RELX
13th May 2026
Investor Seminar
Risk Business Services

Transcript

Disclaimer
This transcript is derived from a recording of the event. Every possible effort has been made to transcribe accurately. However, neither RELX nor BRR Media Limited shall be liable for any inaccuracies, errors, or omissions.

RICK TRAINOR – CEO Risk Business Services

Good morning, good afternoon & welcome. I am Rick Trainor, the CEO of Business Services within LexisNexis Risk Solutions. I have been with RELX for over 20 years having joined through the 2004 acquisition of Seisint, and I have been leading Business Services since 2009.

[Slide 3]
Today, we are going to give you an update on Business Services, with a particular focus on Fraud & Identity.

I will walk you through our strategy – highlighting our sophisticated data analytic capabilities. You will then hear about our technology approach from Risk CTO, Vijay Raghavan. We will then bring the Fraud and Identity business to life with two deep dives. Kim Sutherland, VP and Global Head of Fraud and Identity, will take us through a customer case study on how customers use our fraud and identity solutions. We will then have Matt Adams, CTO and Cofounder of IDVerse and Dan Aiello, Chief Product Officer and Cofounder of IDVerse walk through a new account opening case study. Afterwards, Vijay and I will come back for Q&A.

[Slide 5]
Let me start with where Risk fits within RELX. In 2025, Risk represented around 36% of RELX revenue and about 39% of the profit. Our full year revenue in 2025 was £3.5bn or about $4.6bn.

[Slide 6]
The long-term fundamentals of the Risk business are strong. We have continued on a strong and consistent growth trajectory with average underlying revenue growth of 8%. While there will always be some fluctuations across cycles, you can see consistent 7-9% growth over the last decade with the exception of 2020 due to COVID. Our main business segments have an average growth rate roughly in line with the divisional average and fluctuations tend to cancel each other out over time. We're not only a high revenue growth business but also high margin. And a key factor in this is our scale and the ability to reuse our unique data assets, our technology, and linking and AI capabilities in each of our key segments. This coupled with a focus on continuous process innovation helps us manage cost growth below revenue growth. And the gap between underlying revenue growth and underlying adjusted

operating profit growth is widening with the advancement of technology.

[Slide 7]
While we operate in global industries with structural growth drivers, innovation is the key reason for our consistent performance. We continue to enhance the value we deliver to our customers through new solutions and capabilities that are deeply embedded into their workflows. In this slide, the orange part of the bar is growth that comes from new products…and we define those as products launched in the last five years, which is the typical adoption cycle to roll out new products for us. And new technology is helping us develop and launch products at a faster pace.

[Slide 8]
We have four key capabilities that we leverage to drive innovation and add more value to our customers.

First is our deep customer understanding. We work in close partnership with our customers to help solve some of their most fundamental business challenges. Our solutions are deeply integrated into our customers' workflows where we help inform or automate key decisions, with over 90% of our transactions being machine to machine. Our deep understanding of our customers businesses, combined with our core skill in innovation is a key driver of our success.

Our second key capability is our leading data sets. This is the foundation of our business. Our data assets have been created over decades of licensing, aggregating, linking, and building data. As for scale, breadth and depth of this data, we have tens of billions of public records and data elements across tens of thousands of sources. Most importantly we have many contributory and proprietary data sets that are unique to us and are a core part of our differentiated value proposition. We now have over 25 contributory databases across Risk. This is where our customers contribute their data to us so that we can provide them back risk analytics across the market or across industries to solve specific use cases. I will speak to this in the context of the Business Services use cases shortly. We continue to grow the depth and breadth of our data, and we are also adding different types of data to provide greater risk insights to our customers. It is important to note that we serve customers that operate in highly regulated markets. It is incredibly important that the answers that we deliver to our customers are highly precise, accurate, explainable and compliant.

Our third capability is our advanced linking and analytics. We have a long history of using AI and other advanced analytic approaches. This underpins our linking capability, which allows us to connect these vast amounts of disparate data points to create one unique view of an individual or a business. We also utilize our sophisticated analytics and AI in the solutions we provide to our customers through scoring models, attributes, and diagnostic tools which enables them to make decisions. Our models have been refined and improved over decades utilizing important customer feedback loops. We continue to apply the most sophisticated approaches to ensure our products provide our customers with industry leading quality and accuracy.

And finally, our Technology platforms. We have a fast, scalable platform that allows us to ingest more and more data, and seamlessly plug in new AI technologies. This also allows customers to connect to our solutions seamlessly.

[Slide 9]
We serve four business segments within the Risk division… where we help our customers assess and manage risk and identify fraud.
Business Services is the largest segment and represents nearly 45% of Risk revenue. This is where we'll focus today. Insurance is the second largest segment, at nearly 40% of revenue, Specialized Data Services is just over 10%, and Government is about 5%.
Now let me walk through Business Services in more detail.

[Slide 10]
This slide shows you Business Services revenue by geography, solution, and type. On the left you'll see that we now generate nearly 30% of our revenue from outside of the US. Since I last presented, we have become more global and non-US expansion will continue to be an important growth opportunity and is being driven by the mix of solutions we offer and the relative maturity of each market. In the middle chart I am highlighting the proportion of revenue from local solutions, those built on local data assets for local markets, and our global solutions, which are those data solutions applicable worldwide.

We continue to expand our portfolio of global solutions, which now represents over 45% of our revenue. We have a long runway with these solutions in both the US and Non-US markets and we expect

this to continue to be a core part of our growth engine going forward. Finally, on the right chart, you can see we have a balanced mix of revenue from subscriptions and transactional solutions, and our transactional revenues are under long-term contracts with a volumetric component. There are very few one-time transactions.

[Slide 11]

We serve a large, diverse customer base – with over 18,000 customers in more than 180 countries and territories. Our solutions are developed to meet the needs of customers of every size, from the world's largest and most sophisticated businesses to small and mid-sized businesses. Our revenue concentration is quite low with our top 30 customers making up less than 30% of our overall revenue. Our solutions are used across industries, including financial services, which is our largest customer segment, digital service providers like telcos and retail and eCommerce, and a long tail of others. We also provide solutions that other parts of the Risk division take to market in the insurance, government, and healthcare sectors.

[Slide 12]

We help our customers assess risk associated with a consumer, a business, or a transaction, whether that is fraud, compliance, or credit risk. This helps our customers make higher confidence decisions and makes the transaction process more efficient and safer for consumers. Our business is segmented into three primary business areas.

Fraud and Identity solutions account for a little more than a third of the revenue and is the largest part of our business, and will be the primary focus of today's discussion. What we do here is help our customers evaluate if an identity exists, can it be trusted, and whether a transaction is legitimate. We do this by analyzing hundreds of digital, physical, and behavioral attributes associated with an identity and the transaction to help our customers understand which they should allow through their systems without friction, and which are higher risk, requiring additional levels of diligence, or whether a particular transaction should be rejected outright.

Financial Crime and Compliance accounts for a little under a third of our revenue and is our second largest segment. In this segment, we deliver a suite of solutions that help our customers comply with global regulations such as Know Your Customer, Anti-money laundering, counter-terrorist financing, and

anti-bribery and corruption statutes. We do this by validating that the identity exists and the identity attributes are accurate. We then screen the identity details against various watch lists such as governmental sanctions lists, economic sanctions, and politically exposed individuals and although an identity may have been determined to exist, our customers must also demonstrate that it is legally permissible to do business with them, or to treat them with a higher level of risk.

Finally, the balance of revenue comes from Credit, Business, and other Risk solutions. Here we provide a range of specialized solutions including alternative data solutions for understanding the credit worthiness of consumers and businesses along with due diligence tools. All of our solutions, are underpinned by a combination of highly differentiated data assets and complex analytics, which I will talk about more in just a moment.

[Slide 13]
The challenges facing our customers are large and global, and only getting bigger and more complex. The number of fraud attacks and associated fraud losses are growing driven by automated bot attacks and AI – fraud scams. There are more sanctions and regulations being imposed that must be met by an increasing number of organizations. Cross-border transactions, cryptocurrencies, and other new transaction methods make tracking money flows and compliance harder. And consumers are increasingly using non-traditional borrowing types like Buy Now Pay Later. That coupled with changes to traditional credit reporting make traditional credit files less representative of risk supporting the need for more alternative credit data solutions.

[Slide 14]
With the rapid evolution of AI, bad actors are operating faster and at a larger scale than ever before. There are more sophisticated deepfakes and synthetic identities. And evolving fraud schemes. And more systematic attacks. And for our customers this means that serving their customers and growing their businesses is harder. It is increasingly difficult for them to assess risk and establish trust during a transaction flow resulting in outsized financial and operational impacts.

[Slide 15]
We are incredibly well positioned to help our customers solve these growing challenges. We layer intelligence at every point as our customers interact with their customers enabling our customers to see

a full picture of risk associated with all aspects of a consumer interaction. Our solutions are deeply integrated into our customer's workflows and most of our solutions are machine-to-machine – meaning within a fraction of a second, as a customer is interacting with their customers, we can assess if this is a legitimate person or an agent that they want to do business with, operating on a trusted device, with identity attributes and behaviors that are consistent with recent patterns. At each stage of the process, we verify the connection between the consumer, the device, the agent, and provide intelligence around the risk that helps them make higher confidence decisions. This makes the transaction process smoother, more efficient, and safer for consumers. As a result, our customers can grow confidently, onboard and protect legitimate customers without friction and operate more efficiently and in compliance with worldwide financial regulation.

[Slide 16]

The way we do this is by providing our customers with a comprehensive and multidimensional view of a consumer or a business, including attributes tied to their physical identity, their digital identity and their behaviors. This helps identify when there are patterns during a transaction flow that appear unusual and potentially risky. Our solutions enable our customers to confidently assess whether they should trust the person, the agent, the device, and the behavior associated with whom they're transacting.

[Slide 17]

This deep view of a consumer or business is what fuels our analytics engine. The scale, breadth, and depth of our data assets are truly differentiated. I would like to draw your attention to the following stats that help demonstrate the scale of our network:

We cover virtually all the adults in the United States

We process over 1 trillion sanctions annually

We process roughly 145 billion digital transactions annually

That includes, 81 billion logins, 2 billion new account creations, and 28 billion payments.

[Slide 18]

There are four primary sources of the data in our Risk Intelligence Network – including two foundational and two proprietary sources.

The first foundational source is our public records repository. We have tens of billions of public records from tens of thousands of sources that we have built over decades. Some of the data is no longer publicly available, and some is theoretically public, but extremely difficult and complicated to collect because of the format, general data source availability, or requires manual collection.

The second foundational source is our licensed data, which comes from thousands of different sources to add further intelligence, breadth and context. For these sources, the usage is commercially controlled and regulated, meaning we can only use them in certain ways in our solutions.

And then we have our proprietary, network driven sources. First, we have our contributory data assets which are built through customer interactions with our solutions. To benefit from the value of these solutions, customers must contribute their activity to the Risk Intelligence Network. So, each time a customer transaction happens, the input data, the data attributes, the patterns of behavior, and the outcome of that transaction is captured. This means our data asset is becoming richer and deeper with every transaction.

Finally, we build proprietary derived attributes which further enhance an identity profile or its correlation to risk. All four dimensions are combined to create a longitudinal network of risk insight that grows overtime.

[Slide 19]

This vast data alone has little value to our customers. We transform this data utilizing sophisticated analytics and AI into specific signals and scores and feed that into our customers workflows to assess risk in real-time. We have created a great virtuous cycle. As we process more transactions and outcomes, we are able to see more signals about risk and how patterns of risk are evolving which allows us to create even stronger signals of risk which makes our products stronger and delivers more value to our customers.

Today we see over 400 million transactions every day, and that number continues to grow as we add new customers, as our existing customers grow their usage, and our customers deepen their relationships with us.

[Slide 20]

Our solutions deliver better outcomes for our customers and create significant differentiation in the measurable value uplift we provide. While the solutions we provide our customers represent a small part of their cost base, they have significant positive impacts on the economics of their overall business.

We identify and stop more fraudulent transactions – even in the hardest to assess bands. We deliver less false positives allowing more good customers through without friction. And we make sure only the highest risk transactions are routed to high-cost methods of review. The net of this is higher revenue and lower operating costs for our customers.

[Slide 21]

Customers deepen their relationship with us over time. The left side of this slide shows an example of our relationship with a US financial institution. We initially sold this customer an Identity Verification solution to improve their KYC program. As the customer recognized the value we provided, they adopted more solutions adding new capabilities across more use cases, such as account management and fraud prevention.

While every customer is different, the shape of the journey is very similar across most of our customer base. We price to capture a small portion of the value we provide. As customers see strong price-to-value of our solutions, they increase the number of products they purchase and the depth of our integration into their workflow. As we continue to innovate, we expect that all customers will continue to layer in more capabilities and expand their relationship with us in this way.

[Slide 22]

This slide highlights our strong track record of growth over the past 25 years.
We have expanded primarily through organic innovation, supplemented by targeted and highly complementary acquisitions.

We have a very disciplined approach to M&A, evaluating hundreds of new technologies, new solutions every year. Many of our most successful acquisitions, like ThreatMetrix and Emailage, started as commercial partnerships – which gave us a deep understanding of who has leading capability and what the combined value proposition is for customers.

IDVerse is our latest acquisition, completed in February of 2025, which added AI-powered document authentication and deepfake analytics to our portfolio. Before we acquired IDVerse, we assessed nearly every provider of scale in this space either through partnership or other commercial discussions…comparing technologies, comparing analytics, and testing their ability to catch fraud…this gave us confidence that we were acquiring the most sophisticated capability in the market. You'll see Matt and Dan demo this in just a little bit.
Our customers' challenges are far from static…and our evolving solutions, robust data network, and ongoing innovation keep us well-positioned for future success.

And now let me turn it over Vijay to take you deeper into our analytics and technology approach.

VIJAY RAGHAVAN - Chair, RELX Technology Forum and Chief Technology Officer, Risk

[Slide 23]
Thank you, Rick. I'm Vijay Raghavan. I'm the Chief Technology Officer at Risk. I've been in this role for almost 15 years, and I've been with RELX for almost 25 years. I am also the chair for the RELX Technology forum which shares best practices across the RELX divisions.

Rick briefly touched on our core capabilities, and I'd like to walk through our analytics and technology approach in more detail.

[Slide 24]
Let's start with the function of technology at RELX.

At a fundamental level, we are the enablers of the innovation engine you have heard so much about today.

We help our businesses execute against our growth plans by investing in the right technology capabilities….to enable our teams to innovate quickly and efficiently with the right tools… and to ensure that our systems are flexible, reliable and scalable

Given the nature of our business, it is the role of Technology to make sure we have highly secure environments that protect our customers' data and our IP, and to adapt to changing regulatory requirements

And an integral part of Technology's role is to continuously automate and optimize through the improvement of our processes and our tools

Technology is a real source of competitive advantage across RELX. At the heart of that is our people and their ability to stay at the forefront of the evolving technology landscape. These are highly innovative teams with deep experience and expertise in data analytics and AI and ML techniques and who are motivated to use technology to improve outcomes for our customers, and for ourselves.

[Slide 25]
We have a long history of using advanced technology within Risk.
We first created our big data technology in the 1990s, long before big data was a buzzword.

We then created our proprietary machine-learning based linking technology in the mid-2000s.

We first started talking to you about big data and our usage of analytical algorithms back in 2011.

By around 2015, we had been using AI and ML techniques for over a decade, and that's when we first started sharing externally about how we have woven AI and ML tools and processes into the fabric of our data and our technology.

In 2018, we talked to you about how we used supervised and unsupervised learning in our AI solutions, and how we assessed and evaluated multiple algorithms to provide the greatest value to our customers.

In 2023, I spoke about how we were integrating real-time machine-generated data into our existing fabric of public records data, contributed databases, device intelligence, and digital identities to give our customers even more comprehensive solutions. I also spoke to you then about Generative AI and how it

would give us greater scale to innovate…for example, around knowledge extraction from our data repositories, and automated code generation.

All of these presentations remain available on our website.

What we are doing today with our technology is consistent with our history. We are constantly evaluating new tools to evolve our approach to support better, faster, cheaper innovation, and we use the best and most appropriate tools for the job at hand, to create even more compelling products.

The way this has evolved since the last time I spoke to you in 2023 is that we are embedding Generative AI and Agentic AI tooling into our technology stack. However, since some of these AI tools come with side effects, we have built a trusted AI infrastructure around these tools in order to not compromise the quality and integrity of our solutions. It is paramount that we continue to offer our customers the trusted, reliable, and compliant solutions they have come to expect from Risk even as we adopt new AI techniques.

[Slide 26]
Here's what I mean by that. This slide describes the layers of our technology stack. Across these layers, we use a variety of technologies - including open-source, third-party, and proprietary solutions.

At the bottom of the stack is our infrastructure layer, where we use 3rd party cloud tooling such as servers, networks, storage, databases, and other infrastructure as a metered utility.
These tools are broadly available in the market and are not unique to us. What is important is how we deploy these tools, which we do in a cost-effective and flexible manner.
The more important things in this stack are in the middle and top layers.
In the middle is our abstraction layer which is a proprietary approach that gives us much greater control and flexibility over how we use 3rd party services. We can now easily leverage emerging 3rd party innovations, including Generative AI, LLMs and Agentic solutions offered by cloud vendors and hyperscalers, and switch between these 3rd party services easily. For example, we can integrate a new LLM into our platform within a few hours. But what's just as important is that this abstraction layer helps us ensure that even as we adopt new AI techniques, we don't make trade-offs between the speed

and quality of our answers, or between the quality and consistency of our answers, or between the speed and transparency of our answers. That is critical for our customers.

Resting above the abstraction layer is our Applications and Product layer that represents our core IP, where we ingest data at high speeds, link the data with great accuracy, boil the data down to discrete elements that we call entities, and then build solutions that are easily consumable by our customers. We have been doing this for a long time, but we are continually finding ways to make these approaches better.

[Slide 27]
On this slide, I'd like to drill down just a little deeper into the Abstraction layer and the Applications and Product Layer

Let's start with the abstraction layer. A key element of this layer is our Trusted AI infrastructure that you see depicted in the bottom right. This is crucial, because as we deploy new AI solutions (including Agentic AI and Generative AI), we can assure our customers and regulators that the decisions made by our solutions are transparent and defensible. That's what I mean by not having to make trade-offs.

Our trusted AI infrastructure within our abstraction layer provides us with AI validation guardrails that are superior to pureplay LLM-based solutions that claim to be nearly as good but are either ridden with bias, which is unacceptable to customers; or they are opaque and non-deterministic, which is unacceptable to regulators.

The top of the slide shows two examples of our Applications and Product Layer. Omega AI is our modernized data fabrication process. This replaces our previous generation of technology with one that is cloud-native and AI-enabled. One of the big advantages of our new approach is that we can ingest data incrementally, with near-real-time propagation of data into our products which significantly improves the value we provide to our customers.

The Entity database is the other example. It serves as another force multiplier for us, because it is a canonical, entity-centric representation of data that gives all our products a shared model of entities and relationships. Entities could be people or businesses or vehicles or driver's licenses and so on.

Essentially, we are using AI to create consistent, reusable, and well-connected entities across our platform, for us to not only be able to build our products more easily, but also to create an ontology of digital entities that adds much greater value to our customers.

[Slide 28]
Now let me touch on how we build our products with this technology stack I just described. You have seen this slide before, but it is an incredibly important one. It demonstrates how we get from data to specific actionable insights that help our customers make decisions.

Rick touched on the scale and breadth of our data assets but big data itself is not of much value to our customers. Our technology transforms big data into small, actionable intelligence at scale and at high speed to add value to our customers' decisions – for example, in the form of identity authentication or device authentication or agent authentication. And to give you a sense of scale and speed, our ThreatMetrix product verifies 200 different data points for each transaction it sees within sub-seconds and it does this across 400 million transactions a day.

We do this by layering advanced analytics on top of our data and to cluster, link and identify patterns to improve our solutions. This is what we call extractive AI and it is at the heart of Risk's competitive advantage.

As Rick said earlier, over 90% of our transactions in Risk are machine to machine, in the form of scores or attributes, as opposed to generated text that a customer needs to analyze or interpret. So it is incredibly important that the answers that we deliver to our customers are highly accurate and compliant and that they are consistent meaning a customer always receives the same answer in the same situation with the same inputs. That is quite difficult in the probabilistic way LLMs operate – where answers may evolve over time. Our reliable, deterministic approach is critical because of how we integrate with customers and also because of the regulatory nature of our customers' use cases.

We've honed our proprietary algorithms over decades to continually improve these parameters and to create more and more sophisticated techniques which continue to enable industry leading accuracy with fast cycle times and at lower costs.

[Slide 29]

Due to the nature of the Risk business, extractive AI is fundamental to our solutions. However, we also deploy Generative, Agentic, and other AI capabilities. We layer them on top of our extractive AI approach.

You'll see a few examples here on this slide.

The 1st example is related to Image Analytics in Insurance. In 2023, we talked about our Flyreel product, which is an AI-based image capture solution that allows a layperson to capture video of their property in a home insurance underwriting context or a video of their automobile after an accident in a claims context. We have continued to find ways to improve the way videos are automatically analysed in the background using increasingly advanced algorithms to process those images, assess context and risk, and extract relevant data into our platforms.

The next example is LexID – which is our proprietary approach to link our data assets together in a highly accurate manner. Our linking underpins nearly all of our solutions and we have continued to refine our algorithms to improve our linking over decades. Today we have industry leading linking accuracy. However, we continue to find ways to improve that linking to get even closer to perfection because every incremental bit of improvement in accuracy improves value for our customers. We are now using Generative AI and Agentic AI techniques, coupled with a human-in-the-loop to map raw unstructured data into structured data even more accurately and to further improve our linking accuracy.

The third example on the slide has to do with our IDVerse solution, which you will see in a demo a little later in the presentation. Fraudsters are getting more creative every day with deepfakes. Our proprietary neural network within the IDVerse platform is being constantly enhanced to detect new fraud patterns. For example, two years ago, it would have been sufficient to rely on facial landmarks, eye movement and lip sync to detect fraud. Fraudsters are now able to get past that, so now we've enhanced our neural network to detect liveness by using skin spectral analysis, and optical flow analysis which tracks involuntary movement of facial muscles due to blood flow. Our neural network handles document authentication, biometric face matching, liveness checking, depth-based 3D analysis, injection attack detection and deepfake classification all in a single pipeline – which makes it incredibly sophisticated in identifying fraud. Again, you'll hear more about IDVerse a little later.

These are just some examples of how we are continuing to leverage more and more sophisticated technology to improve the value we deliver to customers…and there are many more.

[Slide 30]
We are also using our technology capabilities internally to enable us to improve processes and make our people more effective in their day-to-day work. You will see a few examples on this slide. I won't walk through all of these, but I will touch on a couple of examples. In our Technology function, we are actively employing AI-assisted coding, which is clearly helpful for product development, but especially interesting is the value it adds to the upgrading of systems, implementing new technology, and advancing our cybersecurity defenses. We do so aggressively but judiciously, in keeping with our approach of including a human in the loop.

There are many more examples across all of our functional are some of which you see here.
We continue to find ways to apply technology internally to operate with more agility and more effective which in turn allows us to innovate faster and serve our customers better.

[Slide 31]
So to wrap up, I hope you walk away with a better understanding of how we use technology at Risk.

Our technology and analytics approaches play a central role in enabling rapid, agile, and low-cost innovation across the business.

We have used AI for decades and continue to deploy the most advanced methods to constantly refine the accuracy and value of our product and enhance the effectiveness and efficiency of our internal teams.

And as technology continues to get more and more advanced, we are well positioned to adopt these tools quickly, deploy them in the most appropriate manner and strengthen our position over the long term.

With that, I'll turn it over to Kim Sutherland to bring our technology to life with a customer case study.

KIM SUTHERLAND - Vice President and Global Head of Fraud and Identity

[Slide 32]
Thank you, Vijay. My name is Kim Sutherland, and I am the Global Head of Fraud and Identity. I have been with Risk for 20 years and during most of that time, I've been focused on building our commercial market strategy for our portfolio of fraud and identity solutions.

[Slide 33]
The way that consumers interact with businesses is evolving and increasing in complexity. During a single interaction a consumer may log into an account on their phone, move from a mobile app to a website, issue a real time payment, and initiate an account-to-account transfer. We are seeing a growing number of interactions through more devices and channels from mobile browser and digital wallets and now to the emergence of Agentic commerce. And this growth means more opportunity for fraud.

Recognizing trusted behavior — and detecting anomalies in real time, across every device and every channel — is no longer optional. It is a baseline expectation.

[Slide 34]
Vulnerability to fraud attacks persists across the entire consumer lifecycle.
We help customers reduce fraud by layering defenses at each of those touchpoints.

The first layer, Digital and Identity Assessment, uses device, location, behavioral, bot and agent intelligence to establish trust from the very first signal, in addition to the basics like identity attributes such as email address, name, and phone number they're also verified.

The second layer applies Decision Analytics - adaptive fraud analytic models, machine learning, and orchestration - to identify anomalies and velocity patterns in real time.

The third layer adds Authentication - from passive methods to bind a trusted device to active methods including biometrics and document authentication.

And the fourth layer - Investigation and Review - closes the loop with forensics, case management, and even the incorporation of fraud feedback.

We leverage an integrated platform for dynamic and coordinated use of these solutions and underpinning the layers is our Risk Intelligence Network - ensuring that every signal adds the required context to assess risk for every interaction.
How these capabilities are deployed is determined by the customer. This enables a fast, frictionless experience for the vast majority of consumers and transactions that are low-risk while providing strong protection when there are signals of fraud.

[Slide 35]
A consumer transaction can seem very simple. But behind that moment thousands of data signals are being collected and analyzed. Fully automated risk decisions are running in real time, and fraud risk models are scoring the interaction. This is done in approximately 85 milliseconds and over 400 million times a day.

And at the core of that decision engine are three fundamental questions.

First — who is this? Does this identity, device, behavior, and combination of signals have any history within our network? Identity recognition is the foundation of trust.

Second — can they be trusted? Are the attributes accurate? Is there any suspicious activities associated with this behavior, this device, or this identity? And critically — is this person a victim themselves, potentially being manipulated without even knowing it?

Third — do we need more proof? Ambiguous signals require further verification.

[Slide 36]
Our approach turns disconnected signals into a single, connected digital identity.

Every digital identity creates data in our network — an email address, a device and how you interact with it, a phone number, a billing address, a payment card, a location. In isolation, each of these signals tells a partial story. But connected together, they can reveal something far more powerful: a trusted identity.

A typical user has one to two email addresses, two to four devices, and two to four payment cards. When something shifts — a new device, an unfamiliar location, automated filling of identity attributes, or behavioral signals that suggest the user is being coerced, which is a hallmark of sophisticated fraud.

Our network recognizes those moments.

[Slide 37]
Let's walk through an example of a consumer logging into their account.
What I'm showing here is an example of how our customers protect digital logins while keeping the experience seamless for trusted users.

On the left is the consumer experience — a familiar login screen. On the right is ThreatMetrix and Behaviosec working together in real time.
As soon as a user lands on the page, we begin building risk context using device, network, and hardware intelligence

Now, I'll complete the login. And you'll see that the outcome is a pass.

In near real time — tens of milliseconds — all of these signals are evaluated behind the scenes – with no impact to the user experience.

What's important for our customers isn't just the decision — it's understanding why that decision was made and that's where reason codes come in.

Reason codes provide transparent, explainable insight into what contributed to trusting this user. In this case, we're seeing multiple positive signals come together.

This is a recognized user logging in from a known device

There’s established historical behavior over time — not a one off interaction.

And this identity is trusted across the digital network.

Together, these signals create high confidence that this is a legitimate, low risk user.

Now let’s look at a different example.

Here a consumer is registering an account with one of our customers. This is the customer’s first time seeing this consumer, and the only data they have are an email address and a device. On its own, that’s not enough data to confidently assess risk.

With our network, we layer in significantly more intelligence. Through our solution, that same email is seen transacting successfully elsewhere — linked to known devices, established payment behavior, and consistent with digital and behavioral patterns across our other customers.

Now we're looking at the same flow, but with a bad actor – here, a fraudster is reusing stolen credentials at scale. On the surface, these look like separate transactions — different emails, different devices, all appearing unrelated.

But our network and sophisticated linking resolves these events into a single identity — not by depending on the device, but by linking across email, location, and behavioral patterns across our network. Even as the fraudster rotates devices or spoofs credentials, the identity holds.

These devices and emails are no longer isolated events but a singular view into a customer’s digital journey

[Slide 38]
So now let’s apply this in a case study.

In this instance, one of our banking customers, utilizing our layered fraud solutions, noticed a bad actor trying to use stolen credentials to access an account… This same device made multiple attempts to log into the account using different stolen credentials in a short period.

In real-time, we connected the device, the behavior, and network intelligence and flagged the behavior as suspicious— and inconsistent with a genuine user – and we immediately stopped the fraud attempts and our customer avoided any associated losses.

The scale and visibility of our network enabled us to link that one incident to multiple connected devices and prior fraud activity instantly. From a single suspicious device, we identified 26 additional high-risk devices and blocked 18 more fraud events across 18 different organizations. The result — we were able to stop a coordinated fraud ring that was moving across institutions and channels…and additional customers were able to quickly prevent losses.

No single institution could see the full picture on its own; however, one incident prevented fraud across our entire network.

This example demonstrates how the scale and global reach of our network deliver significant, measurable value to our customers.

So I will now turn it over to Matt and Dan to walk through how we create a safer new account opening journey

MATT ADAMS - Chief Technology Officer and Co-founder, IDVerse
DANIEL AIELLO - Chief Product Officer and Co-founder, IDVerse

[Slide 39]
Thank you, Kim. My name is Matt Adams, and I am the Chief Technology Officer and Co-founder, IDVerse.

And I am Daniel Aiello, Chief Product Officer and Co-founder, IDVerse.
We founded IDVerse in 2016 and have been with Risk since the acquisition last year.

Together, Matt and I lead product and technology for the IDVerse product suite, including the platforms and identity verification capabilities our customers use globally.

[Slide 40]
New account opening has always been one of the most demanding trust decisions in financial services. Institutions make a binding decision about a new customer with very limited history at the moment of decision. Bad actors only need to succeed once.
There is constant commercial pressure to approve quickly, because digital growth depends on it. And when something is flagged, the fallback is manual review, which is expensive, slow, and inaccurate, and creates significant consumer friction.
Every safeguard introduced to mitigate risk, from CAPTCHA to SMS one-time passwords, document data checks, Q&A, phone calls - adds friction to the customer experience and are often insufficient. Financial institutions have long balanced three competing imperatives: growth, friction, and protection.

[Slide 41]
That balance has been fundamentally disrupted by AI. Our own Risk Intelligence Network sees this in the data. In 2025, synthetic identity fraud attacks tripled within the 12 month period.

Fraudsters are producing complete synthetic identities, fabricated documents, fake faces, and deepfake videos. Breached personal data supplies abundant raw material. Credentials trade on underground marketplaces for as little as ten dollars. Neural-network-generated fake IDs for around fifteen.

Generic AI tools and frontier models are not designed to detect these threats.

[Slide 42]
What you are about to see is a recorded demonstration showing how a fraudster, or an agent, generates a synthetic identity document using a Generative AI model. These are fraudulent models, hosted on underground sites. Sites like this are real and persistent.

As the demonstration begins, the fraudster selects a country and state and in some cases with a physical or digital mobile driver licence. Genuine stolen or leaked data can be purchased and injected directly. A synthetic face is generated, or a real one substituted. The output, in seconds, at almost no cost: a very convincing identity document image, sufficient to open a new account at companies without the right safeguards.

The attack method has also evolved. We are now seeing AI agents deployed - prompt-injected to act as adversarial networks, attacking the bank's defences autonomously and at scale.

We can now see the fraudster prompt an LLM to target multiple banks and open accounts, running the IDV process with the synthetic data generated earlier. It is a guard-railed demonstration that simulates a real, coordinated attack. As you can see, the Agentic AI replicates a human's interaction: submitting the ID image to defeat template-based checks, and presenting a face image or video to spoof liveness.

The volume and sophistication of attacks are clearly increasing.

[Slide 43]
To combat this risk we offer IDVerse - integrated with the broader Risk Solutions fraud defence platform.

Here we see a customer visiting the website of a bank to apply for a credit card. They choose their preferred card and proceed with their application.

The first step the bank requires is identity verification. By using IDVerse embedded within its website, the bank can verify the applicant's identity while also capturing trusted data to pre-fill the application, reducing friction for the customer.

The applicant taps Start Verification, which seamlessly opens the IDVerse identity verification flow. They view and accept the privacy consent, they are shown instructions and move to capturing their identity document – we are also able to support a growing list of digital IDs – they confirm the extracted details, and present their face for the biometric checks - and within seconds, the user is verified and returned to the banks site to complete their credit card application.

What the customer experiences as simple, is anything but.

[Slide 44]

Behind that short process, multiple layers of proprietary technology operate simultaneously orchestrated by the neural network, combining physical identity data from the document, biometric intelligence from the face, and digital identity intelligence from the broader LexisNexis network.

Across these layers sits IDVerse's purpose-built neural network, engineered specifically for identity and fraud. It is not a general-purpose LLM or third-party AI model. It has been trained for over seven years on real-world fraud attempts not available in public datasets and is updated continuously as new threats develop.

Let me explain the three primary layers of our technology.

[Slide 45]

Layer 1 is document authentication. The physical or mobile digital ID is analysed using our purpose-built AI, designed to detect subtle fraud patterns, document inconsistencies, and a wide range of attack vectors and methods seen across our network.

It performs up to three hundred automated checks. Some of these including pixel-level analysis, colour consistency, lighting angles, micro-security features, font integrity and screen detection, along with file-level metadata analysis.

It recognises virtually all government-issued IDs, across more than 200 countries and territories, and more than 140 languages.

The outcome: A real, trustworthy, and present ID document with a real identity on it.

[Slide 46]

Layer 2 is biometric liveness and face match. The face presented by the applicant is analysed using purpose-built proprietary liveness and presentation-attack detection.

The system detects synthetic injection attacks, including deepfakes, two-dimensional and three-dimensional masks, screen replays, and AI-generated face-swaps, all server-side, without requiring additional steps from the user.

Once confirmed live, the face is matched against the document using our own face-matching engine. Engineered for real-world variation and differing document standards.
The outcome of Layer 2: a live, present person, confirmed and matched to their document.

[Slide 47]
Beneath the document and biometric check is Layer 3 which is a context layer - assessing the device, the network, the behaviour, and how they compare against everything the network has previously seen.

Risk Intelligence Network was covered in the previous case study. What matters here is what it brings to the decision: every applicant is assessed against signals drawn from more than three hundred million daily transactions, contributed by institutions across the network - so every customer benefits from what every other customer has seen.

Document. Biometric and Digital identity. Three layers, each with deep capabilities beneath them - and together they give our customers the confidence to open good accounts, safely.

[Slide 48]
The impact is measurable. Modern AI-enabled fraud, including deepfakes, synthetic identities and coordinated attacks, are stopped before accounts are opened. Legitimate customers complete onboarding in seconds, manual review volumes fall, and the bank can scale digital growth safely. Demand for these capabilities has accelerated across our global customer base since the IDVerse acquisition. As AI-enabled attacks scale, institutions are moving to layered defence because their existing tools cannot keep pace. That demand reflects a clear market reality: AI-enabled fraud cannot be met with static, general-purpose tools.

It requires specialist capability, deep data, expert human judgement, and scale that compounds. That is what LexisNexis Risk Solutions provides, and what this market is increasingly reaching for.

Now let me hand it back to Rick.

RICK TRAINOR – CEO Risk Business Services

[Slide 49]
Thank you, Matt and Dan.

In summary. We have leading positions in attractive growth sectors…AI is accelerating the volume and the complexity of fraud, which is increasing customer demand for our solutions… we are well positioned to help our customers address these challenges by providing them a better, more holistic view of risk through every interaction they have with their customers, delivering a measurable value uplift.

Our objective is to continue to deliver strong underlying revenue growth, in the high single digits, for a long time to come, a decade or more, driven by organic product innovation, supported by targeted acquisitions.

We are well positioned to continue to adopt new technology to add greater value to our customers, accelerate the pace of innovation, and operate more efficiently, with underlying profit growth exceeding underlying revenue growth.

We will now be happy to take your questions.

Moderator: The first question today comes from Nick Dempsey with Barclays. Please go ahead.

Nick Dempsey: Yeah, good evening or good morning if you're in the US. So I have three questions. The first one, have your customers so far asked you to work together with some of the big AI modelling companies so that you combine your data with other big processes using AI that are running through the institutions that are your customers and how do you respond to those requests if you had them? Second question, can Agentic AI be trained specifically to beat your network and

effectively stay ahead of you in terms of fraudulent activity, find the way through all of the sophistication you've been presenting to us? Third question, there are 12,000 technologists across RELX. I know that's across the whole business, but I guess that's pretty weighted to Risk. Do AI tools present an opportunity to make some headcount savings here over time?

Rick Trainor: Yeah, just give me a second just so I get all three of these now. Yeah, so have our customers been working with us? I think the first question was, have we been working with our customers with the likes of some of the big AI companies? We're working with our customers that help identify how they want to deploy, how they want to begin accessing our systems, assessing our risk signals and intelligence into their AI models. We're not there yet in terms of customers actually integrating yet into our systems, but certainly the discussions are being had around how do we get access to those signals to inform what our financial services customers are doing to help them better stop fraud on their side. And from the financial crime perspective, the alert remediation space, certainly they're interacting with us already, pulling our signals into their Agentic processes for false positive remediation, a level one and level two.

And then second question, can Agentic AI be trained to find a way to break through? Vijay, can you help me address that?

Vijay Raghavan: Yeah, certainly. The way I would answer that question is when we talk about the solutions we provide our customers, there's this very delicate balance between a term that we use called two terms, position and recall. Our customers use the same term, but the concept is the same. Precision is a measure of whether we're giving accurate answers without giving spurious answers. So when Rick talked about false positives, that's what we mean. So agentic AI, sitting on top of an LLM does not do that very well. It can be used to augment what we do or we ourselves use to augment what we do, but using agentic AI in and of itself might cause a problem where in fact customers will try to build solutions themselves without our data or without our trustworthy AI. They might have a precision problem where they generate lots of false positives.

So for example, in the financial crime and compliance space that poses a cost problem or an expense problem to our customers. So what do they do? They try to cast a smaller net, whether it's using Agent AI or using some other LLM and they try to improve the precision, but that causes the opposite problem, which causes a recall problem. So the short answer to your question is, Agentic AI in and of itself is not going to compromise the quality of our solutions. You need the data, the breadth of the data assets that we have along with the domain expertise that we have, along with AI tools we have, all that put together is what renders the value that we offer to our customers. And the third part as well, about the 12,000 technologists. So we are absolutely seeing value in generative AI, in AI assisted coding tools. So we are actively experimenting with these. Last year we saw value, but the value that was generated by these tools was also compromised to some extent because of the technical debt that was creating, meaning it wasn't adhering to our standards. Now because of the evolution of concepts like spectrum and development, we are seeing improved value where not only is AI assisted coding helping us, but it's also using our tools and our technology stack. So there is promise, but I will say that while we expect to see some margin improvement over time as a function of better utilisation and productivity of technologies, I do think that some of the productivity will be used to bolster our products, improve the quality and security of our products. So it's a mix and match. Improve our productivity with the gains and also see some margin improvement. Thank you.

Moderator: The next question comes from Henry Hayden with Rothschild & Co Redburn. Please go ahead.

Henry Hayden: Yeah. Hi, everyone. Thanks for taking our questions. We had three on our end. So the first one was on international expansion. You mentioned that you have 45% of your revenue is tied to globally applicable solutions, but so far if we look at the divisional level over the past, let's say five years, has been a fairly limited mix shift in terms of geographic exposure. So we were curious as to how that 45% has evolved over time and how you're thinking about the algorithm going forward from here. Second question we had was around the moats around the

data that feeds some of your solutions. Fairly comfortable with the moats around data and fraud and ID, but more curious as to that in financial crime and compliance, as well as business and credit risk. What level of propriety surrounds that data and what prevents a competitor from potentially aggregating it? Then the third question I had was on customer captivity. So given your primarily indexed to financial institutions, I appreciate there's quite a degree of captivity around answers need to be accurate. Does that same sense of, let's say, a competitive advantage read across to other customer segments as you look to expand there? Thanks.

Rick Trainor: Okay, great. I'll take those. So international expansion, couple points there. Our revenue mix right now is 70 / 30 and our global products, those that are unbounded by local data assets is 45%, roughly half and half. The mix has improved on a revenue side and that's where our international businesses are growing slightly faster than our divisional average and slightly faster than the US. The US is quite strong as well. So we're seeing both of those markets grow and that's why that expansion from when we last spoke has improved, but maybe not as dramatically as you may have thought. But yeah, it continues to see a strong movement between taking our global products around the world and getting expansion there. But again, the US is quite a strong market for us as well, so we see strong growth there. In terms of moat, I think the question was around what is the moat, you understood the moat relative to our fraud and identity solutions, but let me back up a minute.

The data that we use in fraud and identity is the same data that we use across our financial crime and compliance suite as well as our credit risk. So that highly proprietary nature of our public records, our licence content, our network data and the analytics and risk insights that we build off of that all goes into our data repository. And that data is used in financial crimes for Know Your Customer and account onboarding. So a lot of those same insights and differentiation and distinction is applicable to financial crime as well as credit risk. The credit risk data assets, it's all about ability and willingness to pay. And we use the same data asset and build those insights to drive it into the credit risk space. So the

moat is equally across all three of those sectors. And then finally, I think the last question was around is the, what was the question?

Henry Hayden: Relative customer captivity from financial institutions versus other customer segments.

Rick Trainor: Yeah. I mean, our solutions are the same across customer segments. So the reliability, the accuracy that we build into financial services are also built into those other sectors as well, if that's where that question was going.

Henry Hayden: Yeah, that's very clear. Thank you.

Moderator: The next question comes from Jo Barnet-Lamb with UBS. You may go ahead.

Jo Barnet-Lamb: Excellent. Thank you very much. You referenced that you have 25+ contributory and proprietary databases. I think that was in reference to Risk overarchingly rather than Business Services. Is that correct? And if so, how many do you have in Business Services? And I'm sure this remains a very small proportion of your data sets, but could conceivably drive a significant proportion of the value you create. It sounds like it's the combination of many data sources that multiplies the value creation. Is there any way you can frame the influence on outcomes that your proprietary databases have? What proportion of outcomes are touched by proprietary data in some form? Thank you.

Rick Trainor: Yeah, so you're right. The overall risk contributory databases is 25 or so. Business Services has 10 and it's an area that we've been really focused on the past 10, 15 years, driving more and more contributory sources, whether it's network activity, whether it's outcome data supplied back by our customer. So it is a significant source of our data. And in fact, on a daily basis, we're getting more data signals from that data than our licencing and direct sourcing public records data. So it is a considerable value add. In terms of specific proportions, I don't have that number offhand. It's not something we track, but it is a significant value contributor and significantly differentiated. Was there another part to that question?

Jo Barnet-Lamb: Thank you. Well, not really. I mean, I think you've given me what you can give me. I mean, you did reference that you're getting more data signals than from your licencing and direct sourcing. Could you explain a little bit more of what that actually means?

Rick Trainor: Yes. When you think about what's happening every day with our network activity, we're seeing over 400 million signals a day coming through and there are multiple elements to that signal. So that contributes to our data reposit each and every day, and that continues to grow and grow. And actually in the past three weeks, we had some peak days over 500 million. So the signals that we get from those contributory, and that's just one of these contributory sources, is significant and continuing to differentiate and add value across the portfolio.

Jo Barnet-Lamb: That is helpful. Thank you very much.

Moderator: Next question comes from Christophe Cherblanc with Bernstein. You may go ahead.

Christophe Cherblanc: Yes, good evening. Thanks for taking my question. I had one question about customer value proposition. Revenues have been growing high single digit. You were mentioning digital interaction going up, I think 13% per annum, attacks going up 15%. So I think that's giving us a sense of the improvement in the value proposition. If the intensity of attacks is going up as you were stressing, do you see room to extract a bit more value from what you bring to your customers and should we expect acceleration reflecting that increase risk exposure for your clients?

Rick Trainor: Yeah. I mean, our portfolio is roughly $2 billion annually and we expect to see upper single digit revenue growth rates with profit exceeding the growth rate in terms of acceleration or volumes there. Certainly we are seeing more volumes across the digital portfolio with fraud attacks escalating with AI-driven deep fakes and things like that, but it all gets blended into the overall mix. So our guidance on revenue growth remains in that upper single digits overall as a portfolio.

Christophe Cherblanc: But would you say it's fair to assume that the customer value proposition is accelerating versus what you had two, three years ago?

Rick Trainor: Yeah, absolutely. We continue to add more and more capability to the portfolio, continue to expand the value that in the case of ThreatMetrix in our digital solutions bring as well as all of our other solutions bring to the marketplace. So we continue to see strong growth across the portfolio.

Christophe Cherblanc: Okay. And just one last one related to that. You mentioned that you were a low share of the cost base. How low, is it way below 1%? Because based on the client base and the numbers you were mentioning, it seems to be pretty low numbers on an absolute value.

Rick Trainor: I apologise, I missed the first part of that last question.

Christophe Cherblanc: Well, you mentioned that your products were a low share of the cost base of your clients. So I was just trying to get a sense of how low the share was. Is it below 1% of the client cost base? Is it 0.1%, 0.5%?

Just an order of magnitude would be helpful.

Rick Trainor: I don't have a specific on that, but it's a low percentage, single digits percentage if I was to make an estimate.

Christophe Cherblanc: Thank you.

Moderator: The next question comes from Steve Liechti with Deutsche Numis. Please go ahead.

Steve Liechti: Yeah, Hi there. Thanks. I've got three as well. Just going back to one of the previous questions actually, the consistent growth at 7% to 9%, which is a great growth rate, but given as you've alluded to in your previous Q&A, the market and attack growth are growing higher than that. You're innovating very strongly. So I'm just trying to figure out why 7% to 9% is the right number going forward from here. That's the first question. Second question, I don't think you gave a

customer retention number or percentage. Can you give us anything that you can on that for Business Services or broader? And then the third question is on competition apologies, but could you just educate me in terms of who you see your key competitors as being and whether there's been any kind of new innovators in the market that you've lost any share, if you have done too that you might highlight?

Thanks.

Rick Trainor: Yeah, sure. So yes, so back to the revenue growth, we expect to see upper single digits revenue growth for the foreseeable future. Our portfolio is complicated as $2 billion portfolio. So we do have sectors that are growing greater than the average, but offset by some sectors, some solution sets within the portfolio that are lower growth. So in average, it balances out to that upper single digit range, and that's where we feel comfortable with. In terms of customer retention, no, we didn't share that, but it is low, or I guess the inverse of that, what is the our attrition level? It is low single digit range. Our customers stay with us for a long time. As you saw on one of the slides where we show the growth with a customer over time, we continue to see we land an account maybe with one solution, it could be an FCC screening, and then that quickly moves over to fraud and identity and other solutions and we continue to grow our customers over time, but we do serve the largest financial institutions in the world to medium and smaller size accounts as well where they may be purchasing fewer solutions. And if we're seeing attrition, it tends to be in those very small accounts. Second part of the question was, or the third part. Competition for us is it's generally by geography and use case. So in the US physical identity, there's quite a few players in the physical identity space and then globally and digital as well. Digital, much less so, but then it's by FCC, credit risk, fraud and identity. So it all depends by geo and by use case. Really the list of competitors is long and it's rather, I'd rather not get into that level of detail.

Steve Liechti: But is there anyone who is a major part of the market that's at the scale that you are? Apologies. Again, this is my ignorance or is the competition more fragmented?

Rick Trainor: Yeah. When I look at the portfolio from what we do from F&I to financial crime to credit risk and business risk that bring the types of solutions that we bring to market, there are very few. There are very few that have that holistic suite that we have. You'll see some, certainly on the credit risk, the credit bureaus are competitors, but we don't tend to play in their traditional credit space. We're doing alternative credit, basically providing underwriting solutions for those that are not on the credit files and they're partners of ours as well. So it's complimentary, a little bit of competitive on the credit risk side. On fraud and identity from a digital perspective, physical perspective, certainly no one has the depth and breadth of assets that we do and there are players. I mean, bureaus have some components mostly on the physical side, on the digital side less so.

And then around the world, it just really differs by country. And certainly there are a number of startups that are out there. A lot of them are positioning as AI-driven, AI delivery engines and things like that. What they don't have is they don't have the depth of the insights that we have from all the risk signals that our solutions provide. So we tend to see them competing on the fringe and not in the main.

Steve Liechti: Great. Thank you.

Moderator: Again, if you have a question, please press star then one. The next question comes from Ciarán Donnelly with Citi. Please go ahead.

Ciarán Donnelly: Yeah, thanks for Rick and Vijay. A couple of questions remaining from myself. Firstly, on M&A, it's been an active piece of strategy historically. I'd be interested to get your thoughts, do you think the need for M&A to add capabilities given the current pace of technological innovation relative to history has increased and you can point to any areas specifically that might be an area of interest. And secondly, one of your peers talked about developing their own

proprietary model, but in some cases outperforming the frontier models, Vijay, I'd be interested to hear is building your own domain specific model something that you guys have considered and maybe could you help us think about the cost benefit analysis of model usage more broadly? Thanks.

Rick Trainor: Okay. So if I heard the M&A question correctly, let me take it from ... So our whole approach M&A actually starts with organic product development. First, we work with our customers, understand what their problems are, what the issues are, and how best can we solve those. We then look internally, we say, do we have the capability and the timeframes and whether that all works together? And then we say, okay, if that doesn't work for us, let's see if there's our partner solution that we want to consider working with and trying to embed that into our solutions. And that often gives us insight around what a capability gap that we may be missing is all about. And that may be a partner that we eventually acquire, it may be a partner that just gave us insight into the capability and therefore we go into the market to then say, okay, we have a capability that we want to solve.

And then at that point we then look for the best in the industry at solving that problem and work with them depending upon timing and things like that to acquire that business. And we've been, as you pointed out, quite successful. It's a continuous part of our strategy. So as capability gaps do emerge, we then look for that channel approach, then partnership or organic approach first, channel approach, and then M&A. In terms of where we're looking, I mean, it's really about use case FCC, F&I, credit risk business. We look across our portfolio, but specific gaps in our portfolio, that's not something that I'm prepared to share.

Vijay Raghavan: I can take the second part of the question, Rick, about proprietary LLMs. I think that is the nature of the question from Citi. Yeah, so it depends on the use case. So when it comes to our people assets, our device assets and so on, that is a very deterministic kind of solution. We use LLMs, which tend to be third party LLMs to augment the quality and scale of our solutions, but it's not really the forefront. There's no need for us to build a proprietary LLM. In fact, it could

weaken our solution. But when it comes to ID verse, that is in fact a proprietary model. It is a proprietary LLM that we built, a neural network that we built, I should say. So when you heard Matt and Dan talk about the ID verse solution, that is a neural network that we built ourselves starting in 2016, trained with data that has been so over the last 10 years has been trained because it's a very specific kind of use case that operates on liveness detection, document authentication, then we take the output of that and feed that into our Risk Intelligence Network.

So it really depends on the use case. We absolutely do build our own domain-specific neural networks as we see fit.

Ciarán Donnelly: All right, thanks.

Moderator: This concludes our question-and-answer session. I would like to turn the conference back over to Rick Trainor, CEO, for any closing remarks.

Rick Trainor: Yes, thanks. Yeah, I'd like to thank you on behalf of the team for taking the time to join us today. I hope you share our enthusiasm for the business with its leading positions and attractive growth sectors, strong organic product innovation, increasing customer demand for our solutions, which gives us confidence in our objective of continuing to deliver strong underlying revenue growth in the high single digits for this foreseeable future. Thanks and have a great day.