RELX Group
Risk & Business Analytics teach-in

Thursday, 8th November 2018
London

Risk and Business Analytics

Mark Kelsey

CEO, Risk & Business Analytics, RELX

Background

So good afternoon and welcome. I'm Mark Kelsey, I am the CEO of the Risk and Business Analytics division. A little bit about my background. I've had a career in RELX now for over 30 years, and a large part of that on the old Read Business Information where I led the transformation from a traditional publisher to a global data and analytics business. At the end of 2012, I brought together Data Services and Risk Solutions into the Risk & Business Analytics division.

Agenda and why we're here

So in terms of the agenda and why are we here? In previous investor events we have covered insurance and government. Today, we're going to help you understand about two other big sectors: Business Services, and Data Services, and together these account for just over half of our revenues. So I'm going to cover the introduction, then Vijay our CTO is going to talk through technology, and the application of artificial intelligence and machine learning across RELX. Rick Trainor is then going to take us through Business Services, and finishing with a demo from Ian on ThreatMetrix, our biggest acquisition in RELX this year. Hugh Jones, who runs our Data Services business, will then take you through Accuity, and also SBS, our second biggest acquisition of the year And then I'll come back and do the Q&A.

Breakdown

So this gives the breakdown for the RELX businesses in 2017, and you can see the Risk division in green. Broadly speaking, a quarter of the revenues, and a third of the profits. You can also see there's been strong growth. 8% underlying revenue growth and profit growth for 2017, and that consistency is maintained in the first half of 2018.

In terms of size, it's a big business, just over £2 billion turnover for 2017. And on the pie charts, by format, you can see that majority is electronic, and also the most advanced across the RELX divisions on the journey towards sophisticated analytics and high value decision tools. And by geography, you can see that 80% of our revenues are from North America, with the balance from Europe and rest of the world. And Rick and I will talk a bit later on about the international expansion of the old Risk businesses.

And by type, you can see that it's 63% transactional, 35% subscriptions. And of the transactional revenues, over 90% are on long-term volumetric contracts, with highly predictable and recurring revenue streams, with low single digit attrition, and very few one off transactions.

Strong financials

On this chart, you can see the strong financials and consistency of performance. Over the last five years, we delivered good underlying revenue growth. The 8% for 2017 was maintained in the first half of 2018, and also the nine month update. And as you can see, we have strong profit growth, growing broadly in line with revenue growth, and our strategy is to grow our underlying cost base in line with our underlying revenue base. It's a high margin business, 36.7%, and we're not capitally intensive.

Key sectors and relevant size

In terms of our key sectors and relative size, insurance is our biggest, approximately 40% of the total. We deal with all the major US insurance carriers, and we're the clear market leader. We help insurers evaluate risk right across the whole spectrum, from marketing to underwriting to claims.

As I said earlier, the focus for today is Business Services and Data Services, which is just over half of our revenues. Here, we help financial institutions, corporations and other companies mitigate risk, prevent fraud, and cybercrime, and enable commerce. Government is less than 10% of the total, and this includes government healthcare. Commercial healthcare moved to the STM division last year, and the growth rates across these segments are remarkably consistent with a divisional average of 8%.

Capabilities

As a business, we have four key capabilities. It starts with deep customer understanding and talent. That deep domain knowledge combined with a core skill in innovation is a key driver of our success. Data is one of our foundation stones, and we have an incredible position here. And there are four key types of data. First: we have by far the largest public records data in the US. We have been collecting these for 30 years, and we've just started on a journey to replicate these internationally.

The second are our contributory databases, we run on behalf of our customers. One of our core skills as a business is running contributory databases. In the last five years, we have doubled the number in insurance to over 30. We have now added these in Business Services, Government, Aviation and Real Estate. These are unique data assets that give us an incredibly privileged view in terms of the value we can offer back to the customers and the whole picture right across the market.

Our third, and another important source, is we licence a huge amount of data from third parties.

And fourth and finally, are the truly proprietary ones we have built over time. In the US alone, we have over 10,000 sources coming into our data rooms every day, six petabytes of data.

Analytics capability is key to running customers, with scoring models, attributes, and diagnostic tools, to enable them to make decisions once our solutions are delivered.

And finally, technology is an absolutely key resource. The foundation stone here is our big data HPCC platform that brings incredible scale and speed, but particularly linking capability which is fundamental to the value we offer to customers. It's now open sourced and being developed beyond recognition from when we have brought it in. But we obviously use a whole host of other third party platforms and open source platforms, and Vijay will talk about that when he comes up.

Priorities

In terms of our strategic priorities, it's primarily about organic growth, and there are three key themes. The first, we're looking into continuous product innovation in our core markets. We're looking to go deeper and deeper into our customer workflows, adding more decision points. The second priority is about innovation in our close market adjacencies. Again, launching more products. And finally, about expanding to new geographies.

Now in the segments that made up the old Risk Solutions business, we absolutely had a world class business. We weren't playing internationally. At the end of 2012, we had less that $1 million of international revenue. It was a key area of potential value creation. What we have done, we prioritised four key countries, the UK, China, Brazil, and India, with global plays in AML and Telematics. And our focus is primarily an organic play, with partnerships and small selective acquisitions around content and data. And whilst it's still relatively early days, we have gone from less than a million in revenue, end of 2012, to around 150 million today, and it's growing strong double digit. And Rick will touch on that in his session on international.

Key driver of revenue growth

So my last focus is a look at a key driver of our revenue growth, and you can see it here in orange. It's growth from new products, it's innovation. And just to be clear here, we define this as product launched in the last five years, and that's the typical adoption period to roll it across our customer base.

So now I'm going to introduce Vijay to the stage, who's going to talk about technology, artificial intelligence, and machine learning.

Technology, Artificial Intelligence and Machine Learning

Vijay Raghavan

CTO, Risk & Business Analytics, RELX

Thank you Mark. I am Vijay Raghavan, and I'm the Chief Technology Officer for Risk & Business Analytics. I'm also a member of the RELX CTO Forum that provides technology oversight and consistency across the RELX divisions. I have been in my current role for more than almost seven years. I have been in the company for more than 16 years, managing various aspects of our technology, and I have spent over 30 years in various technology roles.

Technology

I'm going to start from where I left off three years ago. When we talk about technology at RELX, it typically involves creating actionable insights from big data. The conventional definition of big data is that it is categorised by volume, velocity and variety, large volumes of data in different formats, being ingested at rapid speeds.

On the left, we ingest massive quantities of data from thousands of data sources in varying formats. The funnel that you see in the middle represents our ability to very quickly make sense out of this data by increasing the quality of the content while decreasing the volume of the data. In other words, we can take all our high quality content, structured and unstructured, and we crank through it with big data technology. We then extract the data points from the content, we link the data points, and we enrich it to make it analysable. After we do that, we apply advanced statistics and algorithms so we can provide professional customers with the insights that they need to do their jobs, whether that's an academic institution benchmarking a performance, or a doctor deciding the best way to treat a patient, or a litigator assessing whether they should take a case to court, or an insurance adjuster deciding whether a claim is fraudulent.

Our customers don't care about big data. They want small actionable data and actionable insights. To generate these insights, we apply artificial intelligence technology such as machine learning techniques, and we can do this in scale.

At RELX, we are technology agnostic. We use various technologies. Open source, third-party, and proprietary to solve specific customer problems in specific domains, applying technology to our leading content and data sets. We spend $1.4 billion in technology annually to drive our innovation. To be clear, that number is for all of RELX. We apply the best of all possible worlds by combining our own technology with third-party technologies, be it open source or commercial, to solve our customers problems.

We re-use approaches and technologies across RELX group. Even though we serve different segments with different content sets, the nature of the problems we solved and the way we apply technology has commonalities that we try to leverage across divisions.

And of course, a key part of our success is our technology talent: people who understand our data and our domains to then create cutting edge solutions using our technology platforms and tools. We have 8,000 technologists, again, across all over RELX, spread across dozens of locations, which means one in four employees is a technologist. We have strong holds in certain cities because we prefer locations where we can recruit and retain technology talent. Our low attrition of 8% is significantly below the industry average for technology. Our employee tenure can be attributed to the fact that our technologists feel appropriately challenged at RELX because they are able to use cutting edge technologies for a purpose, to solve interesting and relevant business problems for our customers.

Defining terms

Before I explain how we use artificial intelligence and machine learning techniques at RELX, which I'll refer to from now on as AI and ML, it's worth defining a few terms. You can see a definition at the top which comes from Stanford University. If you look at the diagram on the left, you will see that artificial intelligence is actually a super set of techniques that sits at the intersection of mathematics and computer science, and is comprised of several tools such as knowledge cases, natural language processing, and decision trees. One of the subsets of AI is machine learning, or ML. The fact is, our modelling teams have been using machine learning techniques for years. In fact, our patented linking technology called SALT is a machine learning algorithm, we just didn't call it machine learning when we invented SALT. And there is a subset of machine learning called deep learning that allows a mathematical model to train itself over time without human intervention using a technique called neural networks.

Algorithms and techniques

There are dozens of AI and ML algorithms and techniques, but the important thing is not how many algorithms we have access to; rather, it's having the expertise and the domain knowledge to know which AI/ML algorithm to use for which purpose. What you see here is that there are different types of machine learning techniques. Supervised learning means that a human being gives the model a training set of data to train the model, so the model can learn from the training set. For example, our customers may be able to give us actual examples of fraud that constitute a training set. Unsupervised learning is a technique that involves training a model using experiential data without using a training set, perhaps because such data is not easily available. For example, this is useful in situations where our customers are not able to give us proven examples of fraud. Within each technique, there are several types of algorithms that we can avail of. But just having access to all these techniques is moot if we don't know when to use which one.

The other point to note is that while we take pride in our proprietary algorithms, such as SALT, our linking algorithm, there are many popular algorithms that are freely available for us to use. Google, for example, open source their TensorFlow Framework, which is essentially an AI/ML algorithm, because they realised that when more people enhance TensorFlow, their own data becomes more valuable.

To highlight the point I was just making, this chart illustrates a comparison of various AI/ML techniques for a particular business problem. This particular chart shows a comparison of algorithms to assess which one is most predictive of auto claims fraud. This is a useful business problem to examine via different AI/ML techniques, because it presents many difficult problems. Auto claims fraud is a rare event, which people are trying to hide. It has a lot of complexity, and includes both structured and unstructured data.

The lift that is shown on the Y axis represents a lift in fraud detection rates by using one of these models. And what we can see here is that a random forest machine learning technique, first from left, is the best technique for this particular problem, as opposed to a certain deep learning technique, third from left, which people tend to think is the most sophisticated algorithm. It may in fact be more sophisticated, but that doesn't mean it is the right fit in all cases. So we constantly evaluate which tool to avail of to solve a given problem.

Application of AI/ML algorithms

In addition to the importance of knowing when to apply which algorithm in what context, what's just as critical is the availability of data assets that the AI/ML algorithm can operate upon.

This picture is a variation of the funnel diagram that I showed you earlier. What this is showing is that the application of AI/ML algorithms on this wealth of data that you see on the left is what allows us to create valuable insights out of the petabytes of raw data that we have. In the end, what our customers care about are the actionable insights that you see on the right, in the form of attributes and scores. A score gives our customer specific and meaningful value that is associated with an entity, such as an insured driver, or a mobile user conducting an online financial transaction that they can act upon.

Scores in turn are made of attributes. An attribute is an aggregated piece of information about an entity. For example, how many times has a consumer moved in the past three years, or how many times have they filed for bankruptcy. Attributes tend to be predictive by themselves, and a collection of attributes put together in the right combination, with the right expertise, can be strongly predictive. Our success is thus a function of our ability to create numerous attributes and models to solve problems for our customers.

As you can see from this trend over the past six years, we have been able to create more models and attributes at an increased pace, as a direct result of our ability to use the right tools and techniques on our rich data assets using superior technology infrastructure and domain expertise.

An example of an AI/ML predictor model that we created is Driver Signature. It's from an insurance scenario, but I'm giving you this example because it is very intuitive. Usage based insurance is different from conventional auto insurance because it's based on telematics data from the car that tells the insurer how you are driving. The problem is that smart phones that are used to record driving behaviour will start recording trips not driven. For example, trips where the insured is actually a passenger in an Uber or a taxi, or shuttle or bike that really should not be counted for the purposes of insurance. Accurate telematics driver scoring should only include trips driven by the insured. So the goal here is to detect non-driven trips without the use having to manually verify all trips.

So Driver Signature is a machine learning model that learns a drivers driving patterns over a short period of time to create a signature based on which it discards those trips that do not conform to those patterns.

To explain Driver Signature further, on the left we see two sets of instantaneous data points for two different trips, and on the right we are assigning some attribute values for that trip. Based on how we calculate those values, we can come up with a score, which can tell us which trip should be counted as relevant or not relevant. In this particular model, the most predictive attributes are these: frequent place, meaning has a driver visited a trip location often; familiarity, meaning does the trip take place in a frequently travelled road; average highway speed, meaning is the average highway speed consistent; familiar speeding, which is typical speeding on a familiar road segment; or weekend driving, meaning does the trip occur on the weekend or not. The key is that we capture an immense amount of instantaneous driving data, and we use an AI/ML model that uses past driving data to determine whether a trip should be counted as relevant or not.

AI/ML example

I'll give you one more AI/ML example. This one pertains more to Business Services and Data Services, which is our focus for today. Our financial services customers use us for their anti-money laundering and Know Your Customer initiatives. They have stiff penalties imposed on them by banking regulators if they allow illegitimate accounts or transactions to get processed via the services. So at their request, we cast a wide net in looking for bad actors, because they don't want us to miss any true positives, that is, entities who are actually bad actors. However, casting a wide net inevitably means that we will find many false positives, and up to now, lots of people are required to remediate these false positive alerts, which costs money. So we have designed a machine learning – a false positive remediation process which examines all the alerts, and determines which of them are in fact true positives versus which ones can be discarded. This allows the customer to have their cake and eat it too. It helps us give a superior product to our customers, and helps us spend less time discarding false positives.

To explain this further, as you can see on the left, our AML/KYC customers spend significant resources on reducing false positives. This is expensive, and analysts, because they are human, are inconsistent in their decision making even if they follow a decision tree to guide them. So we collected data from the hundreds of decision trees that our customers use, and create a model using an AI/ML technique called Gradient Boosting. The goal is to reduce false positives, but to do so without inadvertently suppressing true matches. And as you can see from the results, they're impressive in that the model was able to eliminate a significant number of false positives automatically.

The reason I have shown two types of results on the right is because this model may be adjusted to a customer's specifications. Some customers may be okay with suppressing the maximum number of false positives, at the risk of missing some true matches, and others may be more conservative. Hugh Jones will be telling you more about this from a commercial perspective.

Techniques and tools

Now let's step back a bit and look at – again, as how these techniques and tools are shared across RELX so all divisions can benefit from each other's knowledge. The CTO Forum comprises of the Chairperson and the CTO's of each RELX division get together regularly to share common goals, technologies, and best practices. One of the tools used by the CTO Forum is the Tech Radar which allows us to share tools and processes. The Tech Radar is used as a mechanism across RELX to track which tools should be adopted or discarded, or trialled. For example, at any given point, 10% of the tools or techniques or platforms that we use may be under trial. The important thing is that we have visibility across RELX as to who is trialling what to minimise wasted effort. This comes in handy because as each division creates or tests certain AI/ML algorithms, the other divisions can avail of that experience, or at least avoid repeating mistakes.

Core RELX capability

The combination of our deep customer understanding, rich data assets, technology infrastructure, and knowledge of how to use algorithms has allowed us to create effective solutions for our customers. One indicator of our success is how much time our models and data scientists spend wrestling with the data. In other words, getting the data in the right form, before they can create a predictive model. Most analytics teams spend the majority of their time, 80% or more, trying to get the data in shape. We have created an environment where we spend less than half that time beating the data into shape so that when the data gets into the modellers hands they are able to spend the majority of their time working on the actual business problem at hand. This creates a virtual cycle that allows us to continuously refine our tools and processes to add increasing value for our customers, and provides a significant competitive advantage.

For example, we have continuously improved our machine learning based linking algorithm for the past decade. It is now significantly more sophisticated than it was several years ago, and provides increasing differentiation as it continues to improve.

Closing

In closing, RELX has incredible volumes and depth and variety of data in each of the divisions. All this content is vital for us to be able to use AI and ML, because without this richness of content, even the best algorithms will come up short. We then layer on our sophisticated technology platforms and algorithms in order to create applications and solutions with embedded AI/ML technology. You can see examples of these applications at the bottom of this page, and this is a sampling of some of our key applications that use artificial intelligence and machine learning.

With that, I would like to turn it over to Rick Trainor, CEO of Business Services at Risk & Business Analytics.

Business Services

Rick Trainor

CEO, Business Services, Risk & Business Analytics, RELX

Good afternoon. I also want to thank you for attending today's session. I am Rick Trainor, and I am the CEO of Business Services. The objective of today's session is to provide you with deeper insights into Business Services. Before doing so, I thought I'd take a moment to share a bit about my background.

Background

I have been with RELX since 2004, and I have been leading this business unit since 2009. Prior to this role, I led the Public Record Solutions group within Business Services, and I also led the Content Acquisition team for all of Risk, and I was the executive in charge of the ChoicePoint integration. I joined Lexis when we acquired Seisint in 2004.

This next slide is fairly simple, and the sole purpose is to set some context. Business Services is an $850 million business global, and represents approximately one third of Risk & Business Analytics. From an industry perspective, Business Services serves financial services, digital markets, e-commerce, corporates and collections and recovery agencies. Effectively, we broadly serve any industry that has a need for identity risk solutions other than insurance, healthcare and government, as they are served by other business units within RBA.

Our customer base consists of the largest global financial institutions, the world's leading digital businesses, and many of the Fortune 500. We have approximately 30,000 customers, in over 100 countries, so truly a global business.

Our solutions help customers solve daily business challenges across industries, and we are able to do so because we have developed suites of solutions common to many different industries. These include fraud prevention and identity management, financial crime, compliance, business and consumer credit risk, and collection and other services.

So let me tell you a little bit more about each of these.

Fraud and identity

Our fraud and identity offerings focus on a suite of solutions that help our clients more seamlessly interact and engage with their customers. We reduce customer friction when accessing and acquiring goods and services digitally and in person, while also deflecting and detecting fraudulent transactions or interactions from occurring. Fraud and identity represents our largest solution suite, with many of these solutions global in nature. Our financial crime and compliance offerings relate to a suite of data services and software solutions that help our clients comply with globally applicable regulations, such as Know Your

Customer, antimoney laundering, terrorist financing, antibribery and corruption. These capabilities are also globally available.

Business and consumer credit offerings focus on a suite of solutions that use alternative data to help our customers prospect for and acquire new customers, assess their credit worthiness and perform general due diligence. These are market specific offerings in the US and UK with planned global expansion. Our collections offerings are driven by a suite of solutions to help our customers contact and locate debtors, comply with bankruptcy regulations, and help with the reunification of funds. These are currently local solutions in the UK and the US.

Mandate that matters

Not only do we have a suite of highly valuable solutions, we also have a mandate that truly matters, and this is something as a business we are incredibly proud of. We combine comprehensive data sets with advanced technology and analytics to help our clients evaluate, assess, and predict risk. And in doing so, our solutions help our clients to protect against many of the world's most pressing societal problems.

It doesn't end there. As part of this mandate, we have an overarching mission to enable global transparency and financial inclusion. Be it cyber crime, identity theft, financial exclusion, or financial crime, our solutions at the forefront are powering the global economy and advancing society at large. Our business truly makes a difference.

History

I would now like to share a bit of history to set up how we have evolved, and I'll focus on acquisitions most impacting Business Services. Before 2000, we were an internal department in our broader legal division, collecting public records for their legal customers. Then in the year 2000 we bought a small business called Risk Wise, and that was a catalyst for selling data externally, and for creating a risk focused business. We followed this up with two landmark acquisitions: our Seisint acquisition in 2004 provided us with our core HPCC technology platform, and has since underpinned our activity. including our geographic expansion in the UK and Brazil. Our ChoicePoint acquisition, which primarily brought the insurance market to Risk, it also provided Business Services with deep financial crime and compliance expertise in our market leading Bridger risk[?] screening solution.

We followed this up with three smaller acquisitions. In total, a little bit more than $100 million, primarily for content, market access, and capability, and these were essential bridgeheads for our international expansion. Our varied acquisition provided access to an advanced identity authentication platform used for step up authentication, essential to our layered identity management strategy in fraud.

Our WorldCompliance acquisition provided us access to unique financial crimes, and high risk individuals data sets along with global reach, and now is an essential component of our FCC product line. Our TraceSmart acquisition provided us content and a UK market entry point.

And earlier this year, we closed on another landmark acquisition, of course, that of ThreatMetrix. The ThreatMetrix acquisition provided us with a market leading global digital identity platform, and is an incredibly exciting part of our go forward strategy, which I will speak to in more detail in just a few minutes. As you can see from this slide, we have grown this business by over tenfold since the formation of Risk, an absolutely incredible accomplishment.

Organic growth

I want now to look at growth in terms of product innovation, and this slide illustrates how we have built the business by organic revenue growth and new product innovation. As you can see, each year, we are constantly adding new products, or have – or enhancing existing products to great effect. As a result, we have been able to deliver an 8% underlying CAGR over the past five years, with more than half our incremental growth a result of the new product development process.

International

We have also supported our overall growth strategy with an aggressive geographic expansion strategy, which we began executing a little over six years ago. In doing so, we put together a three pronged approach. First, we developed a sales distribution channel and lead with our globally applicable assets. At the time, this strategy primarily focused on financial crime and compliance capabilities. This gave us the necessary in-market expertise and helped us hone our go to market and market knowledge.

Second, we followed this up with relatively small strategic acquisitions of content sources, and necessary capability gaps, followed by deep product integrations of these pieces.

And third, we then followed on with further focus skilled investments, and today, we have successfully built local businesses in the UK and Brazil, along with a global line of business that includes fraud prevention, financial crimes, and developing solutions in business and consumer credit. Our immediate plans call for continued scaling our local businesses, continued distribution and product expansion of our current globally applicable solutions, and finally continue to expand into additional countries. We have put together a clear international expansion strategy and have backed this up with consistent successful execution, and as of today we have $100 million plus international business, and also have the necessary expertise to gain further scale and reach in these exciting markets.

Risk equation

This next slide summarises fairly simplistically how we do what we do, and it all starts with a number of building blocks which we have coined as our risk equation. First, we have developed very deep customer and use case understandings. So we know our markets, and our customers business processes very well, and are considered an essential partner.

Next, we bring to bear some of the largest repositories of consumer and business data assets. We then process them using our internally developed and open source HPCC systems, and during this process, we apply our advanced linking capability to create unique identifiers which in fact create holistic views of entities, consumers in business, across all our information bases. We then apply a suite of analytical process, machine learning and disciplined product development frameworks to build higher level data attributes from which reports, scores, and answers are built. We then deliver this information and services, be it online, machine to machine, batch, bulk, or through purpose built decision platforms we have developed, such as our risk defence platform, or our dynamic decision platform, or by API calls we plug into others' decisioning platforms, resulting in highly focused customer solutions.

Data resources

Vijay discussed how our technology is a significant enabler for us. I would like to speak to another key enabler: our vast data resources. We collect data from tens of thousands of sources, and collect four primary source types of content. Public records, licence, contributory, and proprietary. We acquire content sources both structured, and those that are unstructured. We build data record by record through field collection, we licence and purchase aggregate files, component files, we create ecosystems where data assets are by-products of another solution. We host contributory consortiums, we leverage our transactions, our inquiries. We manually create data files. We use machine learning to develop derivatives or new predictive data elements, and we leverage metadata to create additional data attributes. It's probably pretty clear, essentially if there is a way to collect or develop data that provides insights, we do so. We believe this is a considerable differentiator for us in delivering compelling market leading solutions. It's also important to note that not only do we acquire vast quantities and types of data, we make this data small by turning it into actionable insights.

ThreatMetrix

Furthering our data acquisition strategy, a little over nine months ago we acquired ThreatMetrix, because ThreatMetrix helped us round out our digital identity strategy. This acquisition was a natural complement to our physical identity business. By physical, I mean name, address, government issued ID, and we are incredibly excited about the potential of this business, and what it does for risk solutions. ThreatMetrix is a leader in the $2.2 billion global risk based authentication sector, with the largest digital identity repository, built from over 3 billion transactions per month.

ThreatMetrix solutions analyse connections among devices, locations, tokenised identity information, and threat intelligence, and combines this data with behavioural analytics to identify high risk digital behaviour in transactions in real time, all on a global basis. Combining the number one provider in physical identity solutions, with the number one provider in digital identity – the digital identity solutions results in a truly compelling value proposition and more complete picture of risk in today's global mobile digital economy. These capabilities will allow us to give our clients across all forms of commerce and geographies a more comprehensive approach to identity risk management.

And this is just the beginning. We also believe ThreatMetrix will over time open up new vectors of growth, similar to the way RiskWise and Seisint fundamentally transformed the business more than a decade ago.

As you can see from this side, the combination of LexisNexis risk solutions in ThreatMetrix, connects the physical and digital world, providing a more robust perspective on an entity, whether it be a consumer, a business, or a device. With 100 million transactions added each day, the depth and breadth of these insights only gets stronger, wider, and deeper. And with this physical and digital linkage, we are uniquely qualified to further deliver innovative global solutions to help solve the identity management needs of the digital market place both today and tomorrow.

How ThreatMetrix Works

So, how exactly does ThreatMetrix work? At the core of ThreatMetrix is our one of a kind digital identity network, contributory network, three times larger than our nearest competitor, and created from a network of the world's leading digital properties, leading brands, and comprised of billions of data points sourced from global transactions. There are an estimated 4 billion people on the internet, and ThreatMetrix knows something about over 1.4 billion of them across 4.5 billion devices. Transactions can be verified in real-time against trusted patterns and behaviour and historical norms, to differentiate high risk anomalies from trusted users. Global clients from a broad range of industries are part of our network, including financial services, e-commerce, fintech, media, and a host of other valuable partners.

Our belief is that it takes a network to fight a network. As fraudsters are becoming more and more organised and difficult to detect. The more transactions we see, the more individual identities we can recognise, and the stronger our network becomes, it is a digital identity network that serves as the foundation of our digital identity intelligence, which delivers real time insights and instant trust scores to drive risk-based decisions.

Digital identity

So let me share more about what exactly – so let me share more about what I mean by digital identity. A digital identity is a combination of a user's online historical transactions, along with an individual – along with how an individual behaves across multiple websites and applications. Data elements such as email, and phone, physical mailing address, and other types of information are anonymised using a process called tokenisation to protect privacy during the analysis. This process replaces sensitive data with non-sensitive equivalents that cannot be converted into personally identifiable information. Using this digital behaviour history, digital identity intelligence can be used to form a highly reliable representation of each user, to verify identity risks of new customers during account opening or origination process, and recognise returning customers for login or payment transactions.

This last point is incredibly important. The ability to recognise good customers. Since good customers represent the largest percentage of interactions, and to be able to provide a more secure interaction while also doing so with less friction is incredibly important to our value proposition. Our ThreatMetrix network currently covers activity from nearly all countries and territories, with up to a 95% recognition rate. This means we can reduce friction for the vast majority of online customer interactions. Clearly, a compelling competitive advantage.

I mentioned that we acquired ThreatMetrix because they were the leader in the $2.2 billion global risk base authentication space, and have the largest digital identity networks. Now, let me show you a few additional facts. The business is growing at 40% plus in a sector that is growing 20%. We see 110 million plus transactions are being added to our network each day. 40,000 websites are protected with ThreatMetrix services. 780 million fraud attacks and 19.5 billion fraudulent payments have been stopped over the course of the year. The list of impressive attributes goes on, and clearly ThreatMetrix is a world class leader.

Fraud examples

I would now like to bring our business to life by walking through a couple of real life fraud examples. For context, here are a few facts that capture the market challenge, and why these particular services matter. Cybercrime costs over $600 billion annually. Identity theft represents half of all consumer fraud. One in ten new account openings are fraudulent, and we have seen a tripling of account takeover fraud, and the money mule problem continues to grow. I will explain what this term is shortly. These are all significant issues, and impact global commerce, and require comprehensive solutions to address.

The first example, I would like to start by walking through a combination of risk and ThreatMetrix new account opening and account takeover example, where we touch upon a holistic suite of services, and this is also a good example of an opportunity we closed when we were working together as partners prior to the acquisition, and this opportunity really helped us understand the power of the combined organisation. Now for the example. One of our US corporate clients who focused on retirement services needed to reduce the risk of new account opening fraud, while all the while minimising customer friction. For this customer, we developed a holistic workflow touching upon a number of our solutions, which began with evaluating the consumers engagement point with our customer. So we evaluated the device risk and the digital identity attributes identified during the new account creation transaction.

This process involves a combination of technology and analytics to aggregate and evaluate over 900 different device attributes, from IP address to geo-location to operating system, all of which are gathered and evaluated while the consumers device engages with our customers online system. While this may be the first time that our client may have interacted with this consumer, this same consumer most likely has had multiple interactions within our vast network of digital identity transactions. So it was not the first time that we had seen this consumer.

But these consumers seeking to open an account were then verified using our instant ID solution, where the verification evaluated the physical identity attributes – name, address, date of birth, mobile phone number – against our large physical data repositories to confirm the identity existed, and that these elements likely fit together. For anonymous transactions, where the identity attributes didn’t align, or the digital attributes didn’t make sense, such as access occurring from unusual jurisdictions, or recent use of proxy service to mask the device, in these cases we stepped up the authentication process, by adding additional layers of identity protection. In this case, we stepped up the authentication to knowledge base authentication solution using our instant ID, Q&A product, which dynamically asks non-credit related, knowledge based questions, or we would send a One Time Password to a device that was verified in real-time with one of our phone finding solutions. In those limited situations where the client was still unable to make an automated decision using this dynamic workflow, our customer’s fraud investigators were then able to conduct manual reviews by leveraging our online research portal, which provides an interactive tool for deep research on identities, assets, and relationships.

In this example, our fraud and identity solutions provided our customer: one, faster insights and real-time decisions; two, improving customer experience by introducing the right amount of friction, and in some cases no friction, and being able to offer omni-channel solutions. And finally, we increased operational efficiencies for our customer, by reducing exception handling our manual review process performed by their fraud investigators. As you can see, our solutions are a highly effective tool for fraud prevention, and are built on layers to provide the right amount of friction at the right place in the process.

Our second fraud and identity use case study is the Pure Play ThreatMetrix example, and it involves an international banking client. In this example, the client wanted to optimise a banking experience for millions of active online customers, while also protecting their financial accounts from fraud schemes, by proactively identifying high risk behaviours, typically associated with fraudulent funds transfers through the use of money mules. As the bank sought to optimise the banking experience for their tens of millions of active online customers, effectively good customers, we were at the same time able to help them protect their financial accounts from these types of fraud schemes.

Background

Now for some background. Global money mule networks form to siphon proceeds of crime to the banking ecosystem in an attempt to avoid detection. These networks have become ever more sophisticated, hyper connected, and relying upon vast numbers of individual money mules who are persuaded either knowingly or unknowingly to set up bank accounts to transfer stolen funds. Using the scheme, proceeds of criminal activities can be filtered through multiple mule accounts and across country borders in their real time, facilitated by ever faster worldwide payment systems. Using our ThreatMetrix digital identity intelligence, related to devices, locations, behaviours and threats, the client was able to uncover fraud networks located within the customers base by identifying links and associations between suspicious accounts that otherwise would have been hidden. The real time ThreatMetrix intelligence for each transaction form the building blocks of our clients machine learning model to detect mule accounts.

Leveraging the vast ThreatMetrix digital identity network of over 4.5 billion devices, and 1 billion digital identities, the client was able to incorporate network link analysis to identify and then model mule behaviour. All the clients rules and decisions could easily be – easily self-managed within the dynamic decision platform, and Further support was provided to this client with ThreatMetrix professional service engagements. Just as one example with this client, over £3 million of mule related money transfers have been frozen, and thousands of accounts identified as high risk, and were closed.

Fraud and identity risk are constantly evolving, and we offer the global market place a robust portfolio of solutions that can adapt to customers' needs in terms of fraud detection and prevention as well as business enablement. The integration of the ThreatMetrix capabilities will continue to improve our ability to future proof our offering for continued impact.

I would next like to introduce Ian Spanswick, VP Professional Services for ThreatMetrix who will provide more colour on our ThreatMetrix Solution, and how we solve the money mule example I just highlighted. I will now turn it over to Ian. Thank you

ThreatMetrix

Ian Spanswick

Vice President, Professional Services, ThreatMetrix, RELX

Thank you Rick. First of all, I would like to introduce myself. I am Ian Spanswick, Vice President of Professional Services for ThreatMetrix, where I have been for two and a half years, based right here in London. As part of the wider global professional services team, centred in San Jose, California, I am proud to lead the European team helping ThreatMetrix customers across the region protect their end user's life in the digital world. Prior to ThreatMetrix, I was at Lloyds Banking Group for nine years, where I led the fight against online application fraudsters, which included implementing ThreatMetrix across multiple application journeys. Having joined from a customer, it allows me to truly understand the challenges and opportunities that our customers are facing, and increase their successes.

Money mules

Before we go into detail on money mules, I would just like to demonstrate how ThreatMetrix sees identities online, and what makes things look suspicious. As Rick has said, the ThreatMetrix idea is a summation of the many attributes that are captured and derived from online interactions, and here we can see several examples that I will talk you through. On the left, we see a simple looking relationship of a digital ID, linked to a single email address, device identifier, account name, and Lexis ID. You can see the connecting lines are thick, representing multiple events, solidifying the relationship between these attributes. This is what trusted behaviour from a genuine end user looks like in our global network.

On the right is a very different story. We see a similar strong relationship between the digital ID, account name, and the email address, which is most likely the genuine end user, but we see many other weaker links with the narrow lines. These links are to a wide range of different devices, accounts, and other attributes. This is a very strong indication that the genuine end user's details have been compromised, and are actively being used by bad actors who could be using them to steal funds, make fraudulent orders, or to turn this end user into a mule, either with or without their knowledge.

This is a real advertisement, but it's run by the financial fraud action UK team, in an attempt to raise awareness of what mules are, and how they can be recruited sometimes unwittingly. And after the money mule receives the stolen funds into their account, most of that balance is then transferred out, often oversees, with the mule keeping some of that money for themselves as payment. Easy money.

Using the power of the ThreatMetrix network, we're able to see that mules are even being recruited from populations in society that would be attracted by the promise of quick funds, and perhaps have not yet experienced the process or consequences of having their credit file assessed for additional facilities.

Here we see the real example where ThreatMetrix has identified networks that are clustered around educational establishments. It's clear to see that the mules highlighted in red are actually part of a wider network that spans between a number of banks and that have been used to channel funds around. The mule victims themselves may not actually comprehend that they are a party to an offence that can carry penalties, and negatively impact their credit file in its inception.

But why are these mule accounts so important to the bad actors? Well they are the vehicles that global fraud rings use to exit funds which are potentially proceeds of crime, to otherwise clean accounts that monetarises a whole range of other fraud MOs: account takeover, credit card fraud, identity fraud. And studying these networks, we can see that the rings are truly international in makeup, and the relationships between different financial institutions and countries within the identified bad actors are both complex and far reaching. So to that end, to solve this global problem, we believe it takes a large scale global network of both trusted and suspicious behaviour to be able to recognise when these accounts are being accessed by the bad actors, and preventing funds from being exited. And ultimately, there is a very real human impact of money mules, and often the victim may not even be aware of what they are doing.

Customer decisions

But how does this ability to recognise suspicious behaviour and patterns translate to decisions made by our customers? Looking at this typical end to end process, on average, we have 100 million events per day that feed 18 billion contextual attribute data points, things like device, geo-location, date time, and other tokenised data into the ThreatMetrix policy engine. And then in real-time, ThreatMetrix matches that data across the entire global identity network, and 6.9 billion rule fires a day produce a response that our customers can utilise for decision. That response can indicate whether an event can be classified from trusted to high risk, and it's powerful to see that half of the overall global events can be immediately trusted with no further action. The scores and contextual region codes are then returned in real-time to our customers to enable them to make the decision, and it's a really compelling advantage of ThreatMetrix, that as soon as a new customer joins the network, they benefit from all this cross-vertical intelligence, immediately, even for end users they have never even seen before.

And reinforcing Rick’s comments on the opportunity presented by the integration of Business Services products, should the outcome of a ThreatMetrix rule not be conclusive, then a call can be made to a supporting authentication tool from the Business Services portfolio to guide the end user back to the online journey.

Protecting financial services

From the previous slide, we saw the sheer scale of the data that we consume and produce, but what I would like to show you now is more detail on how this can protect financial services. And key to our approach here is the multiple touch points where data is gathered, and this allows a picture of an end user’s normal behaviour as they navigate a bank’s online or mobile channels. As described earlier, this introduces the concept of trust that can be recognised and leveraged to enhance the end user experience, quickly and consistently, and without the need for any unnecessary interruption. Importantly, if something out of character, or suspicious, occurs, introduced by one of the MOs we see here, malware, account takeovers, then that behaviour will be flagged, and either a transaction declined, or referred as in the end to end process I detailed earlier.

As we can see from the testament, adapting this process has enabled one of our banking customers to make multimillion pound fraud savings, and protect their end users. But coupled with this is that fraud protection is the ability for our customers to offer a truly great user experience, by leveraging the trust that ThreatMetrix establishes, and passively authenticating end users throughout their entire digital interaction. A perfect example of using this trust is the prevalence of the mobile in our pocket being the key to our online life, and it's critical to ensure that this device and our identity work together to meet the need for certainty, ease, and confidence in doing business online. And ultimately, using the power of the ThreatMetrix global identity network, and the strength of our industry experts, allows our customers to make this end to end process as efficient but safe for their end users as possible, and supports Business Services mandate to address global cybercrime.

Thank you. I would now like to hand over to Hugh Jones to talk about Data Services.

Data Services

Hugh Jones

CEO, Data Services, Risk & Business Analytics, RELX

Hello, I'm Hugh Jones. By way of introduction, I began my post grad business career in strategy in a place called Deloitte. I ran the largest division of a data services firm called Data Monitor here in London, and then I started and sold a software and data firm in the healthcare space to a private equity firm. In 2008 however, I joined the then private equity-backed firm called Accuity as president, and I led the sale of that firm to RELX in 2011. I am now the CEO of Data Services within Risk and Business Analytics.

Data Services is a global business that uses industry specific data sets to create targeted solutions for each particular segment of the seven key market segments. Accuity, in the financial services space, represents just under half. Aviation and energy segments represent another 25%, and there are four smaller segments representing agriculture, tax, HR, and real estate that make up the balance.

Accuity

As I said, I sold Accuity to RELX in 2011, bringing together Accuity with a firm called Bankers Almanac, and RELX was kind enough to allow me to stay on as CEO of the combined entity, I appreciated that. Accuity has delivered double digit organic growth year over year with a CAGR over the last eight years in excess of 10%. Including acquisitions, that performance translates into an eight fold increase in revenue over the years since the initial transaction.

We have made a significant acquisition of Fircosoft in 2014, that has generated entirely favourable results and brought our US solutions into global markets that are new to us. We have also recently acquired Safe Banking Systems which I will refer to as SBS, which I will discuss as well in some detail in just a moment. Due to both the organic and inorganic activities, we expect robust growth rates within Accuity to continue.

At Accuity, our customers have historically been banks, but today, we sell into a wider commercial universe indeed. We use our historical banking expertise and now apply that to a much wider audience. All manner of companies want to route payments swiftly and without failure. All manner of companies want to transact with partners, be that a person or another entity, that represents an acceptable counterparty risk, and all companies want to avoid transacting in any manner with a sanctioned entity, for sure.

For example, if you consider a complicated multinational corporation, they will have diverse global supply chains, employees, and partners, they will want to know how best to reliably and efficiently route payments, assess and onboard new partnerships, and know they're doing business with entities that are not involved in any illegal activity. I will also draw your attention to another area of our slide, which is the US Government and Social Services business. Now in this area, we verify the assets for those seeking particular social service programs that are eligibility tested. Now, for example, we help the US State and Federal Government programs assess claims for these services such as Medicaid. We identify where an applicant does not meet the illegibility based on their true assets versus what they declared on their application. Very naughty.

Combining the fact that Accuity has been the official American Banking Association registrar since 1911, we are well trusted by the banks, and our access to RELX government solutions group, we are uniquely positioned to provide this service efficiently and successfully. We have a rich set of solutions for each of these main customer audiences, depending on their specific need. Many of the main audiences purchase an array of solutions across our portfolio, not simply one or two. They may need payment efficiency solutions combined with transaction screening solutions, even if they're not a bank and so on. As a result, we continue to drive more deeply into existing accounts and onboard new logos. And this is a broad market. It's very deep. Plenty of whitespace. The market and the risk and compliance area alone is in excess of 5 billion. So we see many large entities continuing to rely on legacy and home grown solutions, okay, but these solutions are not able to keep pace with industry, technology, and regulatory change, and this is the reason we continue to focus on the area.

Strong market positions

Let's zoom in. We've a strong market position in many sub-segments. If we focus – for a moment – on financial crime screening, the three core elements of screening: screening transactions, accounts or counterparties and trade. And within the trade area, this is not simply with whom you trade, no, I mean – but what is the nature of the trade, what is the nature of the goods that are being traded and where are they going, their destination? For example, is the cargo a dual-use good and is it going to a volatile part of the world? Now I'll explain – in a moment – precisely what I mean by dual-use goods and why it matters to a real-life example. But we have solutions for each of these elements and options to best fit the sector needs and level of sophistication, and we are the market leader in many of these spaces, or rapidly making progress to that goal.

Specificity

Look, sanctions have been around for a long, long time, but they're becoming a far more frequent political tool globally. Their nature is changing, often getting much more targeted versus previous blanket or country-wide sanctions. A sanction now might be placed on a handful of individuals or a single industry within a country rather than the country itself. I mean, just this week as more details of the US sanctions in Iran are announced, they're quite detailed. The OFAC's added over 700 individuals, entities, aircraft and vessels, 300 of which none of this room have ever seen before. These examples of specificity and exemptions put pressure on our customers to invest in their compliance operations and ensure costs are managed, business operations are reliable and their core business is not disrupted. And this change of approach opens up an opportunity for us to work with our clients and really redefine industry standards of acceptability and what it means to perform.

Firco Filter

What we call the Firco Filter is market leading within the world's largest banks. It offers large complex organisations the most comprehensive sets of tools and techniques to tune the filter to their particular risk appetite. And ultimately, it gives them the control they need to run their business effectively. But it also allows them to respond to the increasingly detailed regulatory demands, queries, inspections, etc. This is a simplified diagram behind me, to help explain how our Firco Filter works for transaction screening. The currency symbols here represent transactions entering the filter, the filter screens transactions or payment directions prior to the bank releasing the funds, and the expectation in a Tier One bank is that this screening is done real-time, right now. Not yesterday; now. As you might imagine, the volume of both accounts and transactions going through Tier One bank screening is in the multi-millions daily. The Firco Filter is known, quite frankly, as the most effective filter on the planet.

SBS acquisition benefits

And this is where SBS comes in. SBS enters the picture when we acquired them in July of this year. Now shortly after SBS was founded, it was actually the first distribution partner of the Fircosoft solutions. And their first offering packaged to the market was built with the Firco filter inside it, embedded. SBS uses our Firco Filter and brings it to new levels of efficiency and precision because they bring with them powerful AI and algorithmic capabilities. Accuity is then therefore a very natural home for SBS with a shared history with our Fircosoft brand. Consider, SBS accomplished great things with a whopping two sales representatives. We can now scale SBS solution by relying on over 150 of our representatives throughout our global markets. Accuity has existing relationships with the client decision makers around the globe today and so we can bring these enhanced offerings to the global markets and drive growth. For example, we have the Fircosoft solution incumbency in 73 of the top 100 banks globally. So we can now introduce the SBS platform as an enhancement to a system they already rely upon. The strength and combination of capabilities will also allow us to compete effectively for new logos around the world.

SBS partnership

I'll walk you through some of the technology and expertise that comes with acquisition, just to drive home exactly why we're so excited with the SBS partnership. Now this is a simplified diagram to help explain how our Firco Filter along with SBS works for accounts screening. The SBS capabilities will wrap around our existing offering and use AI to augment the entire screening process. Existing clients have seen a 50 to 90% reduction in alerts requiring manual human review. We've examples of customers having a backlog of hits in the millions and after implementation reducing this burden to 100,000. It does this by bringing together our customer data and watch list data, like politically exposed persons, sanctions, adverse media, etc., and then using advanced analytics to assign a risk score to each entity, essentially a severity score – or how high is my risk if this is a match? How high is my risk if it's a match?

Okay, but then the SBS system then uses statistical analysis models to also apply a probability score – or said another way, how likely is this a match, a true match? The institutions will have set a risk threshold under which they believe the potential hits are frankly not relevant enough to warrant manual review. That is, the hits are statistically improbable or have low materiality. We don't care. They can do this at a departmental level within a bank. Now large banks have different risk levels depending on department, and so this system delivers the required customisation to the particular business area, profile and risk appetite. And that allows our customers to physically review a much smaller number of potential hits and route them to prioritised – in a prioritised manner – to a much smaller team of decision makers who will review. And this is by far a better use of scarce resources within the compliance function, but it also leads to a higher probability of finding real hits, so improved efficacy. And this is due not only to the augmented dual methodology, but also because the reality of the human experience is that compliance reviewers sometimes make a mistake, sometimes they get tired. Sometimes they miss a hit. Computers don't get tired.

These decisions are then captured and fed back into the start of the process, an account won't be reviewed again unless something's changed, the system flags a change. For example, a new piece of adverse media or a change in a person's entity status as a politically exposed person. This week, this happened to a lot of people in a big country called the United States. This brings both efficiency and effectiveness to the overall system.

Case studies

Trade compliance screening

You can see why we're excited about that, but I want to take you through two really brief case studies on adjacent spaces that we are pursuing vigorously. They're very much driven by regulatory and market dynamics. Let me start in the area of trade compliance.

This is an example of a very recent case study driven by regulators expanding their oversight in their quest to stop illicit business dealings around the globe. Currently, regulators seem to have a particular focus on thwarting potential terrorist activity in the area of international trade. Okay. So we've seen our fines and increased – or we see recent fines and increased regulatory guidance for the airline, shipping, cargo and freight forwarding industries around the world. Cargo departments, for example, must take action to understand who they're doing business with and what is the nature of goods they're shipping. We use our dual-goods database to answer whether a particular shipment contains dual-use goods and are they being shipped to a volatile part of the world. Dual-use goods are those that have perfectly legitimate use cases, but equally could be used for military or destructive purposes. They can be precursor chemicals for narcotics, or worse. For instance, we have a client who discovered that what they thought was a shipment of sealed tubing to a Middle Eastern manufacturer was in fact a shipment of tank gun casings bound ultimately for Syria. And this is typical. Cargo companies, just like banks, face costly reputational and regulatory fines if they cannot adequately screen and stop risky business dealings. However, they can't let these compliance activities disrupt their day-to-day operations – their business to be in business. So again, accuracy, scale and speed is absolutely critical and we're working closely with this industry to provide guidance and capabilities tuned to their sector requirements and we see it as a large and imminent growth area for Accuity with significant average contract values.

Alternative payment providers

The second adjacency which I want to explore with you, and my final example, is in the area of alternative payment providers, non-banks and again, screening, this time transaction screening. We're seeing the use of alternative payment providers for transactions growing rapidly all around the world as more and more transactions happen online via a diverse and growing set of providers. It sets a new challenge and opportunity we feel aptly prepared to seize. These payment providers are now being held to the same regulatory scrutiny as banks have faced for years. They've been expected now to screen every transaction and halt any suspicious activity before completing that transaction. But that's hard because they also have to deliver on their customers' expectation of lightning speed. Think of when you buy things with your phone; after all, this convenience and ease of use is in fact their core value proposition to the market. So the alternate payment providers we work with see high volumes and require high performance screening that we've never seen before. An example might be 40 million transactions a day, each required to be dispositioned in under 100 milliseconds, peaking at times at 700 transactions a second. These daily volumes, by the way, can be over ten times the volumes of a typical Tier One bank. Ten times higher.

So we are working to hit levels of performance that have never been achieved before or – and we believe that our improved throughput and performance will be industry-changing. We found initial success here with the acquisition of recent clients in this space and we see contract values, again, in the millions of dollars for these customers as well.

Ending on that cheery note, I'm going to transfer back to Mark Kelsey for Q&A.

Conclusion

Mark Kelsey

CEO, Risk & Business Analytics, RELX

Thank you Hugh. So to summarise, the businesses that we've just reviewed help financial institutions, corporations and other organisations mitigate risk, prevent fraud and cybercrime, and enable commerce. As a business, we're very well positioned in attractive long-term growth markets. As you've seen, we've got strong capabilities primarily driven from data and technology that we're leveraging well. Our strategy is primarily organic with tremendous opportunities in every sector: core markets, adjacencies, international. And as well as having great momentum on our organic growth, as we've illustrated, our two acquisitions are a great fit in our organisation, and that's why we're so excited about the tremendous opportunities they bring.