Momentum™
Financial Services Group

HOW MOMENTUM FINANCIAL IS NAVIGATING AI, RISK AND COMPLIANCE

DIGITAL REPORT

IN ASSOCIATION WITH:

WK

Momentum™
Financial Services Group

HOW MOMENTUM FINANCIAL IS NAVIGATING AI, RISK AND COMPLIANCE

Risk governance, ethical AI and multi-jurisdictional compliance are reshaping fintech – Momentum Financial Services Group's CTO and COO explain how

Momentum Financial Services Group (MFSG) is a North American financial services business operating across Canada and the US. Through its Money Mart brand, founded in 1982, the company provides a range of financial services to customers across North America, with a growing presence of more than 360 locations in Canada and over 60 in the US. Money Mart serves the 'underbanked': people who may not qualify for mainstream credit products and need a lender willing to say yes when others say no. Money Mart's offerings include short and long-term personal loans, cheque cashing, money transfers and other everyday financial services designed to provide flexible, accessible options when customers need them most. The company offers consumer lending, money services and related financial products through a network of retail branches and digital channels.

When Karina Sidhu joined Momentum Financial Services Group as Chief Technology Officer, one of the first things she noticed was how technology at the company was positioned for a transformative opportunity across their well-known consumer brand, Money Mart.

Google Pay and explored the potential of blockchain technology for retail banking. She later moved into capital markets and then served as Chief Technology and Data Officer for a Canadian pension fund before joining MFSG.

Greg Root, MFSG's Chief Operating Officer, brings a similarly broad background. He spent seven years at Canada' largest telco, before moving into fintech through stints at D&H and Finastra.

Together, the two executives are leading a significant transformation programme at MFSG. Their mandate: modernise the business, expand its product set and do so in a way that is both commercially ambitious and rigorously compliant.

"Marrying technology and strategy is much harder than just building good tech solutions," Karina says. "There's no shortage of amazing ideas when it comes to emerging technology. The hardest part is matching them to the business where it counts."

Greg frames the challenge in terms of people, process and technology. He is also clear about where the biggest risks lie – not just in systems, but in culture. Greg notes that: "The biggest challenge is continuing to drive our customer-focused culture while we adopt new technologies."

That interplay between culture and technology sits at the heart of how MFSG approaches risk. Both executives are emphatic that at MFSG risk is understood as something that must be embedded in every decision, at every level of the business.

"Compliance is key. We are in financial services, and there are always changing parts within the regulatory landscape"

Greg Root
Chief Operating Officer
MFSG

Karina explains that MFSG has adopted what she describes as a multi-layer risk framework. This integrates credit risk fraud risk, regulatory risk and operational risk. Executive oversight sits at the top of this structure, but the day-to-day responsibility for monitoring and managing those risks is distributed across operational teams throughout the business. "Data risk management is not just one leader's job," she says. "It is all of our jobs."

Greg points to an often overlooked but critical element of that framework: education. Managing risk effectively, he argues, requires that frontline staff – the people working in retail branches, call centres and back-office processing teams – understand not just what the rules are, but why they matter. "We believe people will buy into things when

GREG ROOT

CHIEF OPERATING OFFICER

Greg Root is Chief Operating Officer at Momentum Financial Services Group, where he leads enterprise operations with a focus on driving growth, operational efficiency and exceptional customer experiences.

A seasoned transformational executive, Greg brings more than 25 years of experience delivering revenue growth, advancing customer success, and optimising operations across the telecommunications, technology and financial services sectors.

Prior to joining Momentum, Greg served as Global Head of Customer Operations at Allvue Systems and as Senior Vice President of Customer Support at Finastra. He has also held senior leadership roles at various large telco organisations, where he developed deep expertise in large-scale operations and organisational transformation.

KARINA SIDHU

CHIEF TECHNOLOGY OFFICER

Karina Sidhu is Chief Technology Officer at Momentum Financial Services Group, where she leads the organisation's technology and data strategy to drive innovation and business performance. With more than 20 years of experience in technology and data – including over 15 years in financial services – she brings deep expertise in delivering scalable, high-impact solutions. Prior to joining Momentum, Karina held senior leadership roles at BMO and RBC Capital Markets, and most recently served as Chief Technology and Data Officer at the Investment Management Corporation of Ontario. She has been recognised as the 2024 CTO of the Year and is a recipient of a CIO Award for innovation and technology-driven business results.

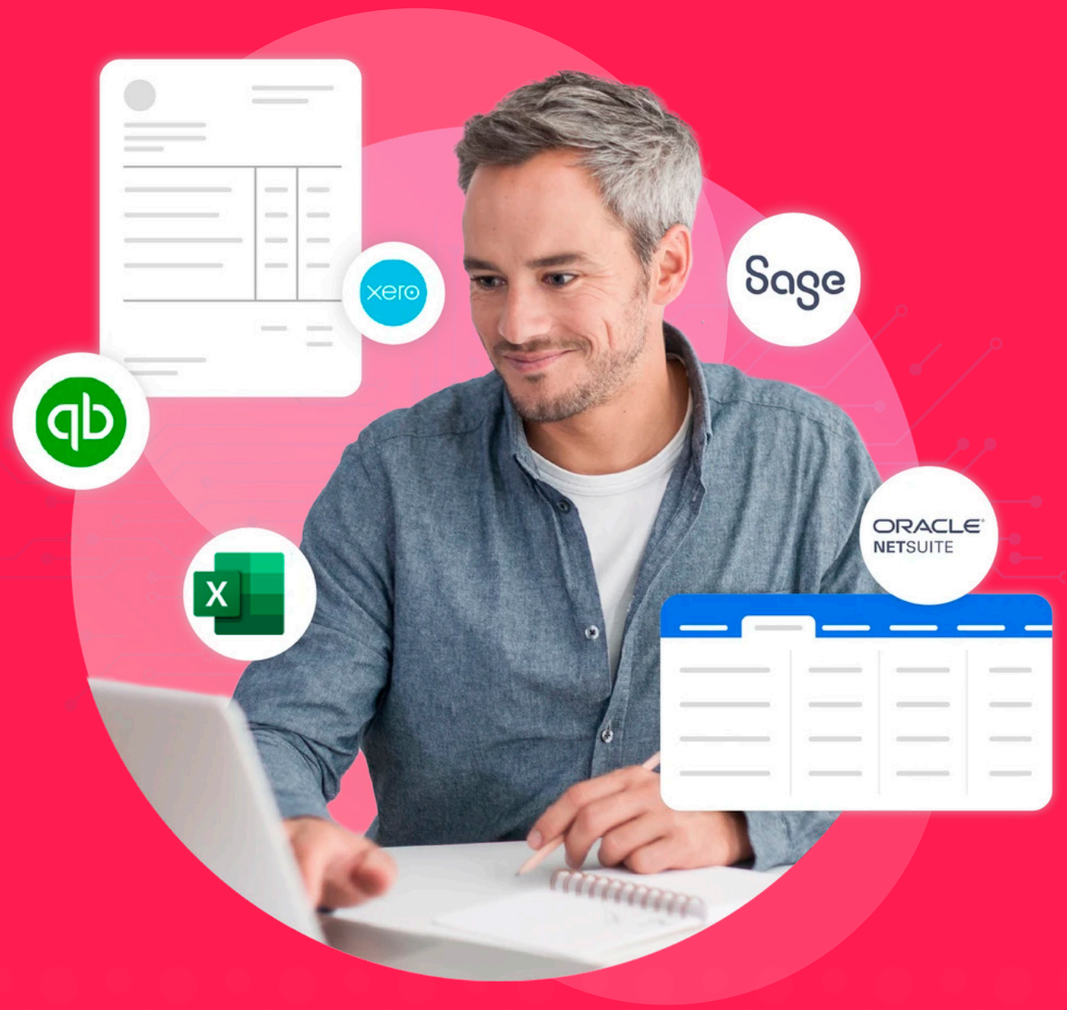
"We've stood up a council that doesn't just look at AI in a vacuum – it covers risk, fraud, privacy, compliance, legal"

Karina Sidhu
Chief Technology Officer
MFSG

they understand the why," Greg says. "The team has done a really good job of educating on all types of risk." That educational mandate has become more urgent as the threat landscape has shifted.

Karina is candid about the growing sophistication of external threats. "There are more and more avenues," she says, "and people are getting better and better at deepfake technology and coming at you – so the risks are growing. " Deepfake technology uses AI to generate convincing but fraudulent audio, video or identity material. In financial services, it has become an increasingly serious tool for fraud. The implication, Karina continues, is that risk education can never be a one-time exercise. "That education is never going to stop because the risks are changing," she says.

How MoneyMart Reduced Manual Financial Processes by 99% with Wrk



In highly regulated financial environments, operational inefficiencies do more than slow teams down. They increase compliance risk, create bottlenecks, and limit an organization's ability to scale. Financial institutions operating across legacy systems often rely on manual workflows, even when accuracy and real-time visibility are critical.

MoneyMart, a leading financial services provider across North America, faced this challenge within a critical operational process. Key data arrived through multiple email inboxes, requiring teams to reference secure network files before updating a large Excel tracking spreadsheet several times per hour. Over time, the spreadsheet evolved into a central operational system rather than a simple reporting tool. As teams created additional files to verify and cross-check information, the process became fragmented, time-consuming, and difficult to scale.

Traditional automation options were limited. Strict compliance requirements, internal security protocols, and legacy systems meant many integration platforms were either unsuitable or required costly system overhauls.

Wrk partnered with MoneyMart to automate this workflow without replacing existing systems or requiring months of implementation.

99%

reduction in manual effort

Wrk designed a secure automation that continuously monitors designated inboxes, accesses secure network files, consolidates the required data, and updates Excel tracking logs in real time.

As a result, daily email reviews dropped from approximately 1,300 to just 10, representing a **99% reduction in manual effort.** This reduced the burden of data entry and reconciliation while improving accuracy in regulated financial processes. By automating a process that previously accounted for roughly **10% of the team's workload**, MoneyMart improved operational efficiency and can now scale securely with real-time visibility.

Learn More

How MFSG approaches ethical AI

Against this backdrop, the question of how MFSG is integrating AI into its operations is both commercially important and ethically complex. AI – a broad term covering machine learning, automation and data analytics tools that enable systems to perform tasks that previously required human judgment – has become one of the most discussed topics in financial services. It also carries significant compliance and governance implications.

MFSG has chosen a deliberate, structured path. Karina describes the company's approach as twofold. On one hand, the business does not want to suppress innovation by being overly cautious. On the other, it is applying "industry best practises of rigour and governance" before any AI solution comes into contact with customers or their data.

Central to that governance is a cross-functional council that the executive team has established. This body does not evaluate AI in isolation. It brings together representatives from risk, fraud, privacy, compliance, legal, operations, technology, data and credit risk – a group, as Karina puts it, that views AI "with a 360-degree lens". Karina says: "We've stood up a council that doesn't just look at AI in a vacuum. We're considering AI, data and technology enablement together."

Many AI projects in financial services fail, Greg argues, because organisations reach for AI as a solution in search of a problem.

MFSG's approach is the reverse: identify the business problem first, then assess whether AI is the right tool. Greg explains: "We are not looking for reasons to use AI. We are looking at our business problems and then seeing how we can attack those through people, process and technology." AI, he adds, is "one tool in the toolkit" – not the whole answer.

All current AI implementations at MFSG operate on a human in the loop basis. This means that no automated system makes a final decision without human oversight. Karina is transparent about the fact that the company has not rushed to deploy AI broadly. "We haven't been bullish on just launching everything and anything," she says. "We're staying very sandbox, test first, human in the loop in all our solutions today. That will change, but only when we're ready and we've got the right infrastructure and governance in place."

WATCH NOW
MFSG: Greg Root and Karina Sidhu on how AI is changing risk

Navigating regulation across borders

Because Money Mart operates in Canada and in various US states, legal requirements have to be built market by market. A loan product, payment flow, customer disclosure or data use that works in one jurisdiction may need to be configured differently in another. That makes compliance a practical design question for legal, operations and technology, not a final review step.

Greg describes the process in practical terms. MFSG's legal and compliance team identifies the rules that apply in each market, then works with operations, retail and technology to turn those requirements into process, training and system logic. For Money Mart, that means compliance has to be built into how products are designed, how branches operate and how digital journeys work. Greg says: "Compliance is key. We are in financial services, but there are also opportunities within regulatory change – and there are things that can have a negative impact to your business. You need to map that out."

That mapping also shapes business planning. A regulatory change can affect which products Money Mart can offer, how quickly a new feature can launch, what disclosures customers see and what the economics of a product look like. MFSG's regulatory change process therefore looks beyond the legal requirement itself and asks what the change means for growth plans, profit and loss and customer experience. "Technology change doesn't happen overnight," Greg says. "We need lead time and we need to understand the impacts of staying compliant."

Karina adds that MFSG uses compliance as a driver of process improvement. Rather than treating new regulations as a burden, the company considers whether the related process can be made clearer for customers and easier for front-line staff to explain. "We've been proactive about regulatory changes and embracing them," she says. "What we often do is use them to enhance our existing business processes and create more transparency."

System modernisation and the cyber challenge

The challenge of modernising core technology systems without increasing the company's exposure to cyber threats is one that Karina approaches with particular seriousness. As MFSG's CTO, she also carries responsibility for the company's cybersecurity function.

She is direct about the complexity. Core financial systems – the platforms that manage lending decisions, payments, customer accounts and regulatory reporting – are rarely simple. They carry years of bespoke, jurisdiction-specific logic, often with compliance rules built directly into the code. Replacing or modernising them is a slow, careful process. “No tech modernisation is easy in financial services,” Karina says. “These are processes built up with bespoke logic that have regulatory logic, compliance mechanisms built in. Modernising is key to transformation, but not a simple journey.

MFSG’s approach is to work with seasoned, reputable technology brands – and to modernise incrementally rather than all at once. The strategy is to improve one part of the technology stack, prove it works and then move to the next. This modular approach is designed to limit risk and business impact of any given project reducing the window of exposure during any transition period.

Greg adds that MFSG’s enterprise transformation office – a dedicated team that oversees process and change programmes across the business – plays a critical role in ensuring that technology modernisation and risk management are treated as connected challenges rather than separate workstreams. “The transformation team brings everyone together,” Greg says, “so that we can understand the problem holistically and align the business goals with our end state solution.

Data as the foundation of everything

Underpinning all of this – the AI strategy, the compliance work, the modernisation programme – is data. Both Karina and Greg are unambiguous about its importance and equally unambiguous about the risks of getting it wrong.

Karina argues that organisations often treat data as a conceptual asset without clearly defining its purpose. Instead, she advises starting with the problem: identifying the specific question the data needs to answer. From there, organisations can “classify data where you need to and protect the right type of data”. Not all data requires the same level of protection, nor is it equally valuable. Being precise about classification – determining which data requires the highest levels of security and which does not – is, she argues, both a governance imperative and a cost-management discipline. Karina explains: “The key thing is know what you’re solving for – have a prescribed approach that manages cost, security and protection.”

“AI will allow us to do things we wouldn’t have otherwise been able to afford to”

Greg Root
Chief Operating Officer
MFSG

Greg brings the commercial dimension into focus. The shift from intuition-based decision-making to data-driven decision-making is, he argues, one of the most significant changes that AI and automation are enabling in financial services. But the quality of the output is entirely dependent on the quality of the input.

"If the underlying data isn't correct, you're just pushing bad data out faster and in an automated fashion," Greg says. "It really is the key to moving forward." The goal, he adds, is to reach a point where the organisation has a single, trusted source of truth – data that is safe, accurate and reliably understood by everyone who uses it.

Karina puts the stakes in even sharper terms. Data-driven organisations earn customer trust by factually understanding their needs. But that same personalisation can backfire catastrophically if data is ever compromised. "If their data is ever compromised, customers are not going to be happy that you thought you knew everything about them," she says.

She continues: "It is a double-edged sword being a data-centric business," which still rings true in the headlines seen today.

For Karina, this is why the data conversation must sit alongside – not after – any discussion of AI transformation or risk strategy. "The conversation around data must go hand in hand with any AI transformation risk discussion that anybody is having," she says.

Momentum™
Financial Services Group

20 Toronto St.
Toronto, ON
M5C 2B8

mfsg.com

POWERED BY:

BizClik