White Paper

# The Currency of Business: How Experts Gain and Maintain Digital Trust in Their Organizations

Sponsored by: Telesign

Grace Trinidad
July 2024

## IDC OPINION

Trust is the currency of today's digital economy. Businesses that earn and keep it thrive. Yet with more than 5 billion users conducting their lives online — whether it's a teen interacting with friends overseas, a busy mobile professional paying their bills, or an enterprise transacting with millions of customers at a time — the stakes have never been higher. So, too, are risks from fraud, which inflicts approximately $8 trillion in annual, global damages. In this white paper from IDC's Future of Trust initiative, digital trust experts from a wide range of industries and backgrounds share best practices on earning and maintaining trust, no matter what the world throws at your organization.

## IN THIS WHITE PAPER



## METHODOLOGY

IDC conducted four interviews with digital trust experts from Microsoft (**www.Microsoft.com**), Persona (**www.withpersona.com**), Global Telco Consult (GTC) (**www.globaltelcoconsult.com**), and Northeastern University (**www.northeastern.edu**) to learn their strategies and methods for increasing trust in their organizations and in the partners with whom they work. Telesign assembled these experts — the Trust Alliance — to share insights and best practices that any organization can utilize to bolster their fraud protections and maintain trust with their customers and other important stakeholders. The content in this white paper comes directly from conversations with Trust Alliance members, held from January

2024 to April 2024. Quotes have been edited for length and clarity. When needed, contextual information or editing that is helpful for understanding a quote is demarcated in brackets.

## HOW AND WHY IS TRUST THE CURRENCY OF BUSINESS

IDC's August 2023 *Worldwide Future of Trust Survey* has shown that business leaders overwhelmingly believe in the importance of trust, with over 70% strongly agreeing or agreeing that:

- High trust in our organization improves our bottom line.
- Trust is critical for our organization to flourish.
- The trust and trustworthiness of the organization lends a competitive edge.
- Trust and trustworthiness of the organization protects business leaders against the consequences of negative events such as data breaches.

Organizations that prioritize trust programs — or investment in security, privacy, compliance, and ESG efforts — indicate statistically significant improvement in operational efficiency, business resilience, and sustainability (see *Prioritization of Trust Programs Yields Improvements on Key Business Outcomes,* IDC #US50475823, March 2023). Despite these gains, investment in trust has often fallen by the wayside as organizations prioritize other business priorities and/or margins. In fact, IDC research shows that 33.5% of organizational leaders globally find it challenging to improve perceived trust and trustworthiness because available resources are focused on other organizational priorities, and 34.6% of global respondents state that the recessionary environment of 2023 led to the reprioritization of strategic initiatives, including efforts to improve trust and trustworthiness (source: IDC's *Worldwide Future of Trust Survey,* September 2023). Yet those who continue to strategically invest in trust programs, despite these difficulties, enjoy greater customer loyalty, increased market share, increased collaboration and innovation, and increased customer willingness to use novel technologies like artificial intelligence (AI) and generative AI (GenAI) (see Sethi, A. R., Dash, S., Mishra, A., and Cyr, D. *Role of Community Trust in Driving Brand Loyalty in Large Online B2B Communities*. Journal of Business & Industrial Marketing, 2023,

### Experts in Their Own Words

"*The number 1 way to break trust is forgetting the human element. We live in a digital society and there's so much that's online, so much of our lives that exist there, so much of our business and organizations that have to operate there. Lacking empathy influences the way you build products, so think about accessibility within your projects, think about the experience that humans on the other end are going to have. If they have a terrible experience, more than likely they're not going to trust coming back to your products again and again.*" — Shinesa Cambric, principal product manager, Microsoft

"*Trust is just table stakes for any organization to be successful. Without trust, you're not getting into that stranger's car, and that ride-share business simply won't exist.*" — Daniel Lee, product lead of Identity, Persona

"*Pay now or pay later. When you lose your reputation, it's difficult to get back. That's why trust is a strategic investment. It's an investment in long-term versus short-term gain and growth.*" — Michael Woodson, former director of Information Security and Privacy, Sonesta International Hotels Corporation, and adjunct professor, Northeastern University

"*Building trust leads to improved conversion rates and fosters customer loyalty. Implementing a seamless and secure onboarding solution is crucial for optimizing customer conversion.*" — Guillaume Bourcy, partner and CIO, GTC

doi.org/10.1108/JBIM-10-2022-0469; Hanstad, T. *Trust Is the Glue of a Healthy Society. Here's How to Bring It Back.* World Economic Forum, 2020, www.weforum.org/agenda/2020/12/trust-is-the-glue-of-a-healthy-society-heres-how-to-bring-it-back/; Kalish, I., Wolf, M., and Holdowsky, J. *The Link Between Trust and Economic Prosperity.* Deloitte Insights, 2021; and Bareis, J. *The Trustification of AI. Disclosing the Bridging Pillars That Tie Trust and AI Together*. Big Data & Society, 11(2), 2024, doi.org/10.1177/20539517241249430).

As the complexity and opacity of our digital infrastructures grow, so does the importance of trust. Greater digital complexity creates greater information gaps — it is becoming nearly impossible to know everything about the products and vendors that comprise our digital infrastructures. Therefore, customers and clients must place greater reliance on quicker trust judgments to make timely decisions. The problem with trust, however, is that it is becoming more difficult to secure, especially for American customers who, in 2023, indicated steeply declining trust in key institutions and the lowest trust of any G7 country studied (source: www.economist.com/united-states/2024/04/17/americas-trust-in-its-institutions-has-collapsed). Most organizations understand that trust is important and that failure to secure it with customers will damage loyalty and market share and decrease the adoption of new or novel technologies. But how can we improve trust in an environment steeped in mistrust?

## BEST PRACTICES IN TRUST AND TRUSTWORTHINESS FROM FOUR INDUSTRY EXPERTS

### Trust Practice 1: Consider the Customer and the Customer Journey and Deliver "a More Human Internet"

In each of the interviews conducted, we heard again and again the importance of empathy — from understanding customer, user, and employee needs to reducing friction in the customer experience and in communicating how and why data is being collected. On the latter point, some interviewees emphasized that users are not comfortable providing certain types of personally identifiable information (PII), underscoring the need to move away from these data types toward others that have greater user acceptance and comfort.

A throughline in these conversations was that trustworthy organizations should deeply consider the needs of their customers and the way they will experience their products, evidencing empathic design throughout the experience of their product. In the pursuit of efficiency, it may be easier to design a single solution or single experience with the knowledge that, at the end of the day, users and customers will force themselves through that singular experience in order to access the resource or service they need. But as Shinesa Cambric, principal product manager at Microsoft, put it, "*The number 1 way to break trust is forgetting the human element. We live in a digital society, and there's so much that's online, so much of our lives that exist there, so much of our business and organizations that have to operate there. Lacking empathy influences the way you build products, so think about accessibility within your projects, think about the experience that humans on the other end are going to have. If they have a terrible experience, more than likely they're not going to trust coming back to your products again and again.*" Michael Woodson, a university lecturer with decades of experience as a cybersecurity executive, considers the trust that is gained when an organization responds to an inquiry or a complaint in a human, empathic way: "*Show what you're doing. Be transparent. Let people know that you're in it to win their business, and you appreciate their business by being tactical in addressing their needs. If there is a complaint, be visible about it. What did you do about it? Don't let it just go. For every complaint, there are six complaints coming. You share those stories because no company is*

*perfect. However, we're a company that believe in you, and we want to make sure that we're with you and for you. Without the customer, you can't have a bottom line, you can't have profit. You have to shift the mindset of the business to customer-centric solutions to gain trust.*"

In creating its identity solution, Persona understood that identity verification, at least at the outset, was first a matter of compliance, a mere regulatory requirement to safeguard businesses as well as protect customer data. But Persona also understood that for many organizations, identity verification is the door through which a customer begins their experience of a product or service offering. In designing its identity solution, Persona sought to balance the friction of identity verification with the customer's experience and data transparency, ultimately seeking to make identity verification as accessible as possible and thus promote "*a more human internet.*" In creating and refining its product, Persona explores the needs of different demographic groups in its design approach, empowering its designers and engineers to consider accessibility for multiple groups, as well as think through the changing life circumstances of a single customer, and what supporting a customer through these life stages would look like. Daniel Lee, product lead of Identity at Persona, said that in thinking about its identity solution, Persona realized "*Identity is not static in the sense of where the user lives, and identity management is not one size fits all. Every industry has different use cases, but even within the same healthcare and marketplace industry, depending on the customer you serve — if you're part of an underserved population, or you're an immigrant, or you're a teenager — your needs are different, and you should go through a different verification flow that's tailored to you.*"

Guillaume Bourcy, partner and CIO at GTC, shared the trust-gaining approach of neobanks and digital financial services companies that offer a "*progressive onboarding solution tailored to acquire, convert, and retain customers.*" As engagement with a company increases, so do the data requirements and security measures the user must take to access their services. During onboarding, the data requirements from the customer are minimal, but as the customer's journey progresses, only then are security measures and identity verification steps increased. This incremental approach allows neobanks to build trust and transparency with the customer over time, while also minimizing user burden at the beginning of the relationship, when less data and less stringent security measures are necessary.

## Trust Practice 2: Promote a Culture of Trust

Through each of these interviews and in IDC's larger research practice, it is clear that trust begins inside an organization. Employee trust engenders both customer trust and strong financial performance, as trust increases collaboration, creativity, and innovation, resulting in better product offerings and happier, more loyal, and more trusting customers. Promoting a culture of trust must pervade the ethos of the organization, starting with the organizational mission. Microsoft's Cambric cites the company's mission statement, "*Microsoft runs on trust,*" as "*something that all of us of here at Microsoft aspire to, and so the way we build products needs to align with that vision.*" And that commitment must begin with organizational leaders who are "*asked to model coaching care. If our goal is to run on trust and to empathize with our customers, we should be modeling that, and the rest of the organization picks up on that behavior.*"

Trusted leaders can further engender a culture of trustworthiness with their employees by modeling that coaching care and fostering an open environment where employees can be authentic. This model of care can ultimately lead to better products as a result of feedback and ideas that employees feel more empowered to provide. Woodson of Northeastern University and Sonesta International Hotels Corporation cautions against overreliance on wholly automated processes and emerging technologies,

which can lead employees to doubt their own instincts. He believes it is better to foster an environment in which employees are trusted to "*think outside the box. At the end of the day, when it comes to tools, trust your gut, don't assume that the tool is correct.*" As the number of companies moving to adopt AI into their infrastructure increases, especially with the integration of AI into security information and event managements (SIEMs) and security operations centers (SOCs) as a nonhuman counterpart to a human expert, so too can the number of alerts that analysts have to manage. Is the false positive really a false positive? Or is there a new signal being captured through the noise that hasn't been accounted for? Analysts and employees who trust their organization are more likely to call attention to these potential flags and dedicate their time to exploring the signals that might be detected in the noise, consequently improving the product or calling early attention to potential issues.

The importance of employee education was also emphasized. As Bourcy of GTC states, "*How do you ensure your employees are the right extension of your security measures and not the weak link? By having the right governance and learning mechanisms in place, your employees are at the forefront of helping to support building trust across your entire organization. You will set yourself up for success by establishing a culture of trust awareness among your employees to guard against gaps.*"

## Trust Practice 3: Build Communities, Alliances, or Trusted Ecosystems

Digital business, and the accompanying increase in the importance and complexity of trust, has given rise to the need for trusted communities, trust alliances, and trusted ecosystems of partners. These digital ecosystems comprises groups of interconnected partners that share insights and support each other's work in building and maintaining trust. The responsibility to manage the risks and vulnerabilities that accompany integration of multiple platforms no longer sits with implementing organizations alone but also with their platform partners and their respective service offerings. As ecosystems and the businesses they include undergo this evolution, organizational or brand partnerships and relationships can mean benefits and/or vulnerabilities for partners and their extended networks. If one organization falls victim to a security breach, its associated network of partner organizations may also suffer compromised data or resources. If an organization is revealed to be or is even accused of abusing customer data at the point of collection, storage, or use, the resulting loss of customer trust can ripple across that organization's entire network. These partnership vulnerabilities take on greater urgency as an increasing number of service providers are consolidating services or partnering with organizations with expertise in complementary services to increase the robustness of service offerings, improve customer experience, and secure a more competitive position in the marketplace.

Trustworthy organizations understand that, in this interconnected reality, we can do more for our customers more quickly if what is learned is shared. Microsoft's Cambric states: "*We're very much an organization that's empowering every organization on the planet to achieve more through empathy, through transparency, and through sharing of intelligence and working with partners. Security is a team sport, so we need to rely on our partners within other organizations and other industries, sharing insights and bringing the best for our customers.*" Lee of Persona adds: "*If you look at the largest new internet companies, almost all of their business models are built on peer-to-peer transactions. And these transactions can only occur if both parties trust who they're interacting with, and not just trust between users, but trust with the organization itself. So the peer-to-peer transaction means that organizations need to ensure that these transactions themselves are trustworthy — and it's not just a single transaction they need to worry about, but the culmination of lots of interactions to ensure that that relationship between the customer and their network is secure.*" Trustworthy organizations work to establish trust not only with their customers and with their employees but with their network of associated partner providers.

Woodson of Northeastern University likens the customer's experience with service providers to conducting an orchestra of empathy: "*at the end of the day, the music has to be in harmony. It has to be a trusted source to bring the sound forward, to get to the end result of a trusted and dedicated solution provided to customers.*"

## Trust Practice 4: Security and Privacy Are Key

The nature of security and privacy is changing. Where security and privacy controls were once considered a cost center, Lee of Persona points out, "*There are ways to frame security and privacy controls and shape them as a differentiator.*" Research on digital trust consistently shows that security and privacy are the top contributors to brand and organizational trust. Lee continues: "*Organizations need to show from a top-down perspective that security, privacy, and keeping up-to-date with all the latest security trends and privacy best practices is critical.*"

While organizations may tire of the costs associated with security and privacy controls, Bourcy of GTC points out: "*These days, anyone with materially important and valuable data is a target, from a fintech company to a digital-native company to a government agency. It means you are most likely going to be breached at one point in your organization's lifetime. However, it is less the 'what' and 'why' you have been breached than the how fast you detected and put remediation and communication plans in place that matters. Indeed, this is a critical step to show your customers that you take the issue seriously and will ensure it never happens again. It demonstrates your adaption to today's market risks and how you are always in preventive and reactive mode to ensure the security of your users and their data.*" Bourcy continues: "*I have seen CISOs and CTOs mentioning that news tools or infrastructure are a burden, and they do not have the budget for them.*" However, there is this famous quote in the cybersecurity industry: "*Before you are breached, it's too expensive. After, it's too late.*" I think that says it all. It's not about spending money on expensive and fancy tools, it's about spending the right amount of money in the right places: employee and customer education, infrastructure, and data privacy. Good processes and governance can take you a long way while saving your wallet.

Woodson states that it is the erosion of privacy and the failure of privacy controls that are most damaging to customer trust. "*If you have a breach due to lack of controls and you're not recalibrating your controls … controls are not a one-and-done scenario. It's an ongoing assessment. You need to understand what has changed in the business that we need to address. What hasn't changed in our process? Have our processes scaled to the level needed so we maintain trust? Assuring that privacy is implied, making sure that we're making them less vulnerable along the way, is an ongoing thing you have to keep up. That is the biggest issue, assuring customer privacy and ensuring that trust is at the core of everything that we do. Making sure to check our controls. Check them once, check them twice, check them continuously. Continuous monitoring is key.*"

Organizations that are working to engender and maintain trust have to balance security and privacy with other priorities that, at first glance, may appear to conflict with their journey to improve customer trust. Customers and users not only expect data security and privacy but also want to be able to easily access their resources without additional steps or friction. For Lee of Persona, this potential conflict is an opportunity. While "*folks think that there's too much friction, if you talk to anybody in fraud detection, there is such a thing as good friction*" or friction that, in the end, protects the user from fraudulent use of their accounts and information. Lee continues, "*This good friction could be really, really good friction if you're very transparent and you communicate what the context is with the end user. What is being performed? What data is being shared? How is the data being processed? Why is it necessary?*" Rather than being just a pain point for the end user, the friction that is introduced via privacy and

security processes becomes an opportunity to educate the end user and earn greater trust. That user now understands the purpose of this moment of friction, reframing the former pain point into a positive: proof of the user's security and privacy.

## Trust Practice 5: Adopt and Develop Trustworthy AI

Research has consistently shown that trust is the number 1 barrier or facilitator of AI adoption. Customers are more likely to trust AI if they indicate high accuracy and reliability, have in-hand detailed information about the population on which the algorithm or model was developed, and trust the reputation of the organization or team that developed the model (see *Will I Trust AI? Survey Research on the Impact of Accuracy, Population Data, and More on the Trustworthiness of AI Technologies Worldwide,* IDC #US51944224, March 2024). Bourcy, GTC, adds: "*Building trust is about transparency. It's critical. That's why businesses should provide clear explanations of how AI systems operate and the data they utilize to make decisions. Making AI explainable will create a trust bond with customers and clients.*" Organizations should also have the talent and resources necessary to closely monitor their adopted and developed AI products, ensuring that "*periodically somebody is assessing the AI or GenAI tool to make sure it's effective,*" according to Microsoft's Cambric.

The necessity of humans in the loop or humans on the loop in AI development and use was reiterated through each of the four interviews. Each expert wanted to ensure there were people maintaining oversight over all AI and automation tools. Woodson of Northeastern University opined: "*What I'm hoping people are doing is taking those false positives and dumping them into a data analysis tool. Let it run and see what is different from the baseline of our own environment. I want people to take a second look, really a kind of quality assurance, to make sure that what was identified is not a false positive. Explore the reasons for it, what kind of false positive was identified, and come up with an analysis on it. A checker of the checker.*" Woodson's observation continues, "*Are our models correct? Things change so rapidly that the model has to be agile enough to adjust to the conditions that are put before us. You do need a check of the checker.*" Woodson expanded this oversight to include evaluation of data and identifying whether the data is legitimately trustworthy using their own internal review of the data and its source.

The inevitability of change within the organization and the need to recalibrate were supported by other interviewees. Lee of Persona states: "*You need to make sure you have a representative data set that's somewhat stable, and that these are the dimensions that you know and care about. Whenever you create a new model, consider how it affects those known evaluation data sets. You're not going to know all those dimensions up front and you're going to be constantly learning, which is why you have to make that investment in your infrastructure and investment in the feedback cycle of learning and refinement.*" Similarly, Lee continues, "*You have to define what accuracy is, and every accuracy definition will have multiple levels. Accuracy is very misunderstood. Organizations need to define what is a true result and what is a false result. And the hardest part is defining that accuracy gray area, which then needs to be broken up into different subclassifications. You might get it all aligned with one organization and then you talk to another organization, and all those standard classifications are out the door.*" Accuracy means nothing in a vacuum.

While these considerations for trustworthy AI may seem daunting, all organizations can manage this complexity by clarifying their approach to AI governance both internally and externally and ensuring that AI adoption is strategically aligned with the organization's mission, goals, and brand identity. As Woodson states, "*You need an architect. You need a strategy. You need a methodology.*"

## Trust Practice 6: Know the Consequences of Breaking Trust

Each of these interviewees invested in and enabled trust because they were aware of and thoughtful about the consequences that came with breaking trust or not investing adequately in trust. Woodson of Northeastern University warns: "*You'll lose a customer, and you'll lose another customer. No longer will you have that cheerleader, that brand loyalty. It'll erode. Pay now or pay later. Yes, trust is an investment, but it's an investment in our sustainability. It's an investment in long-term trust versus short-term gain. We might gain something, but are those gains sustainable? The commitment is very strategic, and if you're in it to win it, all of us will win. Our customers will love us. Our brand will be sustainable, and it will grow. But when you lose your reputation, it's difficult to get it back.*"

For Lee of Persona, breaking trust comes with a number of consequences that ripple through the organization both now and into the future. He states that while "*the obvious consequence of breaking trust is customer churn, folks sometimes don't understand that if a trust-breaking event happens, you're not going to be able to work on anything else for weeks or months.*" Although data breaches and data loss can and will happen, adherence to best practices in security and privacy, such as a commitment to strong data protection, and constrained data collection to only that which is necessary to conduct business transactions go far in ensuring faster remediation and recovery from the adverse event. Lee continues: "*People also need to consider the impact on morale. If you're going to keep a high-caliber team, they don't want to be associated with trust-breaking brands. You're not going to attract high-quality talent and it's kind of a snowball effect.*" IDC research has consistently shown that high-trust organizations are perceived to have the most skilled cybersecurity staff and leadership. If that perception lags, the cybersecurity analysts that comprise their workforce will naturally seek new opportunities.

Trust-breaking events also result in greater regulatory intervention to reestablish trust in that sector and maintain economic activity. For Lee of Persona: "*There are a lot more longer-term effects that are sometimes not as obvious, such as regulatory actions and more processes in the long term. While regulations are not, in and of themselves, a bad thing, when cyberattacks spur them, it's not good for your brand.*" A recent example is the digital intrusion into a subsidiary of UnitedHealth Group (UHG). UHG CEO Andrew Witty estimated that in his congressional testimony the UHG/Change Healthcare cyberattack will impact approximately one-third of Americans, leading to questions about whether the healthcare company had grown so large that a cyberattack against it poses a risk to the health of all Americans (source: **healthitsecurity.com/news/change-healthcare-disconnects-system-amid-cyberattack**).

Breaking trust, even when the incident was not due to negligence, impacts not only customer trust but future partnership opportunities. The increasing complexity of the digital landscape has increased partnerships between service providers, as vendors see these partnerships as a way to strengthen offerings to their customers across a suite of expert services — but potential partners expect a commitment to security and privacy that is commensurate with their own. As Lee of Persona cautions: "*Trust-breaking events affect not only their interactions with the customers but with their partners as well. They can lose partnership deals to another brand that don't have that tarnished reputation. And then lastly, often the trust-breaking event is a breach in privacy or leaked in PII. And that's the scariest thing because it's not just impacting the brand or the end customers — the entire digital ecosystem is compromised. The best organizations help each other get better from a trust perspective.*"

## CHALLENGES AND OPPORTUNITIES AROUND DIGITAL TRUST

### Challenges

While trust is of increasing importance in our complex digital environment and confers multiple advantages to those who have high trust from their customers and communities, it is also becoming harder to secure. Social media and misinformation, global inequality, political unrest, and the COVID-19 pandemic have set the stage for further declines in trust in the coming years and decades.

The 2024 Edelman Trust Barometer indicates that France, the United States, Germany, Spain, the United Kingdom, Japan, and South Korea are now among the countries with the lowest levels of trust, and that the majority of survey respondents across the globe believe both that "*technology is changing too quickly in ways that are not good for people like me*" and that "*society is changing too quickly and not in ways that benefit people like me.*" The acceptance of these very technologies that are causing concern, such as artificial intelligence and innovations in green energy, hinges on whether the public can trust in the ethics and fairness of these and other emerging technologies.

Although IDC research shows that 33.5% of organizational leaders globally have found it challenging to improve perceived trust and trustworthiness because available resources are focused on other organizational priorities and 34.6% of global respondents state that the recessionary environment of 2023 led to the reprioritization of strategic initiatives including efforts to improve trust and trustworthiness (source: IDC's *Worldwide Future of Trust Survey,* September 2023), organizations (and governments) simply cannot afford to de-prioritize efforts to earn and maintain trust. The rapid adoption of AI, GenAI, and automation technologies also means that the likelihood of an adverse event — such as a data breach, deep fake fraud, or bias that causes material harm — will likely increase. But communities and organizations with high levels of trust are more resilient and better able to weather these crises — trust mitigates the damage that can accompany any one of these events.

### Opportunities

Ways to improve trust in emerging technologies, according to the 2024 Edelman Trust Barometer, include encouraging CEOs to speak publicly and transparently about what job skills are needed for the future, about the ethical use of technology, what impact automation will have on jobs, and what actions are or will be taken to safeguard livelihoods. Each organizational leader interviewed here reiterated the importance of human oversight over each emerging technology not only to increase trust but also to increase value and innovation. IDC research has shown that the *security and privacy of personally identifiable information are the top generative AI concerns of IT buyers and decision-makers* (see *Generative AI and Trust: Are Organizations Implementing Trusted GenAI?,* IDC #US51606724, January 2024), and that 75% of respondents worldwide are still in the testing and consideration phase of their organization's approach to generative AI (only 25% worldwide have invested significantly in generative AI with a set spending plan in place). Demonstrating a commitment to security and privacy and insistence on humans in the loop and humans on the loop at critical points of AI decision-making go far in reassuring the broader public that oversight and accountability are being taken seriously and are especially critical in this moment in time while organizations decide what their approach to AI and GenAI will be.

## CONCLUSION

Although securing customer trust is harder now than ever before, organizations that neglect strategic trust efforts risk losing customers and star employees. In Trust Practice 1, we consider the customer and the customer's experience to engender trust. This includes user experience design, user experience research, and user experience expert teams to guide product development in ways that reduce friction points in the customer's experience. In Trust Practice 2, we build and promote a culture of trust. Organizations should review their existing mission statements and internal policies and orient these documents around both employee and customer trust. Leaders are a critical aspect of organizational trust and trustworthiness and should be selected based on their ability to evidence and uphold trustworthiness. In Trust Practice 3, we build communities of trust or trusted ecosystems around shared best practices that enable customer trust. As digital infrastructures grow in complexity and in number, the data protection practices, security practices, and customer and employee retention practices of one organization can have a positive or deleterious impact on its partner organizations. Sharing best practices and learning opportunities can drive trust forward in the entire ecosystem to the benefit of all participants. In Trust Practice 4, we reiterate the central importance of a strong security and privacy posture. Breaches are the most visible and impactful breakers of trust, and while no organization is immune to breaches, all efforts should be made to secure data and protect privacy. In Trust Practice 5, in acknowledgement of the critical importance of discerning AI adoption, we focused on "*Trustworthy AI*" or AI adoption that critically evaluates what data is being used and how, is as transparent as possible, and is being supervised by humans at critical decision points. Finally, in Trust Practice 6, we become acquainted with the consequences of breaking trust. Because approaches to increasing trust vary by organization, by industry, and by leadership style, understanding which trust-breaking events are most significant in their consequences can help prioritize efforts in the right places.

### MESSAGE FROM THE SPONSOR

Telesign provides Continuous Trust to enterprises by connecting, protecting, and defending their digital identities. We verify over five billion unique phone numbers a month, representing half of the world's mobile users, and provide insights into the remaining billions. Our machine learning and data science deliver identity risk recommendations with speed, accuracy, and global reach. Telesign solutions provide fraud protection, secure communications, and enable the digital economy by helping companies and customers to engage with confidence. We convened the digital trust leaders interviewed in this white paper, and formed the Trust Alliance, because of our mission to make the digital world a more trustworthy place for everyone. The Trust Alliance will share insights and best practices that organizations can utilize to bolster fraud protections and maintain trust with their customers and others. Learn more about the Trust Alliance.

## About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology, IT benchmarking and sourcing, and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.).

## Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com

---