



Risk Business Services
Investor Seminar

May 13, 2026

DISCLAIMER REGARDING FORWARD-LOOKING STATEMENTS

This presentation contains forward-looking statements within the meaning of Section 27A of the US Securities Act of 1933, as amended, and Section 21E of the US Securities Exchange Act of 1934, as amended. These statements are subject to risks and uncertainties that could cause actual results or outcomes of RELX PLC (together with its subsidiaries, “RELX”, “we” or “our”) to differ materially from those expressed in any forward-looking statement. We consider any statements that are not historical facts to be “forward-looking statements”. The terms “outlook”, “estimate”, “forecast”, “project”, “plan”, “intend”, “expect”, “should”, “could”, “will”, “believe”, “trends” and similar expressions may indicate a forward-looking statement. Important factors that could cause actual results or outcomes to differ materially from estimates or forecasts contained in the forward-looking statements include, among others: regulatory and other changes regarding the collection or use of personal data; changes in law and legal interpretation affecting our intellectual property rights and internet communications; current and future geopolitical, economic and market conditions; research integrity issues or changes in the payment model for our scientific, technical and medical research products; competitive factors in the industries in which we operate and demand for our products and services; our inability to realise the future anticipated benefits of acquisitions; compromises of our cybersecurity systems or other unauthorised access to our databases; changes in economic cycles, trading relations, communicable disease epidemics or pandemics, severe weather events, natural disasters and terrorism; failure of third parties to whom we have outsourced business activities; significant failure or interruption of our systems; our inability to retain high-quality employees and management; changes in tax laws and uncertainty in their application; exchange rate fluctuations; adverse market conditions or downgrades to the credit ratings of our debt; changes in the market values of defined benefit pension scheme assets and in the market related assumptions used to value scheme liabilities; breaches of generally accepted ethical business standards or applicable laws; and other risks referenced from time to time in the filings of RELX PLC with the US Securities and Exchange Commission. You should not place undue reliance on these forward-looking statements, which speak only as of the date of this presentation. Except as may be required by law, we undertake no obligation to publicly update or release any revisions to these forward-looking statements to reflect events or circumstances after the date of this presentation or to reflect the occurrence of unanticipated events.

Risk Business Services Investor Seminar

Agenda

Risk overview and Business Services strategy

Slides 4-22

Risk technology

Slides 23-31

Fraud & Identity deep dive & case studies

Slides 32-48

Concluding remarks

Slide 49

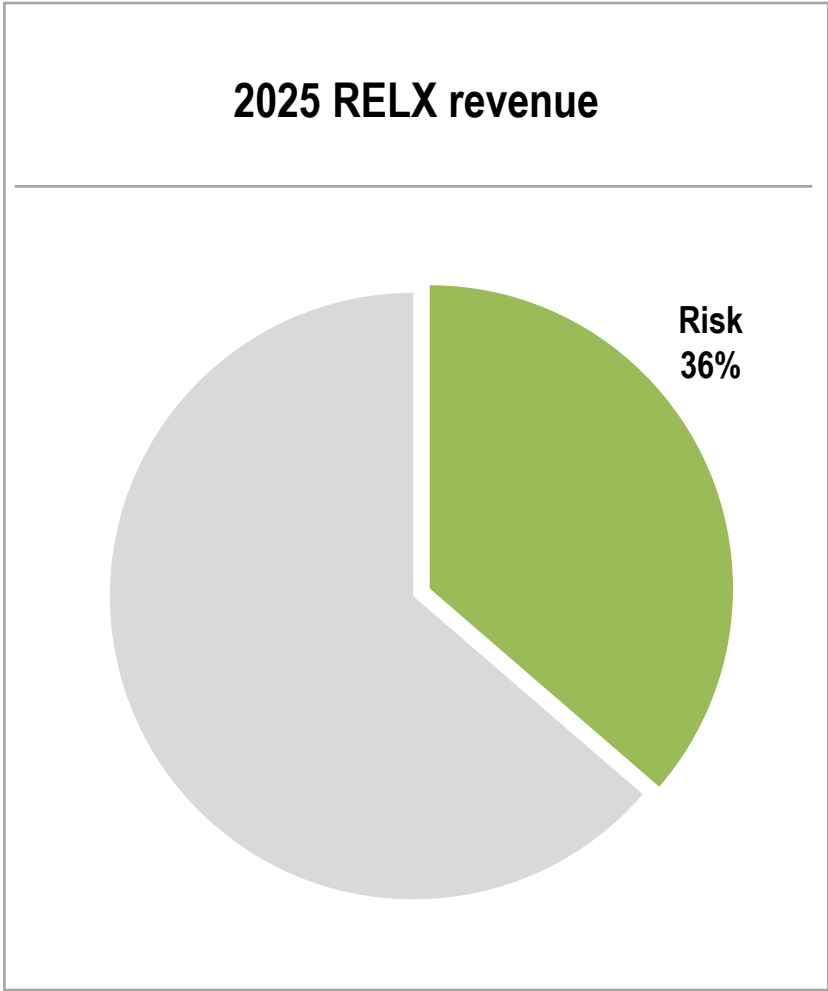
Q&A

Speakers: Rick Trainor, CEO Business Services; Vijay Raghavan, Chair, RELX Technology Forum and Chief Technology Officer, Risk; Kim Sutherland, Vice President and Global Head of Fraud and Identity; Matt Adams, Chief Technology Officer and Co-founder, IDVerse; Daniel Aiello, Chief Product Officer and Co-founder, IDVerse

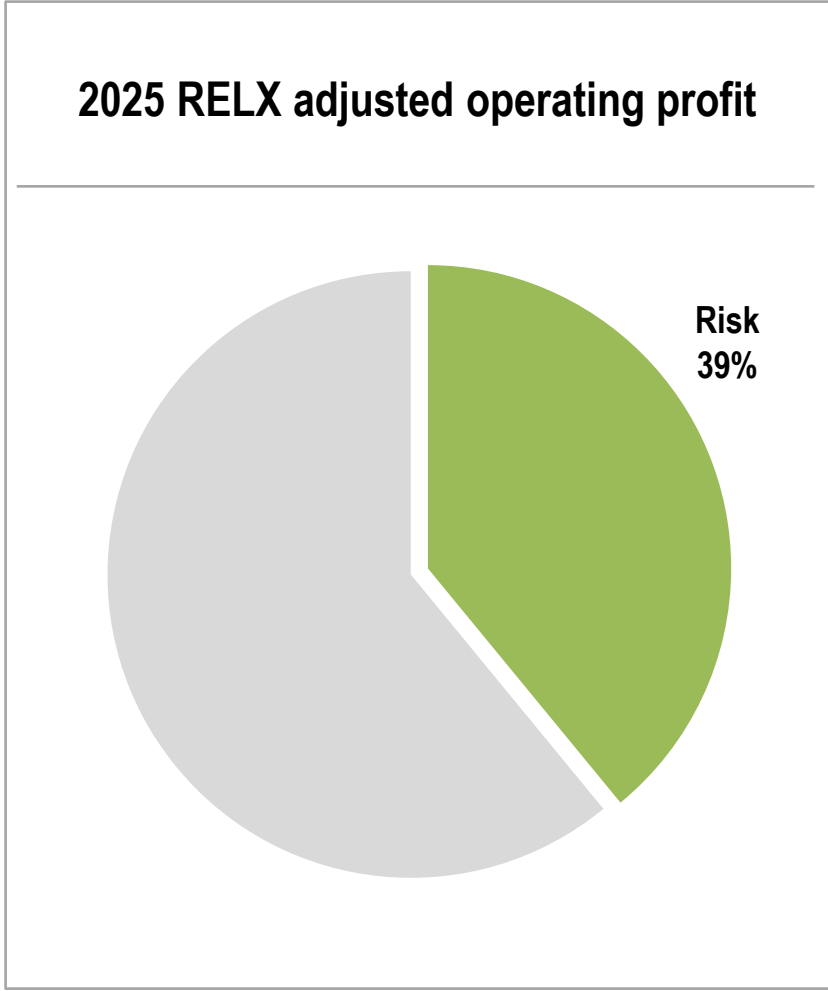
Risk overview and Business Services strategy

Rick Trainor
CEO, Business Services

Risk position within RELX

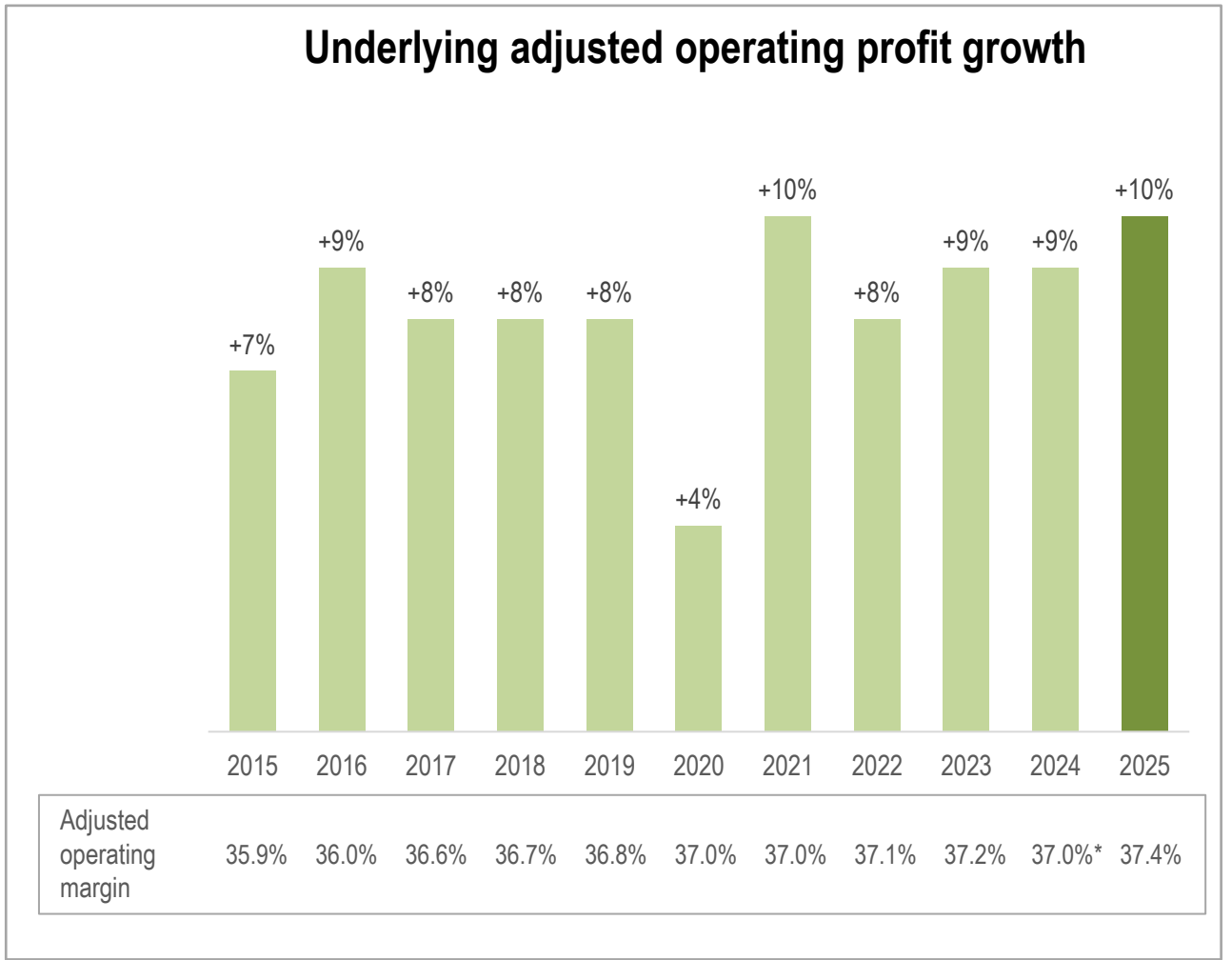
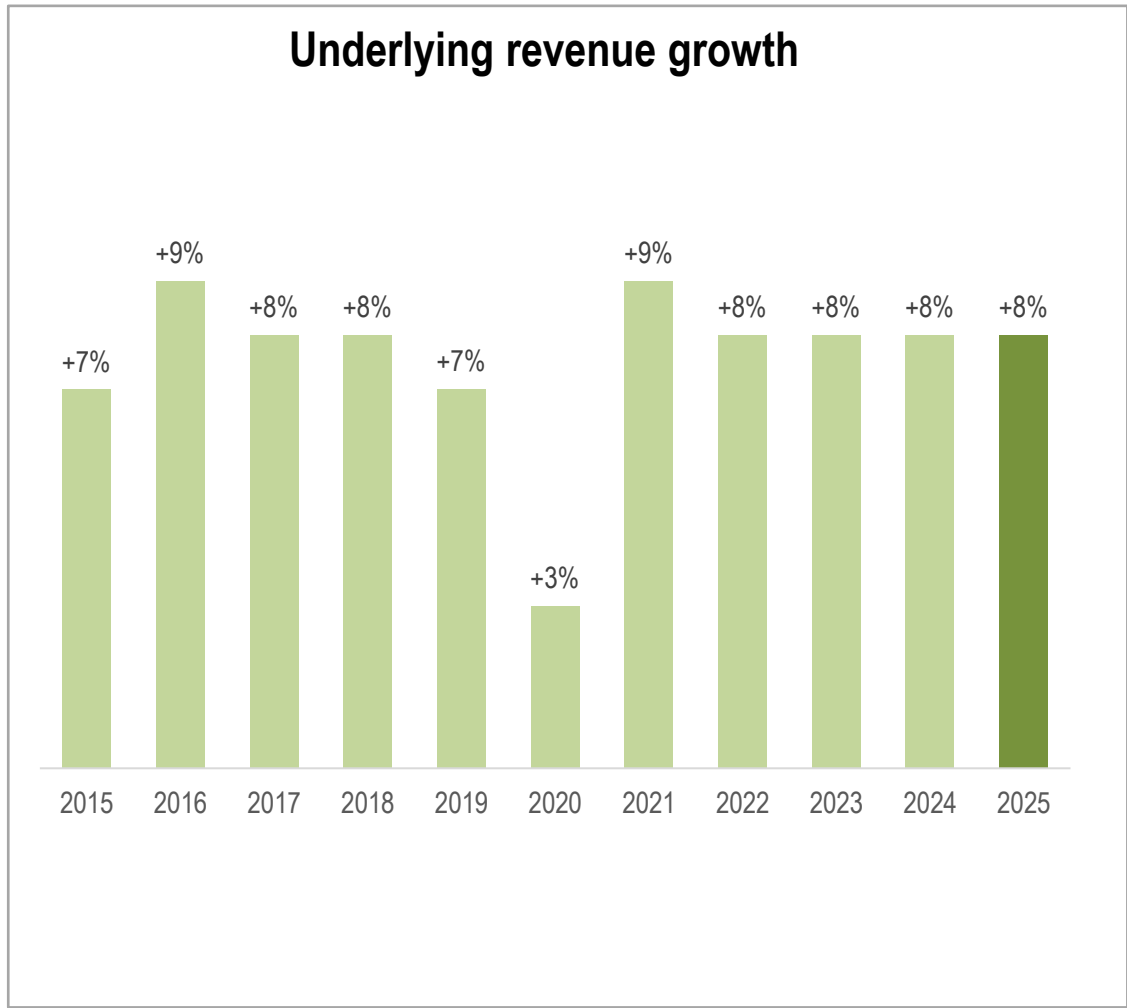


Risk: £3.5bn (\$4.6bn)



Risk: £1.3bn (\$1.7bn)

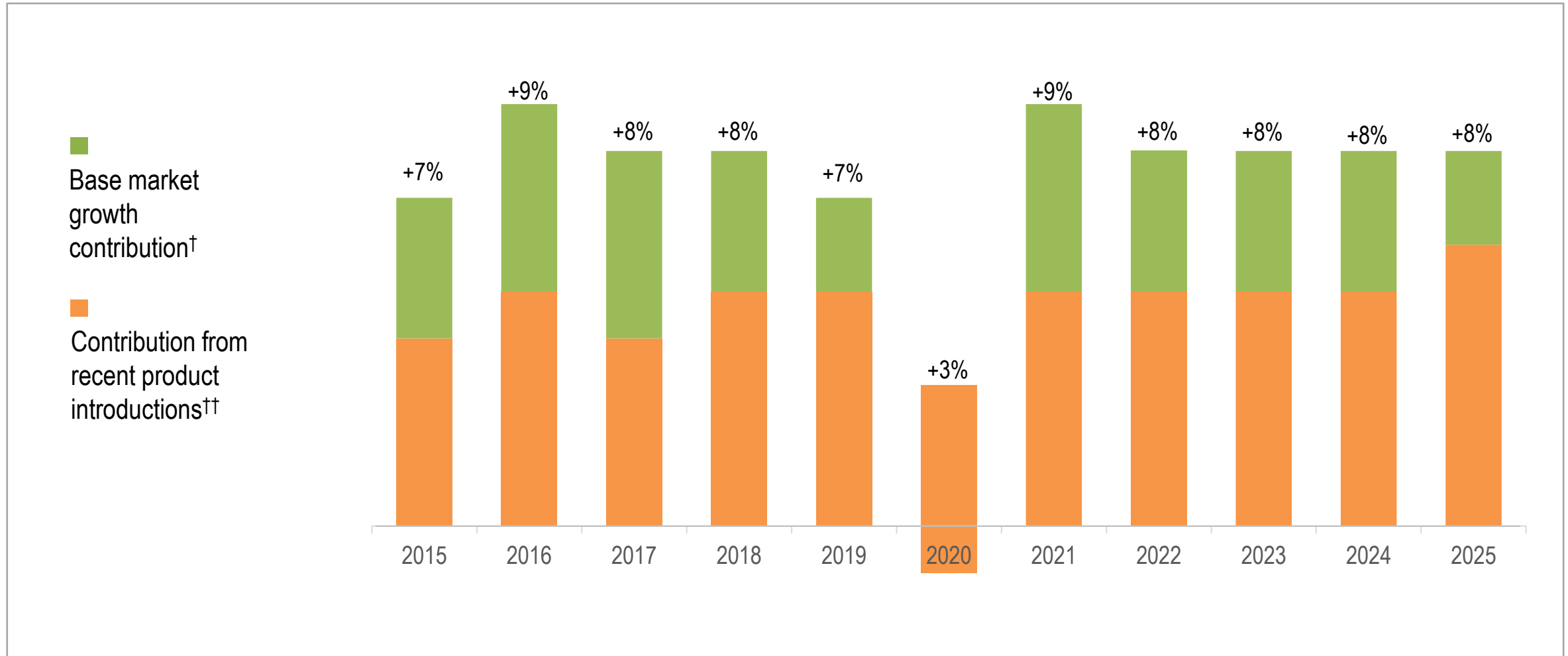
Risk underlying growth rates



2024 and prior growth includes print & print-related

* 2024 margin restated to reflect business area reporting changes

Risk underlying revenue growth



† Products more than 5 years old

†† Products less than 5 years old

Our four key capabilities driving organic innovation engine



1. Deep customer understanding

- Extensive industry expertise
- Long customer relationships
- Deep integration into critical workflows
- Compliance expertise and trust



2. Leading scale data assets

- 25+ contributory and proprietary databases
- Tens of billions of public records
- Tens of thousands of sources
- Decades of history
- Strong network effects
- High regulatory requirements



3. Advanced linking and analytics

- Long history of advanced data science and AI usage
- 1,000+ proprietary models to turn data into insights
- Continued evolution and refinement to drive high precision, recall, and accuracy

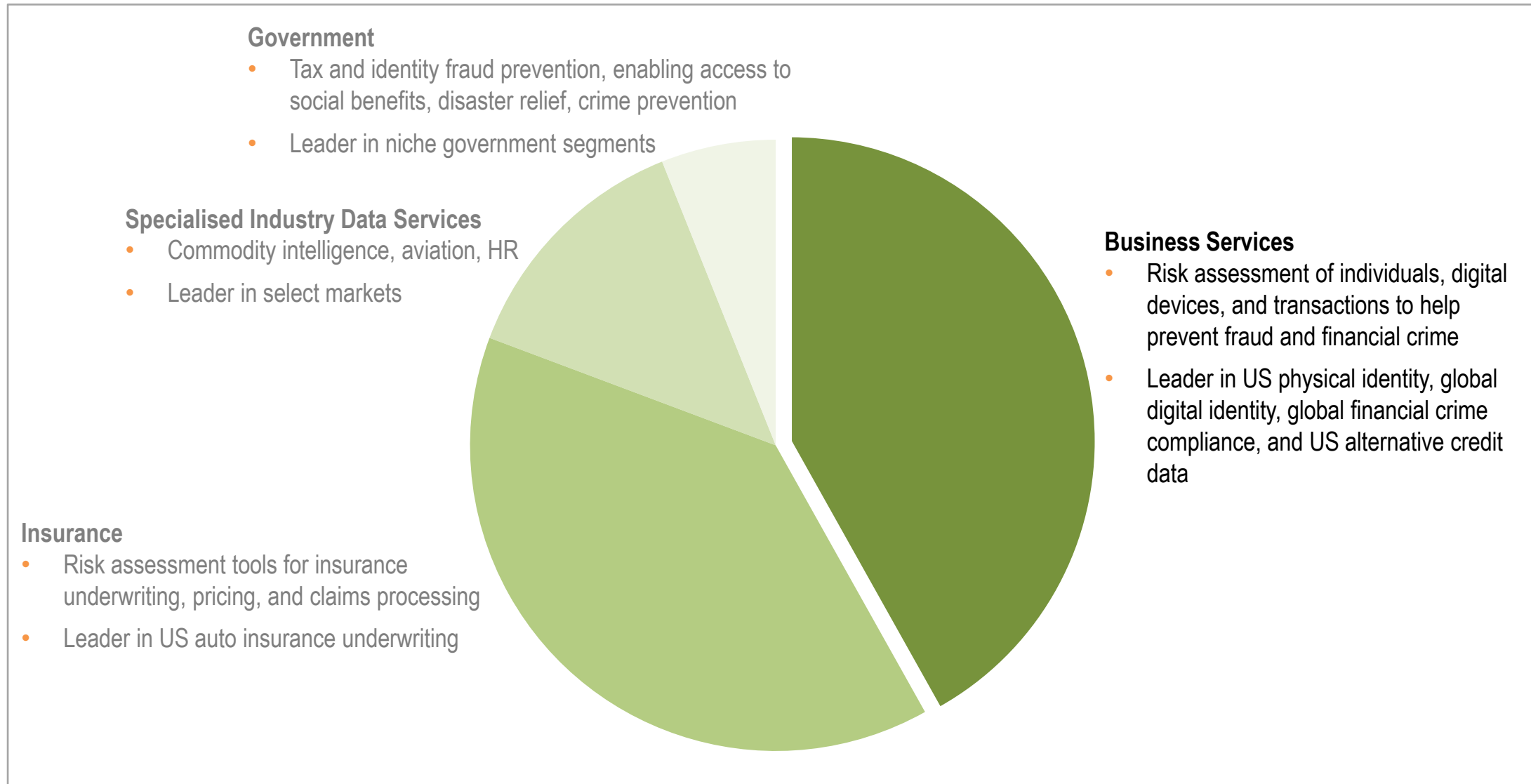


4. Powerful technology in global platforms

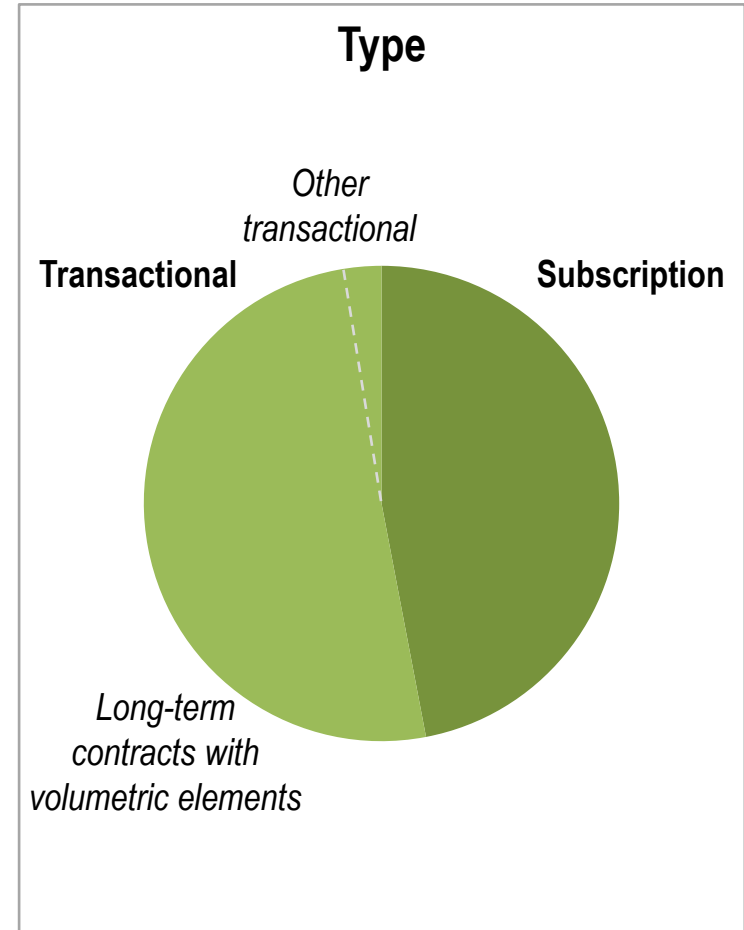
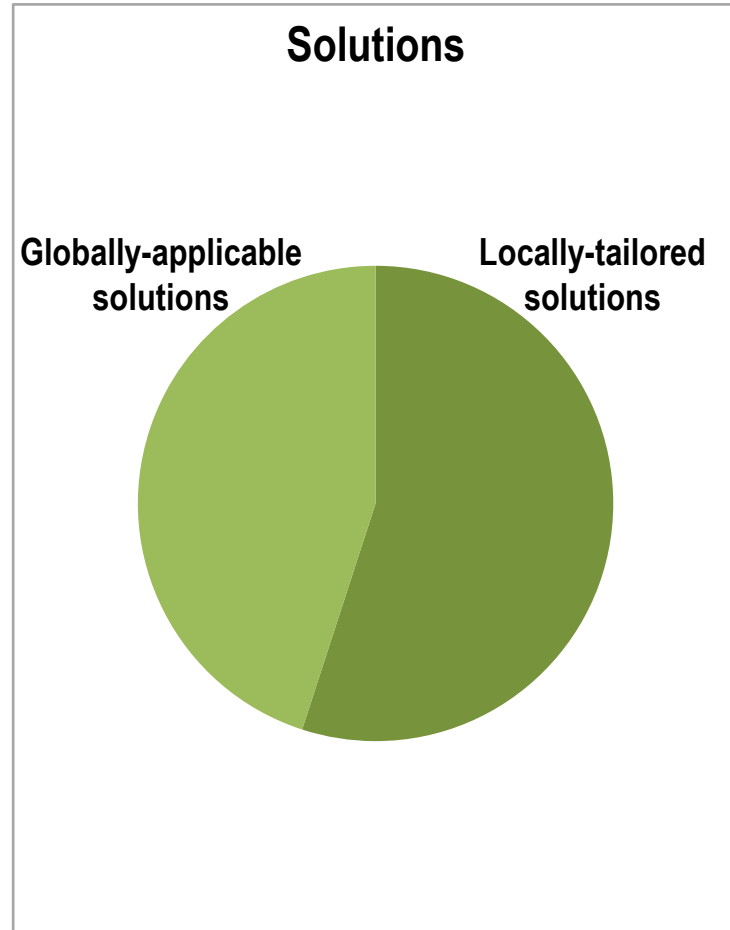
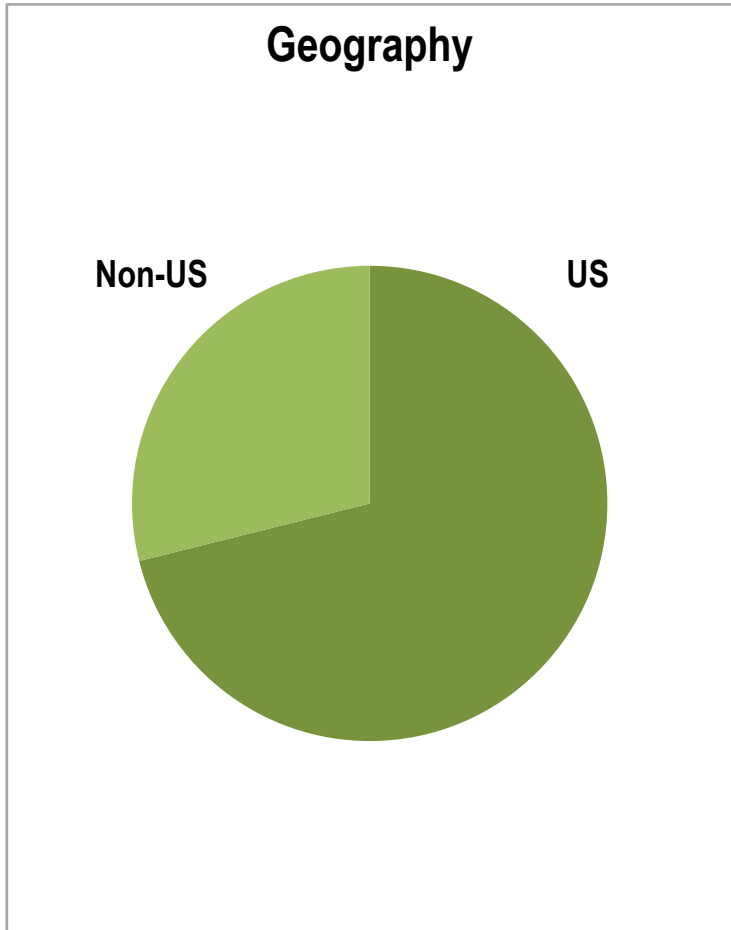
- Single point of execution
- Technology agnostic approach
- 90%+ machine-to-machine delivery at the point of decision-making

Risk revenue by segment

2025

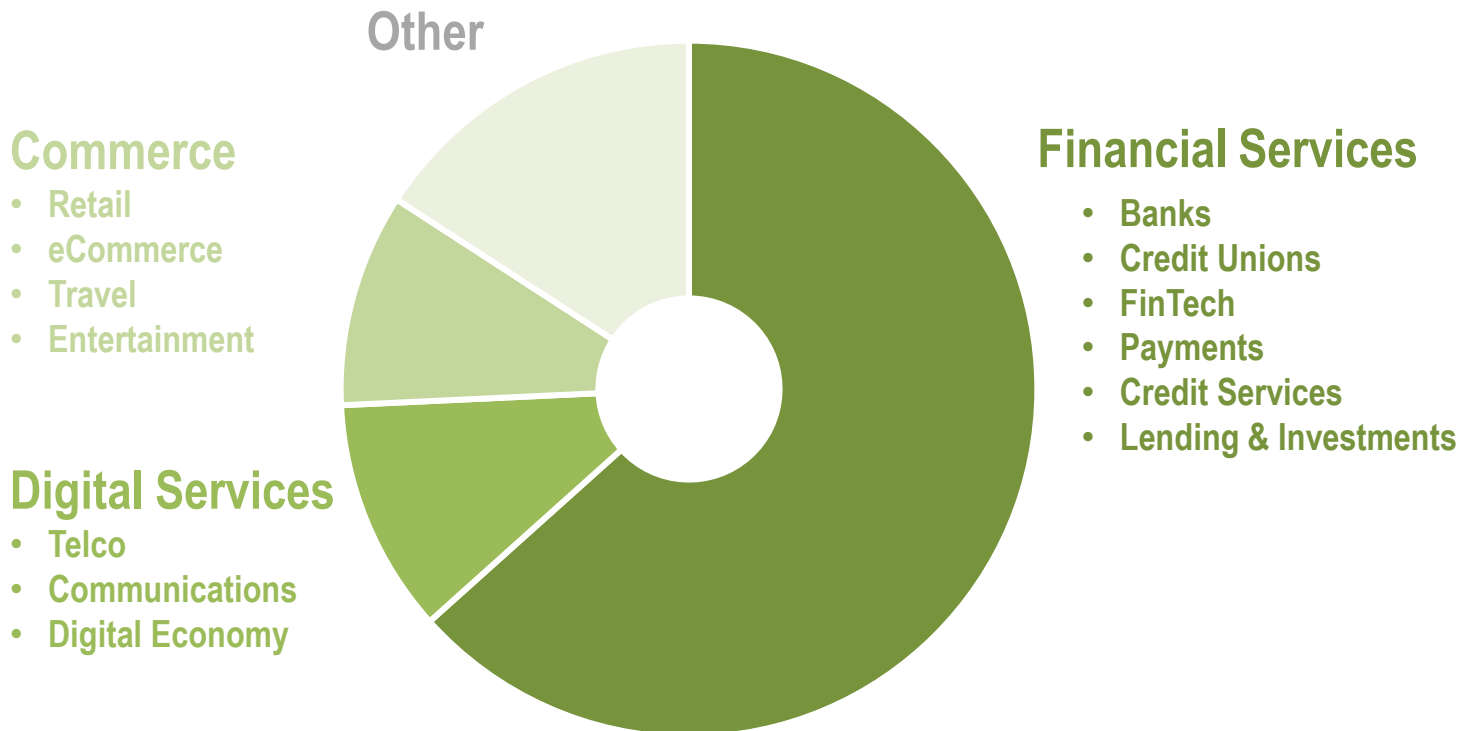


Business Services revenue by type 2025



We serve large, mid-market, and small customers globally and across industries

Customer Segments



Diverse customer base

- 18,000+ customers in more than 180 countries and territories
- Top 30 customers represent under 30% of total revenue

Leading Business Services customers

- 98% of global top 50 banks
- 100% of US top 50 banks
- 90%+ of US credit card issuers
- 50%+ of Fortune Global 500 retailers
- 40%+ of Fortune Global 500 telecom

Our solutions help customers solve daily business challenges

Segment	Fraud & Identity	Financial Crime Compliance	Credit, Business Risk, Payments, and Other
Solutions	<ul style="list-style-type: none"> Protect consumer identities Prevent account takeover Reduce friction for legitimate users 	<ul style="list-style-type: none"> Protect customers from crime Uncover crime risk through account and transaction screening 	<ul style="list-style-type: none"> Enhance understanding of risk and creditworthiness Enable consumers and businesses to access credit and other services
Position	<p>#1 US physical identity data</p> <p>#1 Global digital identity data</p>	<p>#1 Global financial crime screening volume</p>	<p>#1 US alternative credit data</p>

The customer problems we solve are large, global, and growing

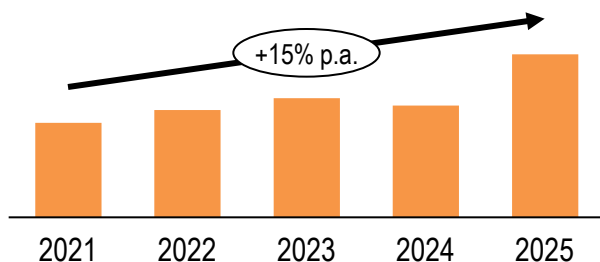
Fraud & Identity	Financial Crime Compliance	Credit, Business Risk, Payments, and Other
------------------	----------------------------	--

Customer challenges

- Fraud attacks continue rising globally, driven by:
 - Increases in **digital transactions globally**
 - Sharp rise in **automated bot attacks**
 - Surge in **AI-powered fraud**, including deepfakes, synthetic identities, and automated phishing
- Reported fraud losses in the US have almost tripled since 2021, reaching c.\$16bn in 2025¹

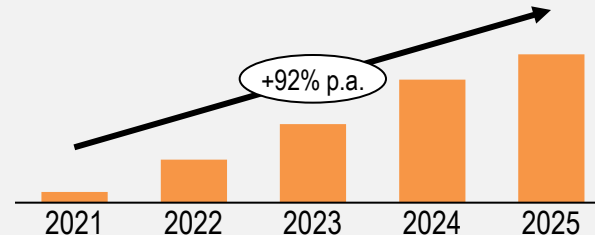
Trend

Reported attacks within LexisNexis Risk Intelligence Network², by year



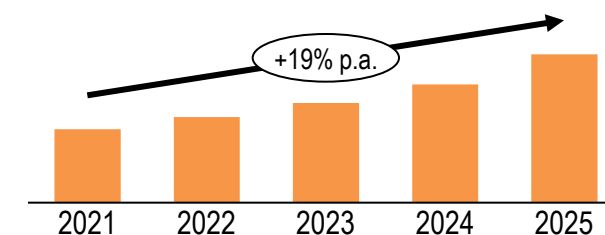
- Compliance is becoming more complex
 - Increasing number of **entities required to comply**
 - Rising number of **designations**
 - Rapid pace of sanctions and regulatory updates requires **continuous refresh**
- Regulators have levied c.\$13bn in AML, KYC, and compliance-related penalties since 2021³

Cumulative new US sanction designations since 2021⁴, per year



- US consumer credit outstanding continues to grow
- Alternative data solutions are becoming more important due to:
 - **Expansion in non-traditional borrowing types** requiring near real-time visibility into signals not typically captured in credit files
 - **Reduced predictability** of traditional credit reports due to changes in data reporting

Global BNPL⁵ total transaction values, select companies⁶, by year



1. US FTC; 2. Risk internal analysis; 3. Risk internal analysis; 4. CNAS; 5. Buy Now, Pay Later; 6. Klarna, Affirm, PayPal, Zip, and Sezzle

AI increases customers' challenges, enabling bad actors to operate faster, with greater sophistication, and greater scale

More uncertainty

- Deepfakes
- Synthetic identities
- Enhanced social engineering
- Crimes-as-a-service

More operational drag

- AI enables mass automated scams, expanding criminal operations
- Complexity outpacing compliance, increasing intervention difficulty

Higher cost of getting decisions wrong

- Small control gaps can lead to outsized consequences
- Reputational damage can be long lasting
- No forgiveness from users or regulators



**Trust is
hard to establish**

**Opportunity is hard to
distinguish from risk**

**Firms need accuracy and
explainability**

Our solutions help customers address those challenges, establishing trust during their consumer interactions

Consumer Account Lifecycle



Our solutions enable critical decision-making...

- Prioritise leads
- Determine credit risk
- Monitor fraud and account risks
- Stop fraud attacks
- Verify identities
- Detect financial crime risk
- Monitor fraud and account risks
- Identify ownership and criminal activity
- Monitor fraud and account risks
- Facilitate ease of payments
- Meet compliance requirements
- Identify bankruptcies
- Improve collection efforts

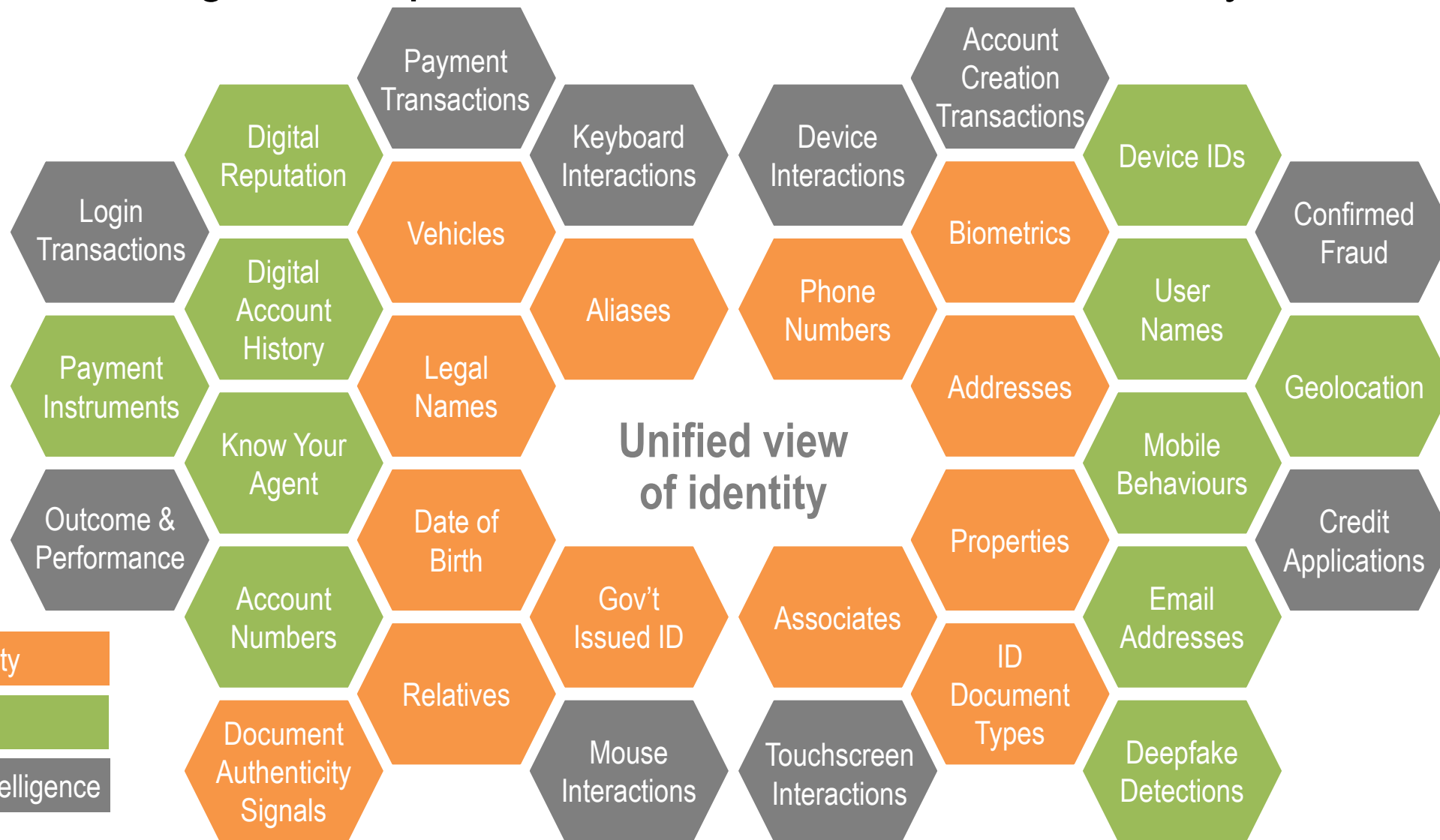
...and increase trust and confidence for our customers as they interact with consumers

More confident decisions

Less consumer friction

Greater operational efficiency

Our unified view of identity across physical, digital, and behavioural signals helps customers assess risk holistically

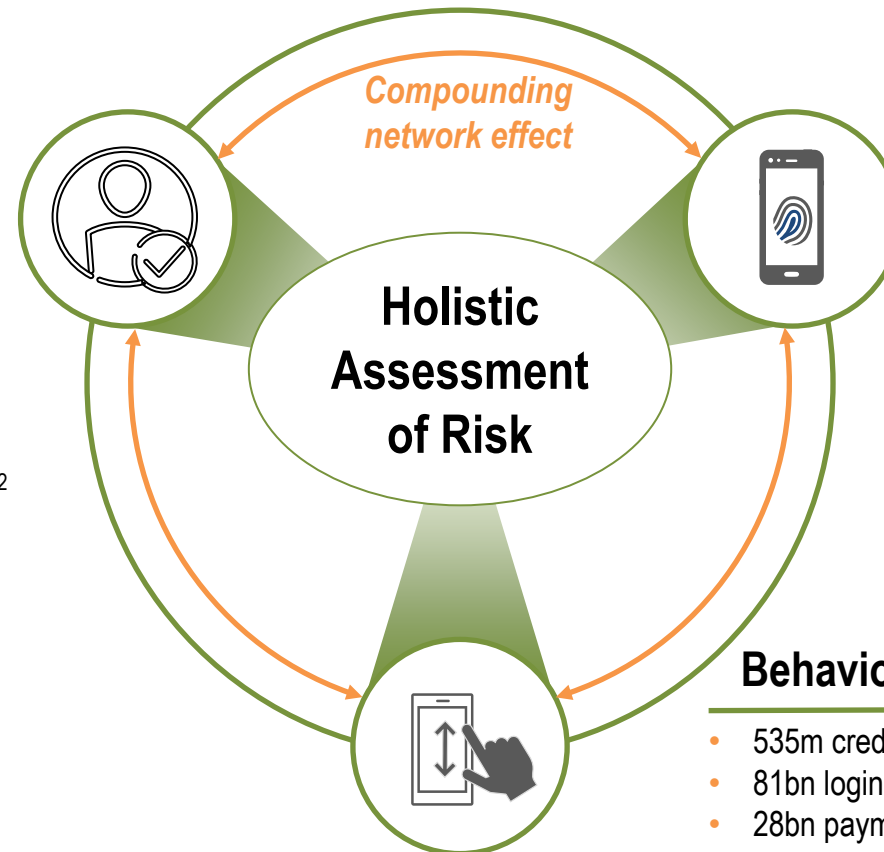


Non-exhaustive

Data analytics at scale to protect consumers

Physical Identity Intelligence¹

- 297m US unique identities
- 14bn name – address combinations
- 47m active US businesses
- 110m business contact records
- 11bn property records
- 10bn motor vehicle records
- 2bn vehicle title records
- 4m PEP profiles
- 1tn+ sanctions screenings processed annually²
- 6m+ vital record transactions processed annually²



Digital Identity Intelligence¹

- 6bn active devices
- 4bn digital identities
- 5bn unique email addresses
- 4bn unique IP addresses
- 3bn unique phone numbers
- 145bn+ unique digital transactions processed annually²

Behavioural Intelligence²

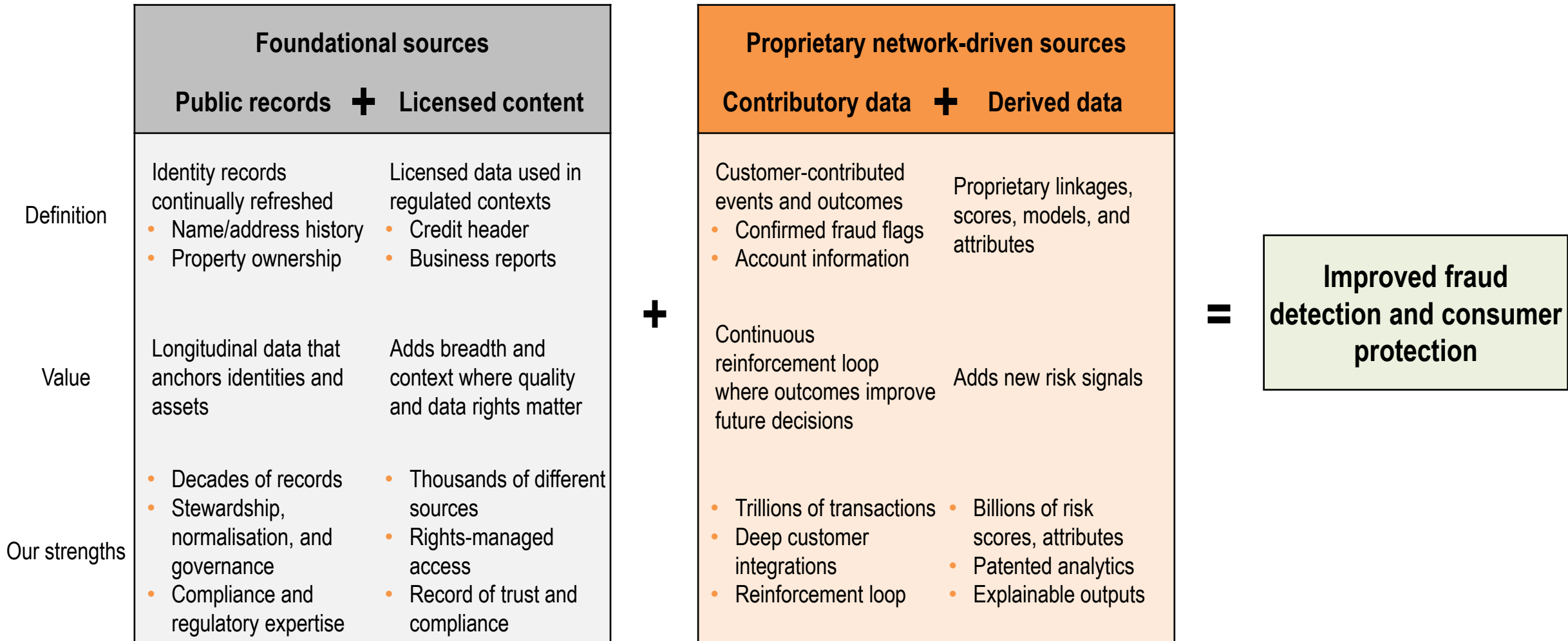
- 535m credit assessments
- 81bn login transactions processed annually
- 28bn payment transactions processed annually
- 2bn new account creation transactions processed annually
- 18bn web interactions collected annually
- 12bn mobile interactions collected annually

1. Physical and behavioural intelligence total in database as of December 2025

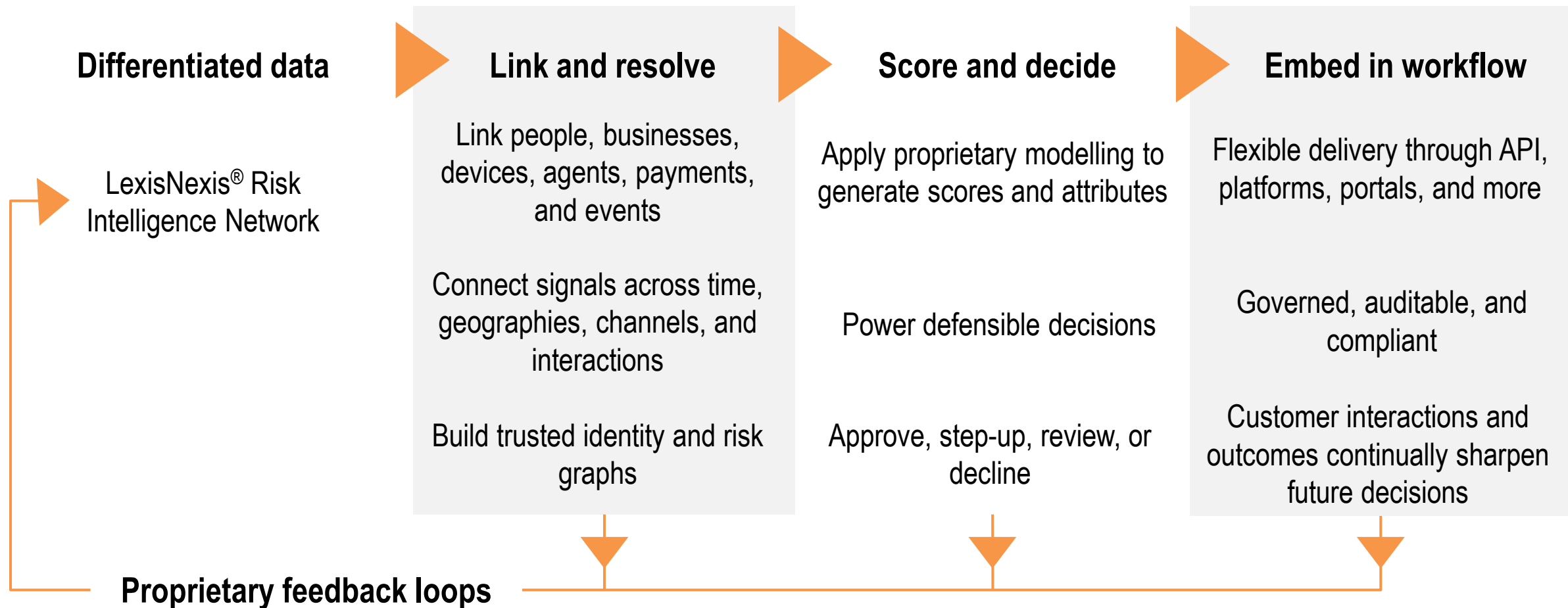
2. Annualised volumes for last 12 months as of December 2025

Four data types contribute to the Risk Intelligence Network

LexisNexis® Risk Intelligence Network



We turn differentiated data into embedded decisions, where every interaction sharpens our network



We provide a measurable value uplift to customers

Our solutions deliver better outcomes

What Risk does

1. We predict more fraud

- Our network can link intelligence across customers, industries, and geographies, enabling fast identification of emerging fraud patterns

2. We distinguish trusted activity from true risk

- We deliver fewer false positives, enabling customers to seamlessly proceed with low-risk interactions

3. We lower operational burden

- We offer greater precision to decisioning, so only high-risk cases are routed to high-cost methods of review

Value uplift delivered to customers

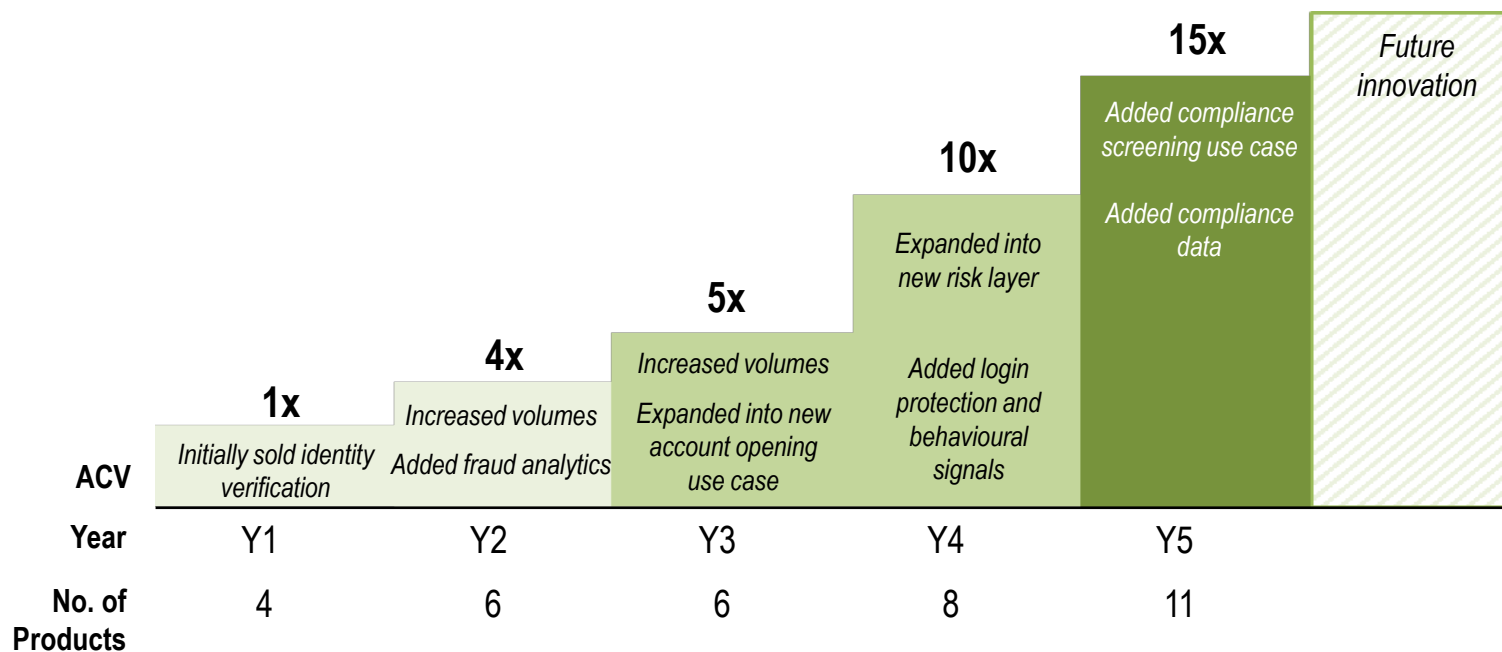
- **More bad actors and risky transactions stopped**
- **Fewer interruptions for legitimate consumers and transactions**
- **Improved efficiency**



Customer value deepens over time

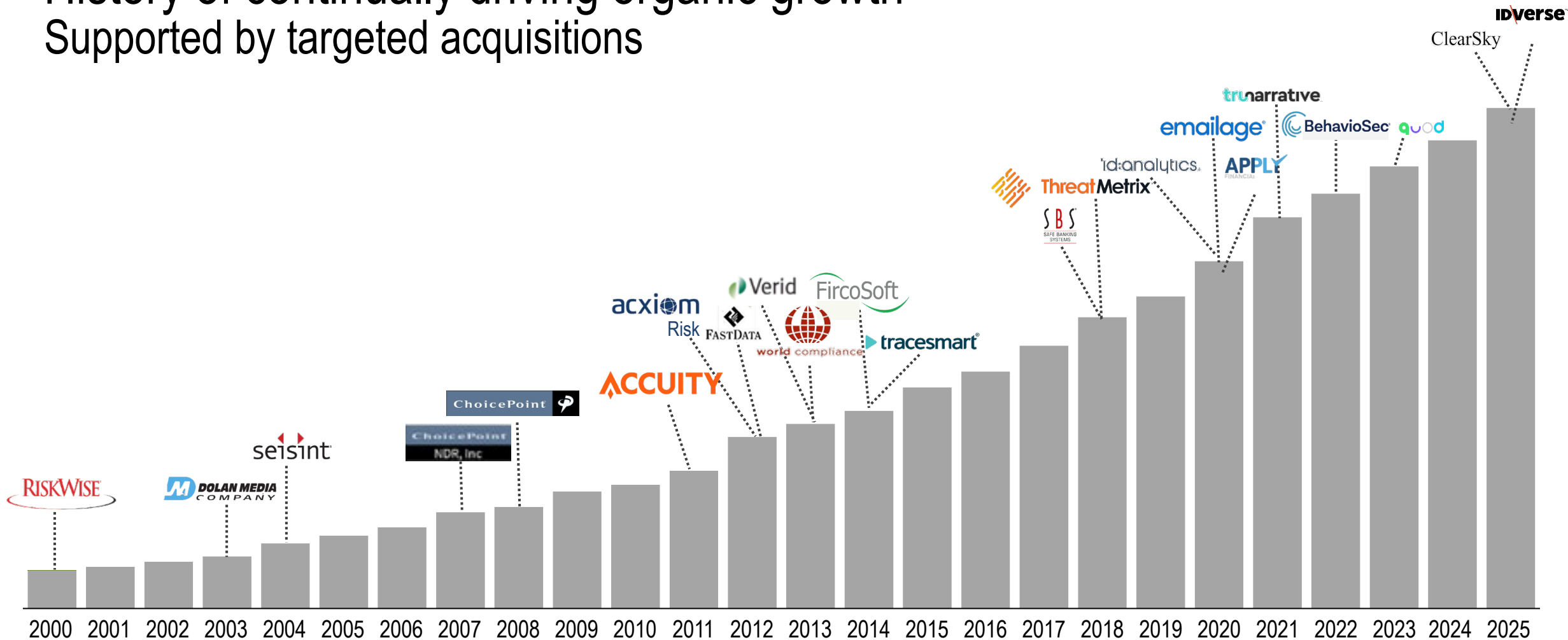
Customer relationship over time, by annual contract value (ACV)

Customer example: US Financial Institution



- A customer uses 8 products on average
- Customers spending >\$5m annually use 13 products on average
- Adoption increases as customer value grows

History of continually driving organic growth Supported by targeted acquisitions



Build out of US data and technology capabilities

Global expansion

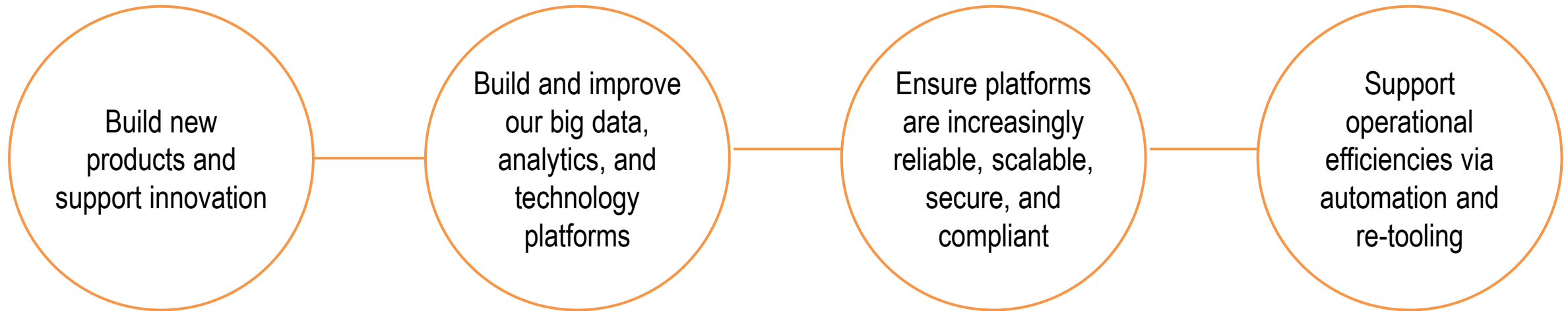
Expansion of digital identity capabilities

Risk technology

Vijay Raghavan

Chair, RELX Technology Forum and CTO, Risk

RELX technology



Global Scale

- \$2bn RELX annual technology spend
- More than 12,000 technologists at RELX
- 15+ years of experience with big data and AI/ML
- Technology agnostic
- Leverage approaches across RELX

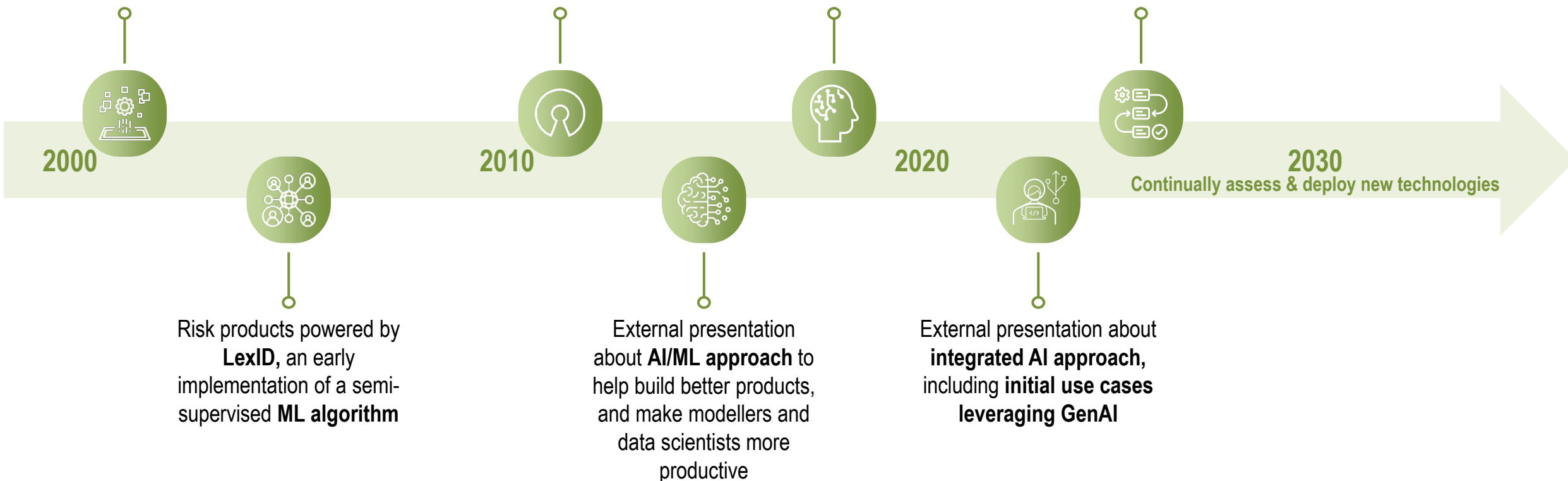
We have a long history with Big Data, Machine Learning, and Artificial Intelligence across Risk

Risk Big Data platform (**HPCC**) gave us a head start in handling large-scale problems

External presentation about Big Data. **Open-sourced** our Big Data platform to invite contributions and increase pace of innovation

External presentation about Risk's **multi-algorithm AI approach** to solve risk problems, leading to better decisioning

Embedding **GenAI and Agentic tools** across product lifecycle, to improve speed, accuracy while enhancing security and compliance posture



Risk's technology platform enables agile innovation at scale

Applications and Product Layer

Core intellectual property including data model foundations, analytic models, and secure product delivery

Enables robust entity resolution, knowledge graphs, self-service analytics, development efficiency, and fast processing speeds



Abstraction Layer

(for control, flexibility, and trusted AI infrastructure)

Proprietary layer that standardises access to 3rd party AI/ML tools to develop data products faster

Enables agility, extreme reuse, vendor neutrality, and adherence to responsible AI that our customers expect of us



Infrastructure Layer

Underlying infrastructure that leverages 3rd party tooling for servers, networking, storage, databases, and AI capabilities

Vendors include cloud providers, managed databases, and LLMs

Risk's trusted AI Infrastructure is foundational to our AI-based products

Applications and Product Layer

Select examples of recent advancements

Omega AI: AI-powered data engineering
Entity Database: Unified data assets



Proprietary Omega AI enabling:

- Improved data processing speed
- Increased development efficiency
- Fast, accurate data transformation
- Automated data mapping of fields
- Anomaly detection and correction

Proprietary Entity Database enabling:

- Trusted, comprehensive data repository
- Self-service analytics & efficient product delivery
- Consistency of data access
- Secure data delivery to products
- Standard APIs

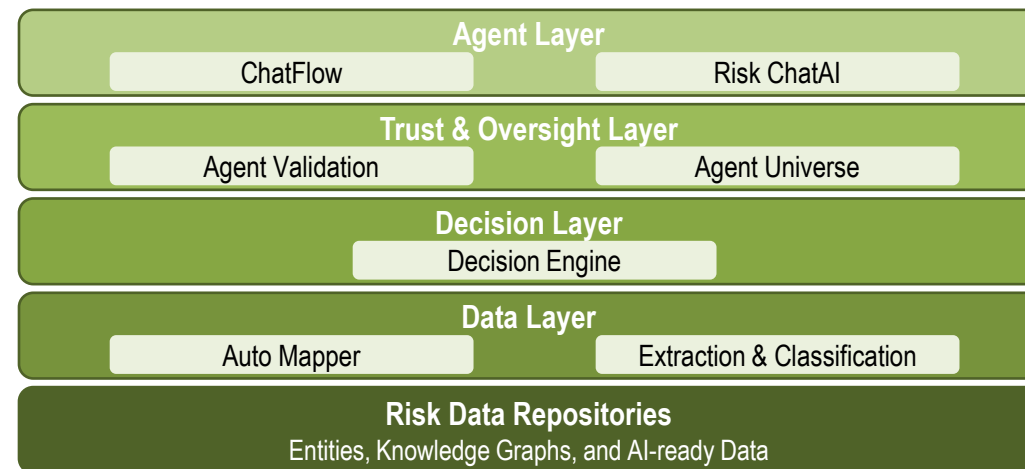


Abstraction Layer

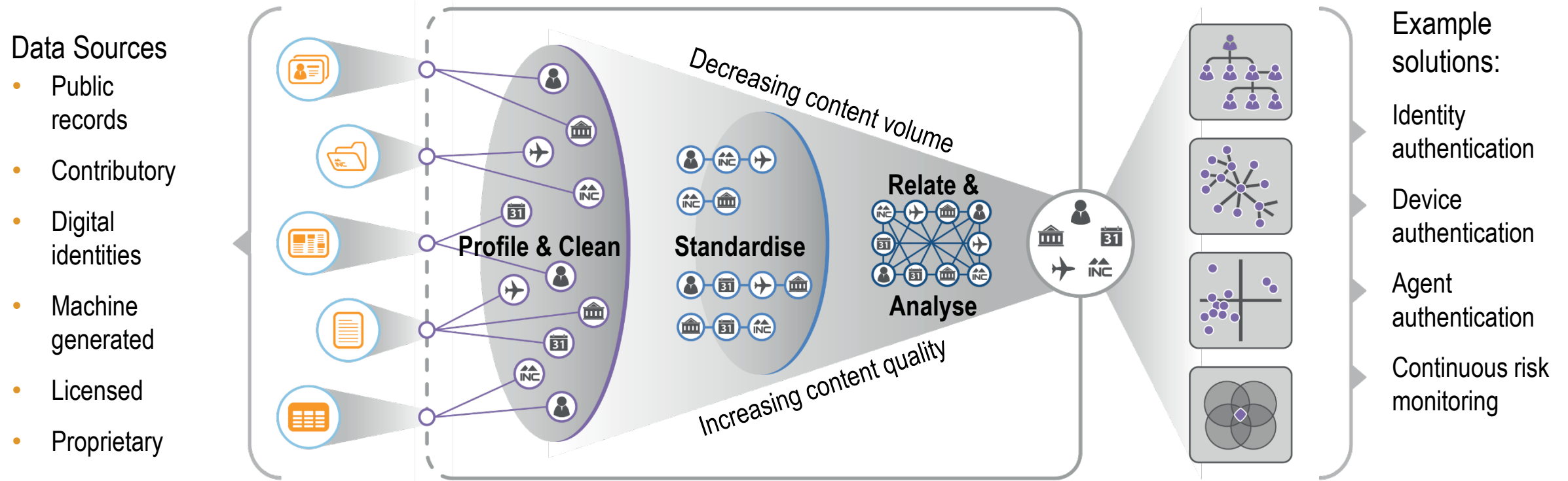
(for control, flexibility, and trusted AI infrastructure)

Select examples of recent advancements

Trusted AI infrastructure: Defensibility, transparency, and determinism on top of AI



Big data and extractive AI at Risk



Unstructured and structured content	Big data platforms	Analysis applications	Customer single point of execution
-------------------------------------	--------------------	-----------------------	------------------------------------

- Over 13 petabytes of data
- Tens of billions of public records
- Tens of thousands of sources
- Billions of device and asset identities
- Billions of records processed daily

- Grid computing with low-cost servers
- Linking algorithms that generate high precision and recall
- Machine learning algorithms to cluster, link and learn from the data
- High speed data ingestion, recall, and processing
- Rapid development cycles
- Platforms to facilitate AI/ML

- Proprietary algorithms
- Predictive modelling
- Machine learning and artificial intelligence

- Modular product suites
- Flexible delivery platforms
- Machine-to-machine delivery

We continue to improve our data foundations and products using latest AI technologies

Select examples

Image Analytics: LexisNexis® Flyreel®

- An AI-powered image capture solution for insurers
- **Analyses property or vehicle images** and extracts critical data
- Helps reduce **physical inspections** and **improve consistency**

GenAI & Agentic AI: LexID®

- **GenAI and agentic AI** applied to **improve linking** and **strengthen holistic view of identity**
- Data foundations **continuously optimised** for AI systems and agents
- Better linking accuracy leads to higher precision and recall

Neural Networks: IDVerse®

- **Deep neural network-based identity verification**
- **Combines AI techniques** such as OCR, document analysis, face recognition, liveness, and face matching
- **Enables faster, lower-friction identity verification**, with automated decisioning

Process innovation and agility

We leverage AI to improve processes and manage cost growth below revenue growth

Select examples

Technology

- AI-assisted coding to enhance code quality, and shorten software development lifecycles
- Automated controls and monitoring to reduce risk and support compliance

Operations

- AI-assisted evaluation of customer contracts to derive pricing, billing, and fulfilment insights
- AI-enabled data extraction from insurance rate filings to drive our rate comparison products

Customer Support

- AI agent to improve response speed and consistency
- AI-driven case routing and prioritisation to improve operational efficiency

Sales & Marketing

- AI-assisted analysis of customer conversations to surface insights and improve conversion

Technology summary

- Technology is a key enabler of our innovation
- We have a long history of leveraging AI and other advanced technologies to improve the accuracy and value of our solutions, accelerate innovation, and enhance efficiency
- By continuing to assess and deploy new technologies, we are strengthening our ability to deliver greater value, at a faster pace, and more efficiently

Fraud & Identity deep dive and case studies

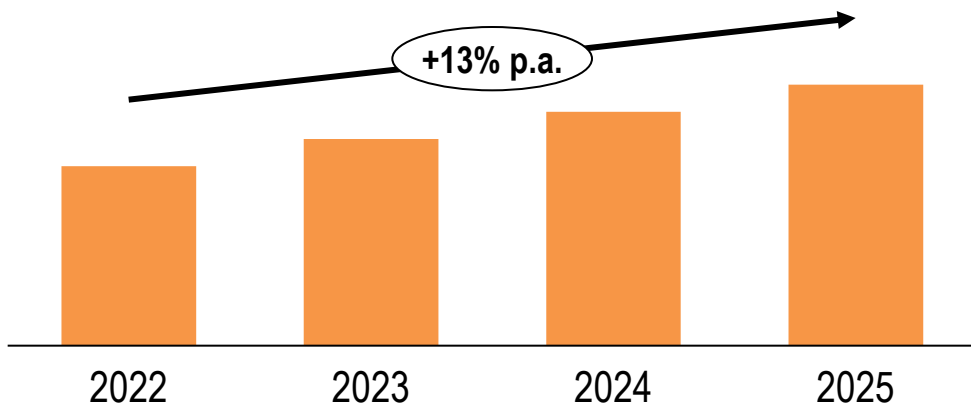
Kim Sutherland

Vice President and Global Head of Fraud and Identity

Consumers are increasingly transacting through broader digital touchpoints, making risk assessment more complex

Digital consumer activity is increasing

Consumer interactions observed in Risk Intelligence Network¹ (bn)



Broader touchpoints driving complexity

- **Multiple channels:** online banking, digital wallet, instant payment, account-to-account transfer, contact centre, agentic
- **More devices:** mobile app, mobile browser, desktop web, tablet, connected device
- **More service touchpoints:** password resets, detail changes, new device registration, chatbot interactions

We layer fraud defences across the consumer lifecycle

Consumer Account Lifecycle



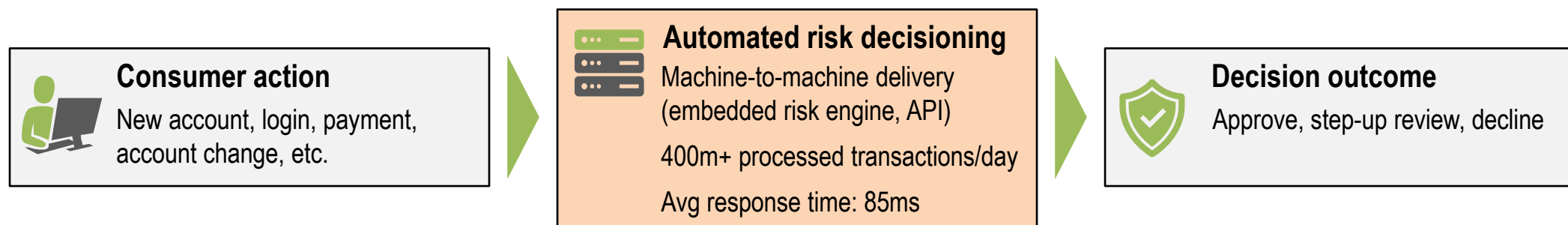
Integrated Platform
Single point of access to fraud and identity solutions

Four layers of defence to protect consumers

Digital & Identity Assessment	Device Intelligence	Location Intelligence	Identity Attributes	Identity Verification	Behavioural Intelligence	Bot & Agent Intelligence
Decision Analytics	Decision Policies	Identity Linkages	Fraud Analytics	Machine Learning	Orchestration	Integration
Authentication	Device Binding	One Time Password	Authentication by Link	Dynamic KBA	Biometrics	Document Authentication
Investigation & Review	Forensics & Investigation	Case Management	Lists	Reporting	Policy Governance	Fraud Feedback

Capabilities listed are illustrative, non-exhaustive

We enable real-time decisions inside the customer workflow



Automated checks executed in real time

1. Establish the identity:

- Have we seen this identity before?
- Have we seen this device before?
- Do we have any signals or history within our network?

2. Quantify the risk:

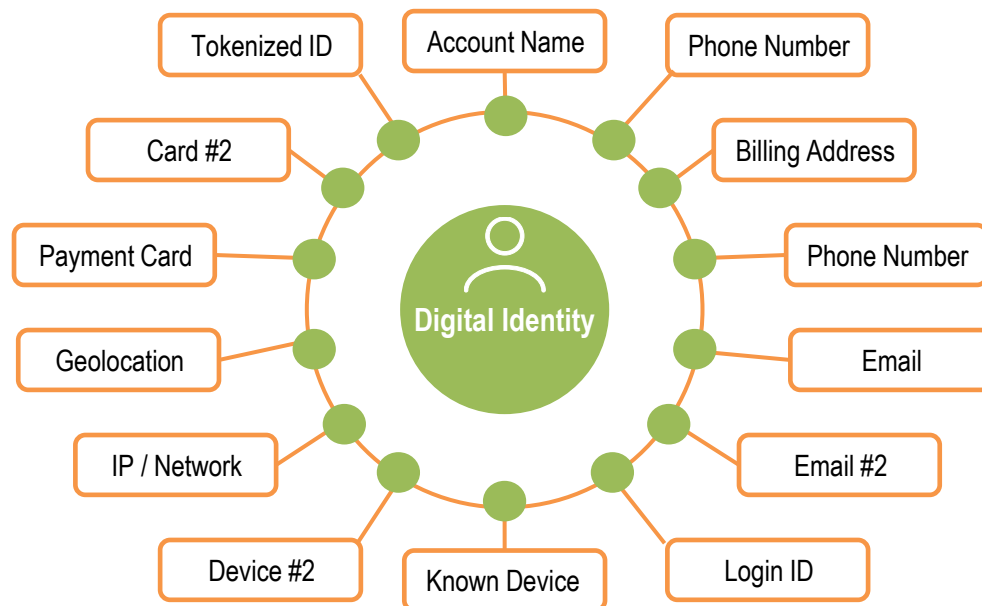
- Are the attributes accurate?
- Is there any suspicious activity associated with the behaviour, device, or identity?
- Is this person vulnerable or potentially a victim?

3. Define the response:

- Do we need more assessment of risk?
- What is the next best action?

Our network turns disconnected signals into a connected identity graph

Trusted identity graph



Typical attributes of a trusted identity:

Email	1 - 2
Device	2 - 4
IP	Static; Dynamic
Billing Address	1 - 2
Payment Cards	2 - 4

Signals that may identify bad actors:

- **Bot fingerprints:** Speed, rhythm, and latency that signal non-human interactions, aggregators, and scripted behaviour
- **Identity shapeshifting:** Rapid attribute changes (email, phone, address) that don't fit the identity graph
- **Coercion indicators:** Unusual behaviour patterns (dwell times, copy-paste) consistent with being guided by another party

Login analysis and network example (video)

The image shows a composite view of a banking website and its associated analytics. On the left, a 'Sign In' form is overlaid on a background image of gold coins. The form includes fields for 'Username' and 'Password', a green 'Sign In' button, and a link for 'Don't have an account? Create One'. The website header features 'Generic BANK AND FINANCE', navigation links 'Borrow Save Spend', and buttons for 'Payments / Deposits' and 'Create Account'.

On the right, an analytics sidebar displays the following information:

- Scenarios: < Scenarios
- Scenario: Save Clear
- Session ID: a4c43929-ae00-4ed0-a615-b2926676... with a Reprofile button.
- Implementation and Advanced Inputs buttons.
- Behavior tab selected under Events.
- BehavioSec Profile section with a note: '(Typically, just use one of the 'canned' profiles. Or train one your 3 default profiles; these are unique to you.)' and a 'Select a Profile' dropdown.
- Mouse Coordinates: 1511, 500
- Offpage Counter: 3
- Left Clicks
- Middle Clicks
- Right Clicks
- Tabbed Fields
- Pasted Fields
- Cut Fields
- Coppied Fields

At the bottom, three small thumbnail images are visible: hands counting money, a view of Earth from space, and an ATM sign at night.

Case study: One blocked attack exposed a broader, international fraud network

Context

A **bad actor** attempted to log into an account at customer Bank A using **stolen credentials**

Multiple attempts were made using **different credentials** in a short period

Immediate Benefit

Our solutions enabled Bank A to stop an account takeover before loss occurred

Embedded **risk engine automatically** captured high-risk signals

Network Benefits

Risk Intelligence Network linked original device to other risky devices

From one incident, we:

- **Linked 26** more devices that had been used fraudulently
- **Blocked 18** more fraud attempts across **18 different organisations**

Why it matters

One incident prevented fraud across our entire network

Without our network, no single organisation can see the full picture to combat fraud at scale

New account opening case study

Matt Adams, Chief Technology Officer and Co-founder, IDVerse
Daniel Aiello, Chief Product Officer and Co-founder, IDVerse

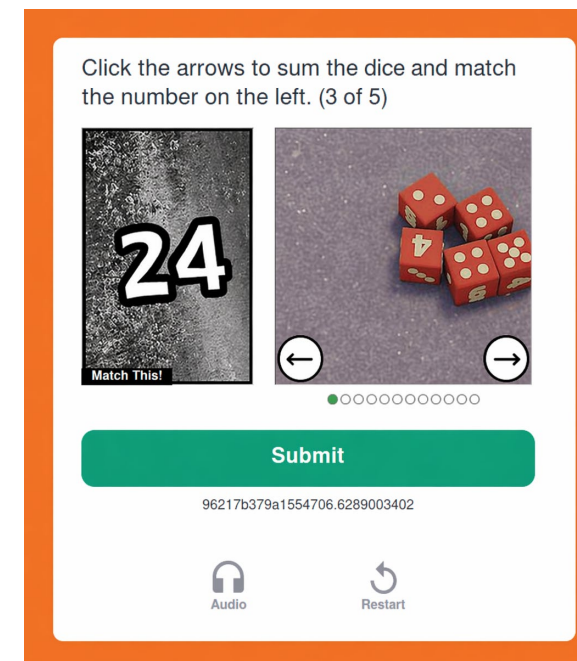
New account opening is a high-risk decision

What makes new account opening difficult?

- Digital onboarding creates fraud opportunity
- Limited history at moment of decision
- Bad actors only need to get through once
- Pressure to approve quickly
- Manual review: expensive, slow, inaccurate

Every safeguard adds friction to consumer experience

- **Captcha**
- SMS OTP
- Document data check
- Q&A
- Phone call
- In-person visit



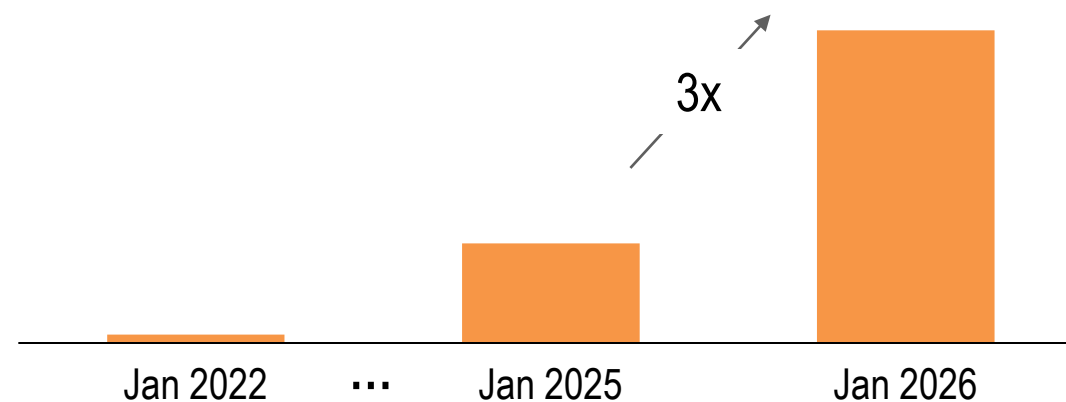
Synthetic identities and deepfakes are creating new challenges, at a scale never seen before

Synthetic identities are easier and cheaper to acquire

- Breached PII¹ and stolen credentials supply **abundant raw materials for fraudsters** - available online for as little as \$10²
- **AI-generated fake IDs** - complete, realistic, produced for around \$15³

We've seen acceleration of synthetic identity attacks

Deepfake attack volume⁴, 2022-2026



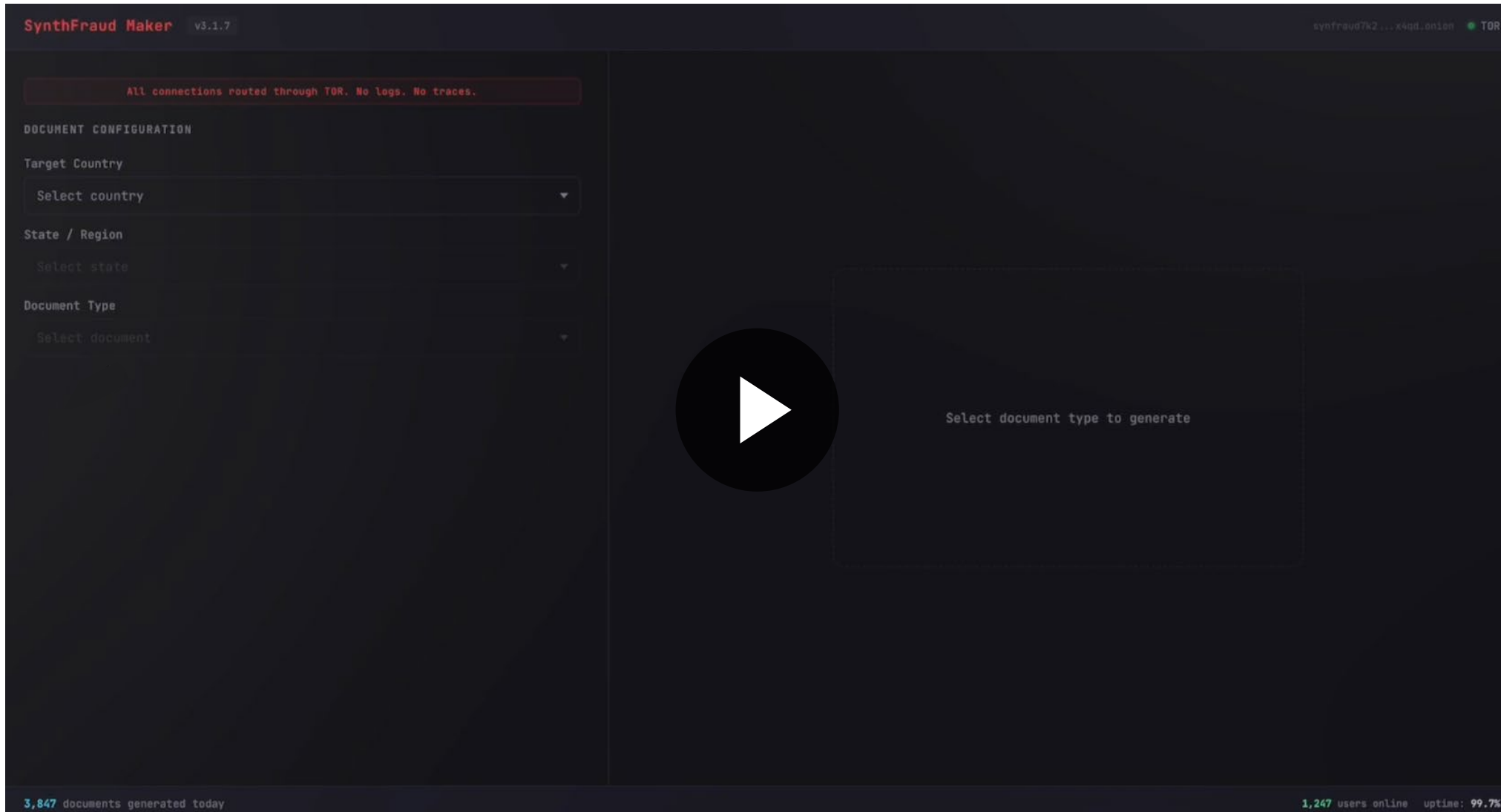
1. Personally Identifiable Information

2. Verizon Data Breach Investigations Report, 2024

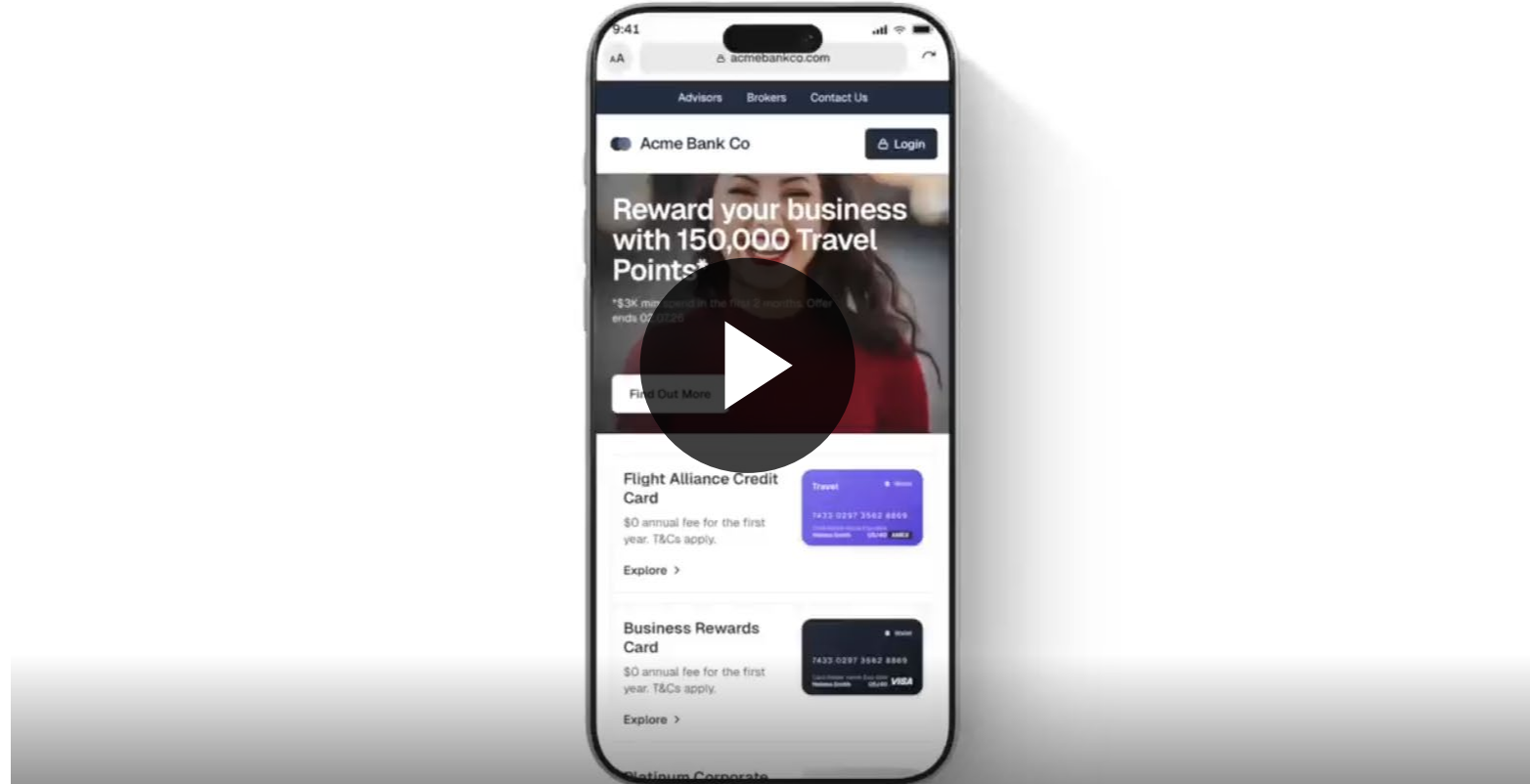
3. 404Media, "Inside the Underground Site Where 'Neural Networks' Churn Out Fake IDs"

4. Risk internal analysis; attacks seen within IDVerse workflows

Fraudster generating synthetic identity (video)

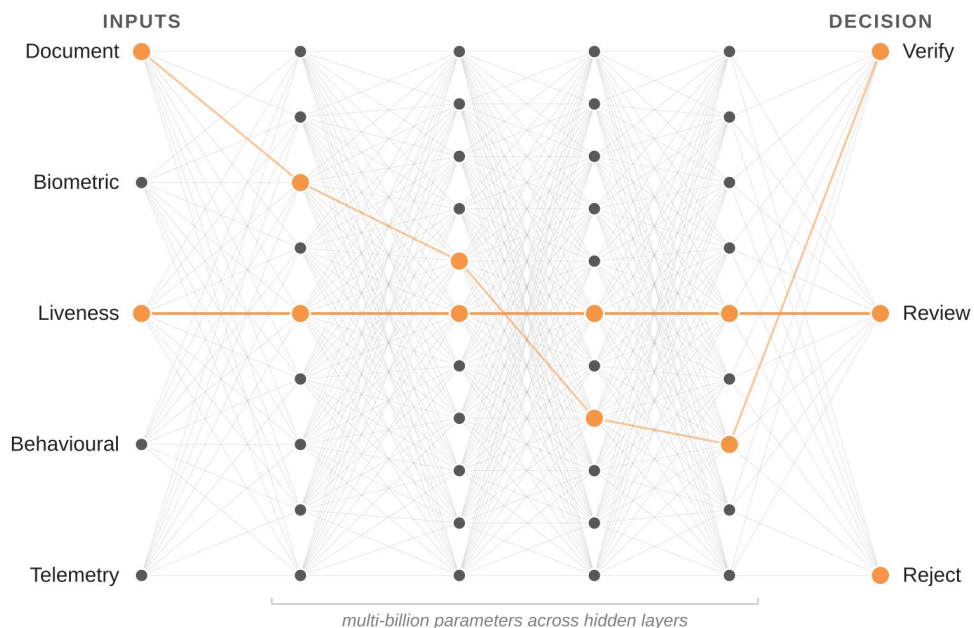


IDVerse - Consumer new account opening (video)



Our Engine: A multi-billion parameter neural network

Deep neural network learns subtle patterns



Purpose-built AI engine for identity fraud

- **7+ years** of training on real-world fraud attempts – data not available in public datasets
- **Refreshed continually** as new attack patterns emerge across our network
- **Multi-billion parameter model** to catch new signals, forgeries, deepfakes, and emerging variants in real time

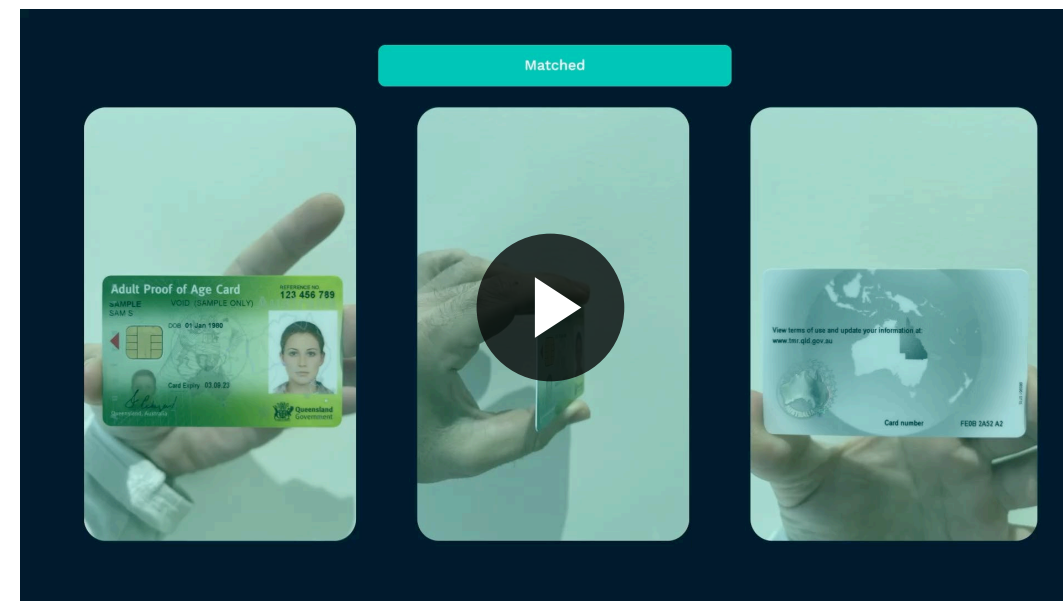
Layer 1: Document Authentication (video)

A proprietary deep neural network interprets the document holistically

- **Up to 300 automated checks:** pixel-level analysis, colour, lighting, font, alignments, screen detection, deepfake detection, metadata analysis
- **Global coverage:** virtually all government-issued photo IDs, 220+ countries & territories, 140+ languages. Growing digital ID acceptance
- **Structured data extraction:** OCR-captured identity data contextualised for downstream onboarding



Outcome: A real identity as presented on a real, trustworthy and present ID document



Layer 2: Biometric Liveness & Face Match (video)

Proprietary liveness and presentation-attack detection, running server-side with no additional steps for the user

- **Injection-attack detection:** deepfakes, 2D and 3D masks, screen replays, AI-generated face-swaps
- **Server-side analysis:** no additional steps, motions, or prompts required from the user
- **Live-face-to-document match:** the confirmed live face is matched against the face on the authenticated document

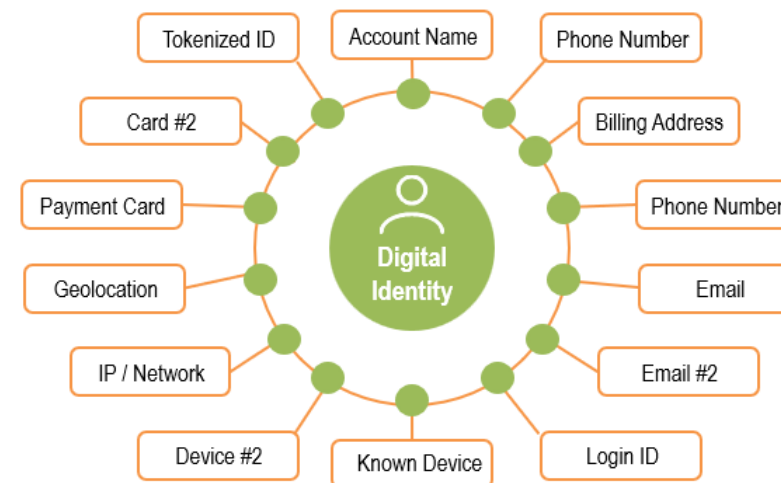


Outcome: A live, present person - confirmed and matched to their document

Layer 3: Identity Intelligence

Our Risk Intelligence Network analyses the identity data of every transaction in addition to the document and biometric verification

- **Does the device, IP, and location fit the applicant?**
Context analysed across every transaction
- **Are there synthetic, compromised, or manipulated signals?**
Risk patterns assessed in real time
- **Does the broader network support trust?**
Cross-referenced against global identity intelligence



Trusted identity graph



Outcome: A 360° view of identity risk, through a single integration with the world's largest Risk Intelligence Network

Our solutions allow customers to grow their business confidently

- Trusted applicants move through in seconds – friction applied only where risk requires it
- Bad actors are stopped before fraudulent accounts can be opened

Key takeaways

- We operate in large, global, and fast-growing segments
- Rapid technology advancements are accelerating global fraud attacks, increasing customer demand
- Our solutions enable our customers to have trusted interactions with their customers throughout their lifecycle, delivering measurable value uplifts
- Our objective is to continue to deliver strong underlying revenue growth for a long time to come, driven by organic product innovation and supported by targeted acquisitions
- We leverage evolving technology to add greater value to our customers, accelerate innovation, and operate more efficiently, with underlying profit growth exceeding underlying revenue growth

Q&A