



EQUIFAX[®]

White Paper

Identity Trust — Your frontline defense in the battle against fraud

Catch fraud at the front door, while facilitating secure, seamless consumer interactions

Laurie Anderson
Sr Director, Product Marketing, Equifax
Identity, Fraud and Compliance

March 2021

Contents

What exactly is Identity Trust?	3
The shift to next-gen ID verification	4
Change is needed — data is no longer enough	5
Digital transformation = increased need for digital signals	7
Components of Identity Trust.....	8
Start building Identity Trust today.....	9

What keeps fraud executives awake at night? The short answer is, a lot. A 2020 PWC global fraud survey¹ puts the price tag of all fraud — internal (employees) and external (customers, hackers and third-parties) — at a stunning \$42 billion. Another 2020 study² estimates ecommerce businesses will cumulatively lose more than \$200 billion to online payment fraud between 2020 and 2024.

It's a battle to the bottom line, no doubt, and while it may sound like fraudsters are winning, businesses are reloading their weapons and adjusting strategies with next-gen identity and fraud risk models. They're integrating multisource data with advanced Artificial Intelligence (AI) technology and modeling techniques to establish a level of trust in every online identity, a concept called "identity trust." By assigning identity trust in real-time, at every digital touchpoint, organizations can verify the identity behind online transactions, account creations and logins, in split seconds.

Here, we explore the concept of identity trust and why it's critically important given shifting, pandemic-driven consumer behaviors. We also explain the role identity trust can play in an organization's digital transformation and offer practical steps to build identity trust within your business. Keep reading, the battle against fraud is about to get more interesting.

What exactly is Identity Trust?

At its essence, identity trust is about having confidence that: 1) the people accessing your services are who they say they are; and 2) their intentions are what they say they are. This is important for a couple of reasons. Being able to trust consumer identities as they're presented in real-time across any digital interaction helps strengthen and protect the entire customer journey, from account generation and login to payments and disputes. In turn, this can help increase approval rates — and ultimately, revenue — while reducing manual reviews, false positives and chargebacks.




Identity trust helps ensure the user trying to log in to a banking app is an authorized account holder — not a fraudster who hacked or stole the information. Or, say a retail customer is attempting to checkout online as a "guest." Identity trust comprehensively cross-references and validates their identity including their device information, in real time, without adding friction that might cause a legitimate customer to abandon their cart.

Identity trust decisions are complex, drawing on a multitude of intelligent data, behavior patterns and signals, and typically involve the three key stages identified below. The process is dynamic and multifaceted, as it's designed to present a 360-degree view of risk, in seconds.

By assigning identity trust in real-time, at every digital touchpoint, organizations can verify the identity behind online transactions, account creations and logins, in split seconds.



Three stages of Identity Trust assessment

1. Affiliation 	2. Risk 	3. Authentication 
Match input data against credible or authoritative data sources	Calculate and analyze data and attributes to identify risky and fraudulent behaviors	Validate or prove the identity using key forms of personal identification
Example: Matching basic personal identifiers (such as national ID) and digital identifiers (such as email, phone) against trusted data assets	Example: Using factors such as velocity (volume of transactions within a short time), inherent data insights (pre-paid mobile phone vs. traditional mobile account) and fraud scores	Example: Using one-time passcodes, biometrics, document verification and liveness detection testing

The shift to next-gen ID verification

Credit risk models and fraud risk models are different. Credit risk models primarily focus on the individual's ability to pay, whereas identity and fraud risk models focus on confirming the identity and intent behind the transaction. It's an important distinction because while both are essential tools, if you're only assessing credit risk, you could be overlooking gaps in identity trust.

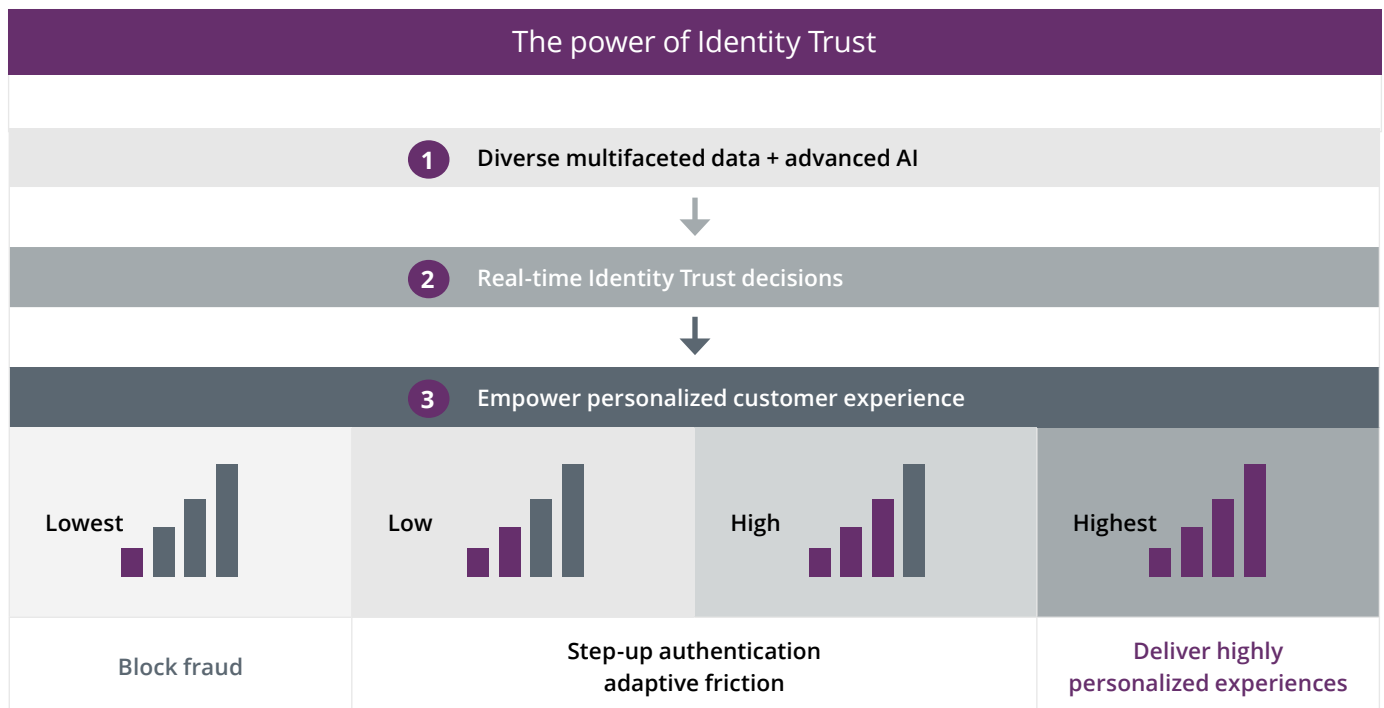
Then there are legacy fraud analytics. Often rules-based and labor-intensive, they can be fueled by siloed data and outdated technologies that are incapable of analyzing disparate data in real-time. The result is an incomplete view of risk and increased customer friction. Also, these solutions aren't typically scalable across an enterprise for optimal coverage of all digital interactions. This could leave you vulnerable to sophisticated, fast-moving fraudsters.

Today's next-gen identity and fraud solutions level up the fraud-fighting arsenal. They're powered by multiple, diverse data sources, a mix of digital and biometric attributes (IP address, facial recognition and fingerprints), behavioral insights (screen time, usage, etc.), dynamic signals from shared devices and accounts and advanced AI modeling techniques — even platforms — all across a single enterprise. Everything is validated, cross-referenced and connected in seconds "behind the scenes" to detect anomalies or other issues that might indicate fraud. The result is a fast and flexible approach, that's also comprehensive and sophisticated.

Businesses can visualize trusted identities and fraud risk across their organization and make the best decision for every individual consumer interaction. Meanwhile, consumers can enjoy a near seamless, frictionless experience that keeps them engaged through account opening and beyond.



If you're only assessing credit risk, you could be overlooking gaps in identity trust.



Businesses can visualize trusted identities and fraud risk across their organization and make the best decision for every individual consumer interaction.

Val needs a vacation: The impact of Identity Trust on your customer's journey



This is Val.

His brother is getting married out West and he wants to surprise his wife with an extended trip to the Rockies after the ceremony.

He's planning to finance the trip with a low-rate vacation loan.



He visits his credit union's website and logs in using his personal information, including name and email.

In real time, Val's information is matched and assessed against multiple data sources including identity data, utility data, mobile phone data and email data.



This behind-the-scenes data assessment provides passive, non-intrusive identity resolution to build trust in Val *and* his device.

The credit union can instantly establish trust in Val to help make a risk assessment prior to making an offer.



Because the cross-checking of his data is done behind the scenes, Val isn't inundated with authentication questions and can complete the application online from the convenience of his kitchen table in 10 minutes...

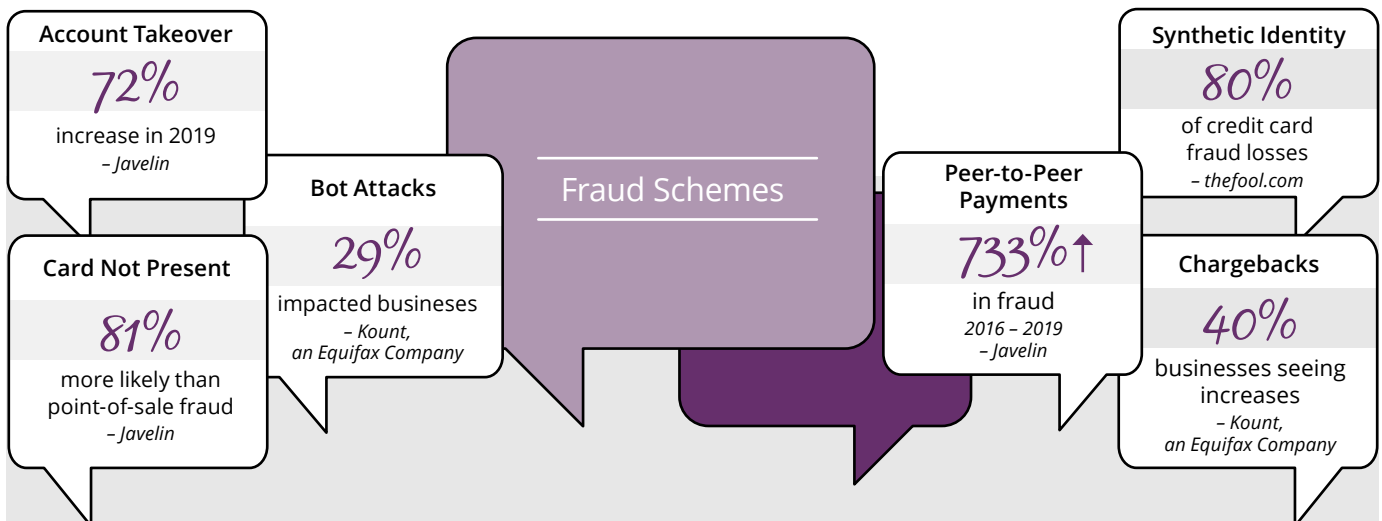
...just in time for dinner, where he plans to tell his wife the good news.

Change is needed — data is no longer enough

The shift from static, one-dimensional data analytic views toward actionable, big-picture insights delivered in real-time is overdue for many reasons.

- **The pandemic.** Fraudsters are nothing if not resilient and opportunistic, as they race to exploit the "crisis of the moment." Today, that crisis is the COVID-19 pandemic. With consumers forced to shelter-in-place for months on end, ecommerce sales surged an astonishing 44 percent over 2019, reaching an eye-popping \$861 billion in 2020.³ Fraudsters followed the money trail, with the dollar amount of attempted fraudulent transactions rising 35 percent⁴ in April 2020.

Fraud schemes including account takeover, synthetic identity, card-not-present, chargebacks and peer-to-peer payment fraud plague all industries, causing businesses and their customers untold frustrations, inconveniences, expenses and losses. Left unchecked, these types of fraud losses are on track to escalate more than 50 percent⁵ in coming years, topping \$25 billion annually.



- **The customer experience.** After the unprecedented challenges and difficulties of 2020, businesses are fighting hard for every customer. As a result, it's more important than ever before to strike the right balance between better fraud detection *and* an improved customer experience. A 2020 survey by Kount, an Equifax company⁶, revealed that 25 percent of Americans say they would not return to a website if turned away from a legitimate transaction (i.e., false declines). Instead, they would take their business elsewhere.

Businesses are getting the message loud and clear. According to a recent Aite survey, 65 percent of organizations admit that improving the client experience plays a greater role in getting their fraud investments funded.

25% of Americans say they would not return to a website if turned away from a legitimate transaction (i.e., false declines). Instead, they would take their business elsewhere.



- **The digital ID.** Digital identities (digital IDs) are sweeping the world. As the name implies, digital IDs are electronically issued—versus traditional paper identification like driver's licenses and passports — by government entities, businesses or individuals with the consumer's consent. They can include everything from personal data and biometrics to emails, PINs, passwords, security tokens, mobile devices and more.

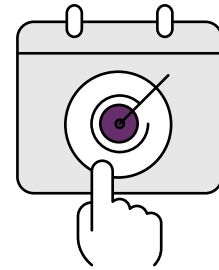
A recent study⁷ estimates that the number of digital identity apps in use today, more than 1 billion, will explode to more than 6.2 billion by 2025. For context, the total population of the world today is 7.8 billion.

Digital transformation = increased need for digital signals

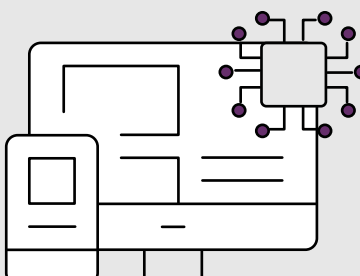
Digital transformation is *the* buzzword today. It refers to the use and integration of digital technology across all areas of business to improve value, outcomes and experiences. As more transactions move to digital, and at a higher frequency, customer relationships are being tested and challenged with every interaction. This is when it becomes important to apply digital signals acquired from the interplay of multifaceted data used to compile a digital profile of the consumer. These data and signals can facilitate trusted, split-second identity decisions.

Let’s take a closer look. Identity trust decisions occur throughout the customer lifecycle and across multiple touchpoints. For example, trust decisions are made when a customer applies for a new financial product, attempts to log in, makes a high-value financial transaction, contacts the call center, makes a change to their contact address and so on. Considering the scope and diversity of these interactions, organizations need access to a continuous feed of multisource data and digital signals regarding a consumer’s past interaction, present context and predicted intent.

Identity trust decisions occur throughout the customer lifecycle and across multiple touchpoints.



Using digital signals to mitigate fraud	
Assessing a consumer’s past interactions, present context and predicted intent	
Past Interactions	<ul style="list-style-type: none">• Access a consumer’s past interaction data (while preserving privacy) to determine deviations from behavioral norms. For example, is the consumer attempting to gain authorized user status on multiple accounts of others, or is he suddenly hyper-monitoring his credit report?• Historic data can help connect various entities for AI and machine learning capabilities to uncover hidden insights and patterns.
Present Context	<ul style="list-style-type: none">• Be context aware by only using attributes that are relevant to the trust decision being made. For example, is the consumer enrolling in a gym membership or accessing tax records?• Contextual clues from real-time signals such as IP address/ location or time of day can help provide the best customer experience while managing risk.
Predicted Intent	<ul style="list-style-type: none">• Use AI and machine learning models to assimilate and analyze various digital and non-digital signals. For example, this might involve building algorithms to determine identity discrepancies, such as “address is nonresidential” or reported as being misused.• Integrating signals with AI-enabled technology allows organizations to pinpoint fraud types with high precision so that appropriate methods can be applied to thwart fraud attempts.



Digital transformation refers to the use and integration of digital technology across all areas of business to improve value, outcomes and experiences.

Components of Identity Trust

Knowing that identity trust is essential to any business operating in today's digital world, what are its key ingredients? As with all things in analytics, identity trust begins with the data. More importantly, however, is how that data is put together to create a big-picture view of risk. Here we explore the components of identity trust in greater detail.

Multisource, multidimensional data. The importance of data diversity cannot be understated. To build a fast-moving, "all-angles" view of fraud risk, you need access to multiple data sources. It helps fill gaps in identity assessments and reduce uncertainty around the identity, therefore reducing risk. A few examples are provided below.

- Direct-from-government data sources, such as Social Security Administration and Department of Motor Vehicles
- Employment data including dates of employment
- Public records, such as bankruptcies, liens and lawsuits
- Transactional data, including digital purchases and attempted purchases
- Self-provided data such as social media data
- Passive data linked to websites, emails, mobile devices, IP addresses/location and more
- Meta-data generated from: 1) consumer interactions such as applying for a loan; 2) associations with other elements such as same phone but different mailing address; and 3) feedback outcomes such as a successful attempt using a one-time-passcode

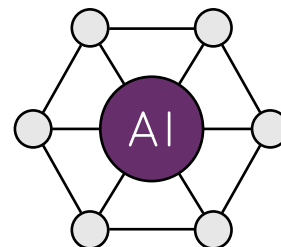
An important clarification here: more data isn't always better when establishing identity trust. The goal is to tap the *right data*, whatever that might be based on your risk levels and business model. Once the right mix of data is in place, apply the appropriate AI-driven modeling technique to experiment, establish baseline behaviors, predict intent and deliver precise, meaningful assessments in milliseconds. We'll touch on AI next.

AI and machine learning technology. The analytic models created to fight fraud today must be equally — if not more — innovative and iterative than fraudsters themselves. This makes machine learning models — both supervised and unsupervised — ideal for fraud mitigation. When appropriately designed and trained, these models will continually learn and adapt to fast-moving fraud patterns, with little to no human intervention. Read: fast, adaptive fraud detection.

Moving to a machine learning model is critical to battling today's high-tech fraudsters, but it can be hard to know how or where to begin. To correctly formulate these models, it's important to start by accurately articulating the business problem. Ask critical questions upfront so that relevant design parameters such as training population, sampling and weighting schemes, segmentation, and even appropriate algorithms, can be chosen wisely. For example, you might pose the following questions:

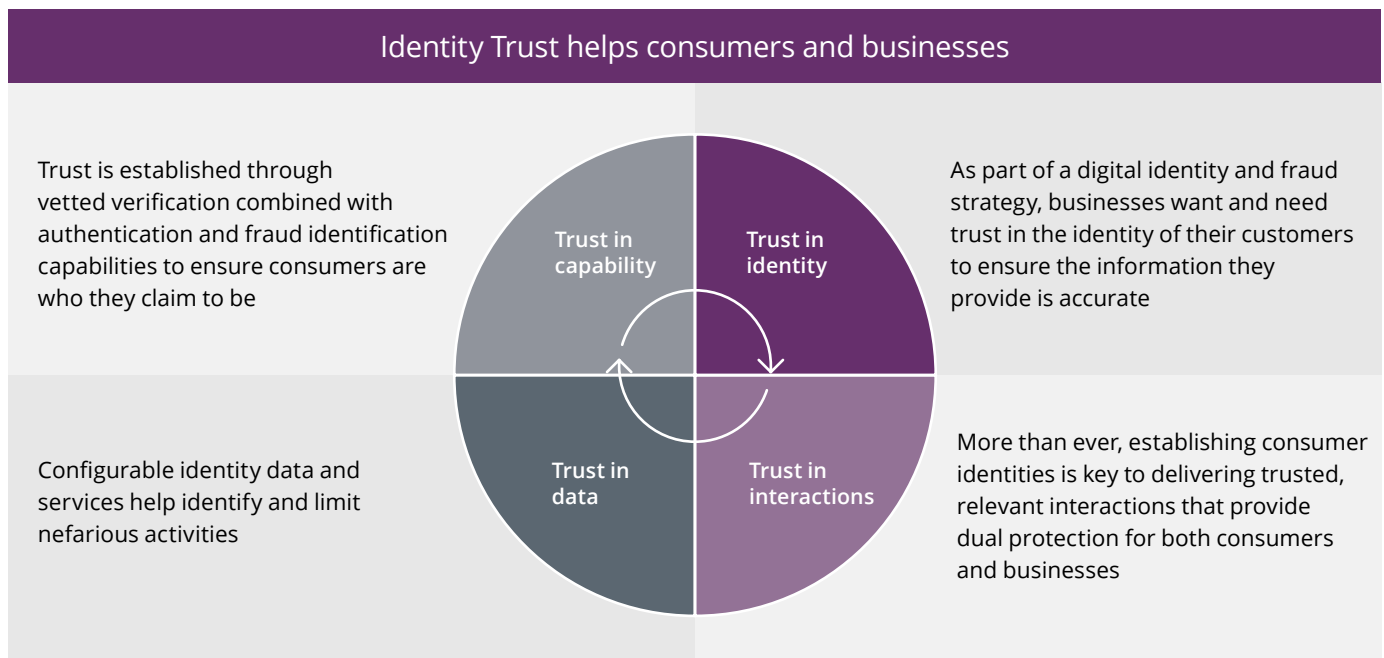
- Are you looking to replace an existing fraud model or augment the model as an additional layer of defense?
- Would you like to predict behaviors of a fraudster or capture patterns of fraud victims?
- Are there any biases in the label definition that need to be accounted for?

Moving to a machine learning model is critical to battling today's high-tech fraudsters



A guiding concept of trust: it's a two-way street. When done right, identity trust seamlessly bridges the gap between consumers and businesses, enabling them to efficiently move through a digital interaction. For consumers, it allows them to maneuver online interactions with ease, convenience and little to no headaches. What's more, those experiences are more likely to be personalized to their needs and preferences, further deepening trust in the business and its brand.

When businesses can trust consumer identities, they can preserve the resources normally dedicated to reviews, false positives and fraud recovery. In turn, they can potentially redirect those efforts and resources toward creating more rewarding and personalized customer experiences that help grow the business, and the bottom line.



Start building Identity Trust today

Managing identity and fraud risk requires dedicated, unwavering focus and effort across the enterprise. For businesses looking to modernize their approach, the first place to start is by establishing identity trust at the point of contact for every consumer interaction. This helps you to mitigate risk before it enters the business, while at the same time facilitating growth through improved operational performance and efficiency, faster account approvals and a better consumer experience.

Here are a few thoughts on getting started.

- *Initiate a top-down discussion.* Once the Chief Security Officer, fraud risk executives and analysts are on board, come together for an honest discussion about the best way to balance security and identity trust with the consumer experience, and determine what the first step should be moving forward.
- *Identify all consumer touchpoints in exhaustive detail.* A cornerstone of identity trust optimization is its enterprise-wide scope. Start by categorizing interactions in buckets that make sense for your business. For instance, this might be functional teams for larger organizations — think: marketing, sales, customer support, risk decisioning, etc. — broken down by channels such as email, phone, website, mobile app, etc. Another way to think about it is to track the consumer journey and document every possible point of engagement.

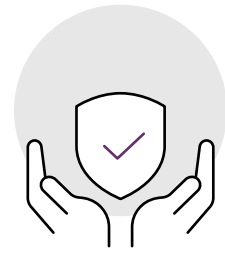


Managing identity and fraud risk requires dedicated, unwavering focus and effort across the enterprise.

- *Examine your existing digital fraud mitigation process.* This may take some time, but it's important to understand the various data and technologies underpinning your current strategy. What are your current goals and objectives and how can those be updated? What's working well and what's not? From there, start building or modifying your strategy.
- *Consult with a provider on the best way to adjust your current strategy or start from scratch.* Maybe you need different or more diverse data sources and digital signals to better understand consumers from all angles, in real time. Perhaps your anti-fraud processes are performing well, but your customer experience is clunky, and it's being reflected in your sales. Or maybe, you're ready to explore how the automation and adaptability of AI-driven technology can streamline and strengthen your fraud efforts. A trusted solution provider — one with proven experience creating identity trust solutions — can work with you step by step to build a solution that's customized to fit the precise needs of your business.

The battle lines against tech-savvy fraudsters are constantly being redrawn. Establishing digital identity trust can help you continuously evaluate new and evolving fraud risk and consumer identities in real-time across all digital channels, therefore, reducing your fraud vulnerability. At its essence, the power of identity trust is its reciprocity. It's founded on the ability to trust digital consumer identities no matter how or where they're presented to your business and the consumer's ability to seamlessly navigate online interactions without added friction. Getting it right involves an intricate mix of targeted, "behind the scenes" multisource data and signals combined with adaptive AI and machine learning technology.

If you haven't started the identity trust discussion within your organization, the time to act is now. Think of it this way: fraud is a moving target that's constantly closing in on your business. Digital identity trust is the scope on your fraud-fighting weaponry that can help you see it coming and mitigate against it.



Digital identity trust is the scope on your fraud-fighting weaponry that can help you see it coming and mitigate against it.



800.685.5000

equifax.com/business/digital-authentication

About Equifax

At Equifax (NYSE: EFX), we believe knowledge drives progress. As a global data, analytics, and technology company, we play an essential role in the global economy by helping financial institutions, companies, employees, and government agencies make critical decisions with greater confidence. Our unique blend of differentiated data, analytics, and cloud technology drives insights to power decisions to move people forward. Headquartered in Atlanta and supported by more than 11,000 employees worldwide, Equifax operates or has investments in 25 countries in North America, Central and South America, Europe, and the Asia Pacific region. For more information, visit equifax.com.

1 <https://www.pwc.com/gx/en/forensics/gecs-2020/pdf/global-economic-crime-and-fraud-survey-2020.pdf>
 2 <https://www.juniperresearch.com/press/press-releases/online-payment-fraud-losses-to-exceed-200-billion>
 3 <https://www.digitalcommerce360.com/article/us-ecommerce-sales/>
 4 <https://www.wsj.com/articles/borrower-beware-credit-card-fraud-attempts-rise-during-the-coronavirus-crisis-11590571800>
 5 <https://www.infosecurity-magazine.com/news/global-ecommerce-fraud-to-top-25/>
 6 <https://kount.com/blog/new-research-reveals-the-ecommerce-keys-to-holiday-survival>
 7 <https://www.biometricupdate.com/202010/digital-identity-apps-to-outnumber-cards-by-2023-juniper-research>