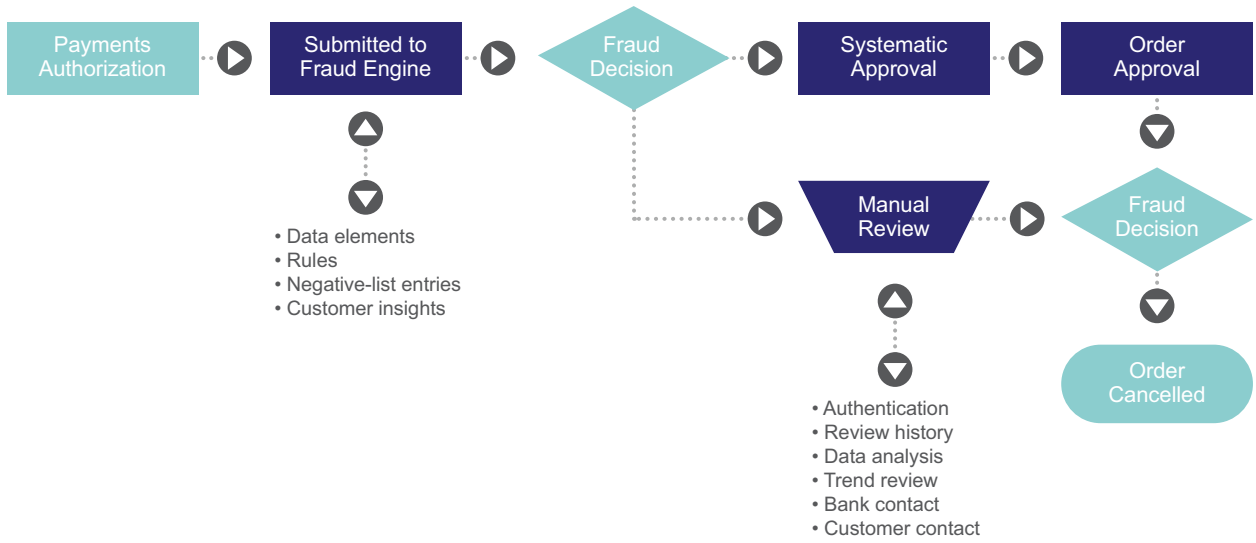
The solution is a blended approach that begins with advanced ML algorithms and augments the process with data analysts for optimal fraud protection with minimal false positives. (See Figure 5.) In fact, a blended approach is a virtual requirement for fraud-protection providers that offer indemnification – assuming the merchant's responsibility for any chargebacks. Neither automation nor manual review alone is accurate and timely enough to make indemnification practicable.

Of course, there are times when one or the other approach is most effective. If you're selling goods the user would expect to access immediately – such as instant download of a computer game – then fraud analysis needs to be instantaneous, and there's no time for manual review.

But manual review can allow for successful order conversions that ML would otherwise decline. Let's say you have a transaction that ML would decline because of a medium risk score. Manual review could show that it's a good customer and that data points such as proxy IP and email address are never seen yet valid. So, you avoid declining the tender and retain your relationship with a good customer.

Or let's say ML would approve a transaction because the data points are valid. But human review reveals that it's actually an account takeover. You avoid a fraudulent purchase and chargeback that ML would have missed.

Figure 5: The Fraud-Protection Process



The human touch is also required to continually improve ML algorithms. Data scientists need to evaluate ML performance and train the ML models. Ideally ML should become more accurate over time, and the purpose of manual review will change accordingly.

To determine whether your fraud-protection vendor uses the right balance of automated and manual processes, ask these questions:

1. How long does review take? Automated review should occur as close to instantaneously as possible. Manual review should occur fast enough to meet the service-level agreements (SLAs) that are right for your business model. Both processes should be transparent to your customers.

2. What percentage of orders involve manual review? Manual reviews are sometimes necessary. But depending on your industry segment, ideally you want to drive down their proportion of all transactions to less than 2% – and certainly far lower than the more common 15%.

3. What are your hours of operation? Ecommerce takes place around the clock. Your fraud protection should keep pace.

4. How do you update your ML models? Your vendor should continually backfill its ML models and decision trees with updated data, and those updates should occur quickly. When your provider first turns on the service, you should expect approval rates to be lower at first but then rapidly improve.

5. Can you scale for peak? Manual processes don't scale as easily as automated ones. But your company might earn a large portion of its revenue at peak times of the year. Your vendor should be able to keep up, even with manual reviews, so that fraud protection never impedes your conversion rates.

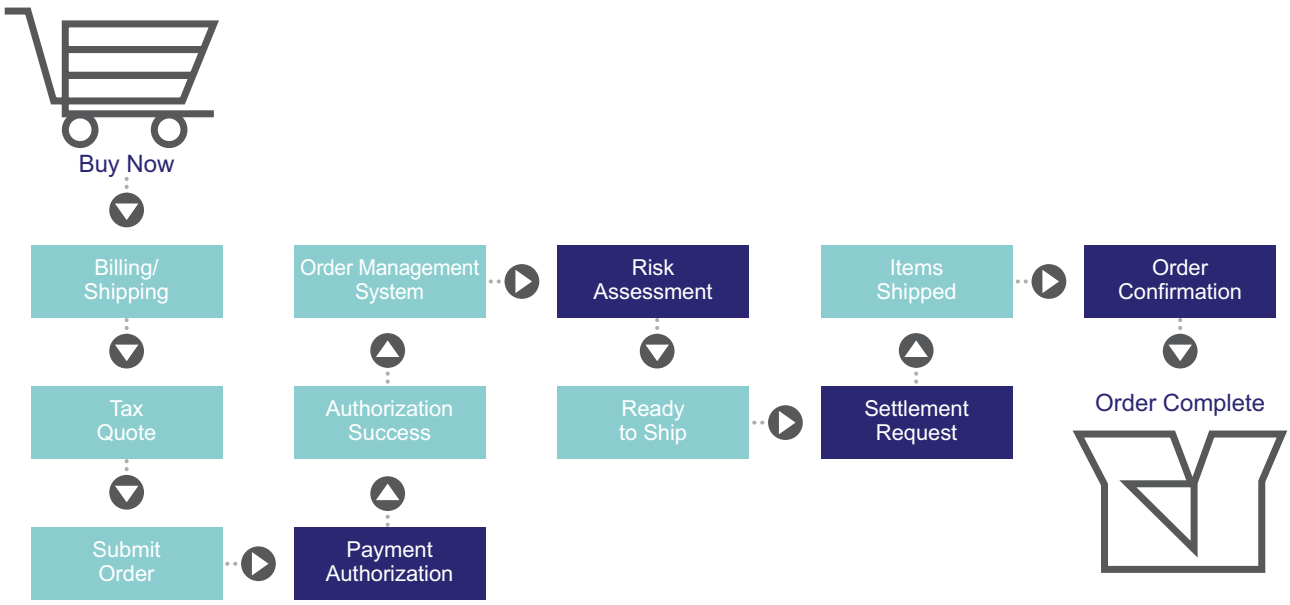
The right combination of automated and manual fraud protection ensures a low number of rejected orders, a minimal amount of human intervention and zero chargebacks to your business. The result should be a positive experience for your customers and a healthy revenue stream for you.

4. Maximize Payments Approvals and Sales Conversions

In the early days of ecommerce, the customer checked out with a credit card, the merchant connected the transaction to its payments gateway, and the payment was either declined or approved. There was little thought about strategies for increasing approval rates.

Today, clicking Buy Now launches a myriad of activities around payments, tax, fraud and omnichannel fulfillment to make sure customers get the products they want, when they want them. (See Figure 6.) And those activities include tactics for minimizing declines and maximizing conversions.

Figure 6: The Post-Click Process



That makes good business sense. After all, before you even list an item for sale, you invest a lot of time, energy and resources in identifying, sourcing, stocking and marketing the product. Yet the vast majority of shoppers who visit your electronic storefront will leave without making a purchase. If a customer clicks Buy Now and is ready to give you money, you want to do everything in your power to convert that sale.

Merchants that approach payments strategically can optimize conversions and increase revenue. Achieving those goals begins with analyzing why declines are happening.

Start with your payments provider. Is it analyzing and providing insights into which types of declines you're experiencing and why they're happening? A small portion of declines occur for no reason at all. If you re-send such declines through another processing route, they might be overturned and approved. Most retailers don't have the luxury of having multiple processing connections, so ask your payments provider about this.

Then look at your user experience. There may be ways to redesign your checkout to make sure customers are using the best tenders for optimal conversions. Or, if an initial tender is declined, present the customer with another payments option or a payments-installment plan.

The bottom line is that you work hard to make sales; don't let any of them get away. To optimize conversions, ask your payments processor some questions:

1. What's your system uptime? System availability is crucial, because you want to convert every Buy Now to a sale. You also need a process for when the system is down. Can you re-route to an alternative payments processor? Can you "hold" the transaction and re-send it later, when the system is back up?

2. How do you handle "soft declines"? Declines can occur because a credit card is invalid, the account limit has been exceeded or there's suspected fraud. A soft decline occurs for no valid reason and sometimes when there's a glitch in the system. One solution is to hold the transaction and re-send it later so the sale isn't lost. But your vendor should have a strategy for dealing with soft declines.

3. Do you offer alternative means of authentication? For example, the 3-D Secure protocol allows for a private session between a customer and the issuing bank for authentication. If the customer is deemed a higher risk, he or she is prompted for a one-time password (OTP). Improvements in the latest version of 3-D Secure enable a friction-free customer experience.

Merchants that don't take actions to optimize conversions risk fewer sales and lower revenue. Even worse, if you don't deliver a fast, convenient checkout experience, you could lose not only the sale but the entire customer relationship. You want to make sure that you can accept their payments and that they come back to your store. With the right approach to payments processing, you can simultaneously improve customer satisfaction and drive new revenue.

5. Optimize Recurring Payments

Time was, retailers simply sold products – and hoped, when the products were used up or worn out, that customers would return to buy replacements. Business models in which customers made regular, periodic payments for ongoing product delivery were reserved for sectors like the newspaper industry.

Today, every business wants a slice of the subscription pie. From shaving razors to pet food to "surprise boxes," a broad range of subscription-based product and service offerings keep customers coming back for more.

For merchants, it's about more than maximizing spend. Recurring payments are a superb way to build and maintain relationships with customers that make them loyal to your brand. It doesn't hurt that the approach effectively takes the customer out of the market – and paints your competition out of the picture.

Yet few merchants think about how payments processing can help optimize recurring payments. The fact is, payments processing is essential to making subscription services cost-effective for you – and satisfying to your customers.

Subscription services are typically built on credit-card transactions. And that presents a significant downside to recurring payments. When a customer's card expires – a regular event – or when a customer replaces a card because of loss or theft – a common occurrence – your cash flow immediately and completely stops.

What's more, you then need to contact the customer to update the card data before transactions can continue. That involves time and cost for you, as well as inconvenience and a less-than-ideal experience for your customers. And there's a chance the customer will discontinue the subscription.

> Smart retailers no longer view payments processing and fraud management as routine tasks.

That's where effective payments processing comes in. Smart merchants now insist on proactive monitoring of card-on-file data. A qualified payments processor will interact with major credit-card brands to confirm if a previously used card has been replaced. That will allow you to proactively update card data whenever an expired card is renewed or a lost or stolen card is replaced – on the fly and invisible to the customer.

As a consequence, you keep the subscription revenues flowing. Even more important, you maintain an excellent customer experience – and sustain your most valuable customer relationships over the long term.

Ultimately, today's smart retailers no longer view payments processing and fraud management as routine, out-of-sight-out-of-mind tasks. In fact, they're central to the experience you deliver customers – at a time when nearly two-thirds of companies rank improving customer satisfaction a top-3 reason for embracing digital commerce.[9] By approaching payments and fraud protection strategically, you can better understand how these vital processes affect your business – and leverage them to build stronger customer relationships and revenue streams.

Authors:
KC Fox, Senior Vice President, Technology Services
Bryan Heron, Senior Product Manager
Tyler Hodgins, Senior Solution Consultant

1 "Digital Payments Methods That North American Retailers Accept or Plan to Accept," Statista, 2019
2 "2018 End-of-Year Data Breach Report," Identity Theft Resource Center, 2018
3 "Chip Technology Helped Reduce Card-Present Counterfeit Payments Fraud by 80 Percent," Visa, 2019
4 "Retailers to Lose $130bn Globally in Card-Not-Present Fraud Over the Next 5 Years," Juniper Research, January 2019
5, 6 "2018 Holiday Outlook," PwC, 2018
7, 8 "The State of Retail Payments – Outlook for 2019," Forrester, November 2018
9 "The Gartner Digital Commerce Vendor Guide, 2018," Figure 2, Gartner, August 2018

About Radial

Radial inc., a bpost group company, is the leader in omnichannel commerce technology and operations. Premier brands around the world confidently partner with Radial to deliver their brand promises, anticipate and respond to industry disruption, and compete in a rapidly evolving market. Radial's innovative solutions connect retailers and customers through advanced omnichannel technologies, intelligent payments and fraud protection, efficient fulfillment, supply chain services, and insightful customer care services – especially where high-value customer experiences are critical. We are flexible, scalable, and focused on our clients' business objectives. Learn how we deliver today's retail for you at radial.com and follow us on Twitter @radialcorp.

Connect with us: 1.877.255.2857 | sales@radial.com | radial.com |

Radial
a bpost company