THE GHANA FINTECH REPORT

Q4 2023 EDITION

A Sustineri Attorneys' Quarterly Fintech Newsletter

Table Of Content

FORWARD

Richard Nunekpeku
The Editor

Dear Esteemed Readers,

We are thrilled to release the 4th Quarter edition of the Ghana Fintech Report, representing a continuation of our journey in exploring the dynamic landscape of enablers of the Financial Technology (Fintech) industry in Ghana. This edition marks a significant leap forward, focusing on the pervasive influence of Artificial Intelligence (AI) and Machine Learning (ML) in shaping innovative use cases within the Fintech space.

The regulatory spotlight as part of the "Inclusive Fintech" enablers is on the Cyber Security Authority (CSA). We delved into its pivotal role in safeguarding the integrity and resilience of the Fintech and Consumer Protection ecosystem as well as its newly introduced licensing regime for cybersecurity service providers.

Further, we provided comprehensive insights into trends and innovations driving change within the ecosystem by looking at the evolving deployments of Buy Now Pay Later (BNPL), Save Now Buy Later (SNBL) payment or credit options, and monetization opportunities with the advent of Web3. Notably, we explored the emergence of Compliance as a Service (CaaS) and other groundbreaking developments shaping the future of finance.

On the consumer insight front, we examined the crucial role of consent in promoting consumer centricity in the deployment of innovations and further looked at checklists for consumers in sharing their data with third parties.

In our industry spotlight, we showcased "eCampus", a Ghanaian company at the forefront of driving compliance and self-learning tools for companies and individuals exemplifying the transformative impact of Fintech in enhancing educational and regulatory compliance landscapes.

Additionally, we chronicled significant past events, including the maiden "eCEDI Hackathon" organized by the Bank of Ghana, an event that underscores the regulator's commitment to fostering innovation and collaboration.

We extend our sincere gratitude for your continued support, feedback, and engagement. Your involvement motivates us to persistently explore and document the evolving Fintech landscape through our quarterly Ghana Fintech Reports.

We trust that the insights and knowledge shared in this edition will prove invaluable in navigating the exciting and transformative developments within the Fintech industry in Ghana.

PUBLISHERS AND CONTRIBUTORS

ABOUT THE FIRM

We are Ghana's foremost Fintech and Start-up focused law firm, committed to providing differentiated legal services by leveraging our experience as proven entrepreneurs, business managers, and business lawyers which allows us to think and act like entrepreneurs, business owners, and managers we work with at all times.

As a team of young legal practitioners, SUSTINERI ATTORNEYS PRUC takes pride in acting with integrity, avoiding conflicts, and working with clients to design innovative legal solutions that meet their specific needs.

At SUSTINERI ATTORNEYS PRUC, we consider every client's brief as an opportunity to use our sound understanding of Ghana's business, commercial and legal environment, professional experience, and sound commercial knowledge to provide solutions that do not only address immediate legal needs but also anticipate future challenges and opportunities.

Our pride as the foremost Fintech and Start-up focused law firm stems not only from our understanding of the potentials of emerging technologies and our belief in the ideas of many young people, but also from the difference our network of resources and experience can make when working closely with founders and entrepreneurs. To this end, we operate a 24-hour policy urging our clients to reach out to us at any time and on any issue.

We strive for excellence, ensuring that our solutions provide sustainable paths for our clients' businesses by adopting a common-sense and practical approach in our value-added legal service delivery – and employing our problem-solving skills.

Our goal is to help businesses to become commercially sound and viable, as well as regulatory compliant, by engaging in legal and beneficial transactions to promote their business competitiveness for sustained operations and investments.

And as our name implies, our priority is to always leverage legal means to promote the sustainability (long-term viability) of our clients' businesses.

We are different, and the preferred partner for growth.

SUSTINERI
ATTORNEYS

CONTRIBUTORS

Richard Nunekpeku,
Managing Partner
richard@sustineriattorneys.com

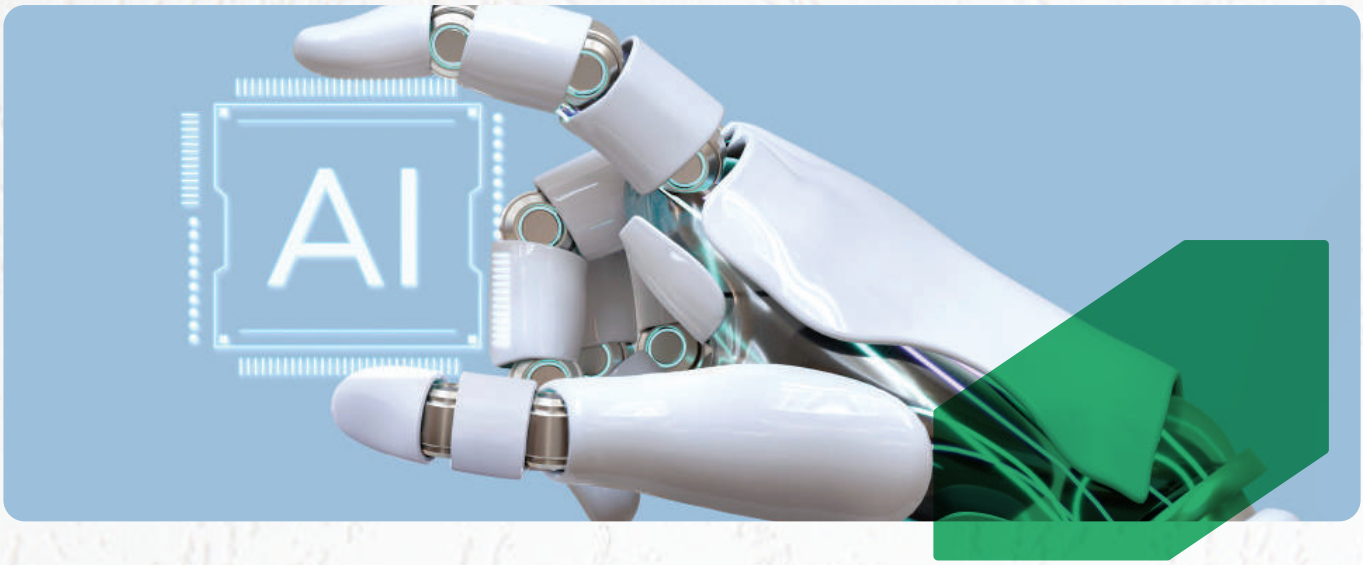
Cecilia Antwi Kyem,
Associate
cecilia@sustineriattorneys.com

Adwoa Birago Nyantakyi,
Associate
birago@sustineriattorneys.com

Harold Kwabena Fearon,
Associate
harold@sustineriattorneys.com

INNOVATIONS RESHAPING FINANCIAL SERVICES

03



ARTIFICIAL INTELLIGENCE (AI) AND MACHINE LEARNING (ML)

Two emerging technologies with the potential to shape and reshape the offering of financial services globally are Artificial Intelligence (AI) and Machine Learning (ML). Currently, the transformative influences of these technologies are being experienced and deployed at an increasing rate across all industries and financial service is not an exception.

The opportunity to maximize the unique benefits of AI and ML to drive efficiency, accuracy, and innovations within the financial sector is real due to the abilities of these technologies to analyze vast datasets, produce meaningful insights, and make informed decisions with a click of a button is becoming the mainstay of financial services offerings today across the world.

While the revolution is just beginning, we have come to understand Artificial Intelligence (AI) as the innovative simulation of human intelligence in machines enabling computers and machines to perform tasks that typically require human intelligence such as visual perception, speech recognition, and decision-making as its full potential is not fully realized.

Machine Learning (ML) on the other hand has proven to be the development of algorithms that can learn from and make predictions or decisions based on vast datasets and seek continuous improvements through continuous learning over time.

It is the combined and tailored use of these technologies that is making analysts predict their transformative influences on financial services in ways some of which are discussed below.

SOME UNIQUE CHARACTERISTICS OF AI AND ML

Technologies in various forms are being used and available within the financial sector industry. However, the unique ability of AI and ML to achieve adaptability, pattern recognition, and automation at an incredible speed is proven to be game-changing.

A. Adaptability: AI and ML possess the ability to adapt and evolve with improved performance with time, making their use in financial service decision-making dynamic and in tune with the evolving financial sector landscape.

B. Pattern Recognition: Particularly, ML has proven useful in pattern recognition enabling the ability to identify and learn complex patterns from large volumes of historical datasets. This will be paramount for the identification of trends, patterns, and potential risks in financial datasets and help address concerns such as fraud, etc.

C. Automation: AI enables automation at greater efficiency and speed leveraging ML algorithms. This helps in automated decision-making based on identified data insights and holds the promise to streamline processes, reduce manual labor, and improve overall financial sector efficiency.

PRACTICAL USE CASES OF AI AND ML IN THE FINANCIAL SECTOR

It is practically impossible to make an exhaustive list of all the potential use cases of AI and ML in financial service delivery. However, some key use cases stand to benefit immensely from the deployment of AI and ML going forward.

A. Credit Scoring: With the increasing development of deferred payment options such as Buy Now Pay Later (BNPL) and other credit facilities, ML algorithms have the potential to improve the underlying credit scoring models by incorporating a broader range of data points and making a more accurate assessment of individual's creditworthiness.

B. Fraud Detection: Fraud and its related concerns continue to be the dark spot in the excitement around the potential of technologies generally to change our lives. With AI-enabled systems, the use of pattern recognition methods could be leveraged to identify and prevent fraudulent activities in real-time proving to be a proactive approach to enhancing online security for financial transactions.

C. Customer Service: Some customer service concerns have become mundane and repetitive. The opportunity to address some of the concerns through the use of Frequently Asked Questions (FAQs) has become limited as same has been without a human touch. Chatbots and virtual assistants powered by AI will enable new customer interactions through real-time instant responses and inquiries in a humanly possible manner while facilitating seamless communication between financial service providers and consumers.

D. Algorithmic Trading: Investments will continue to be a significant part of the financial sector and ML algorithms can analyze market trends, historical data, etc. to make informed trading decisions and optimize investment options.

E. Personalized Financial Advice: With advances in technologies, personalized service provision is taking center stage. AI-enabled tools can analyze individual preferences, patterns, and financial behaviors to design and offer personalized advice, improving the quality of financial services.

POTENTIAL RISKS ASSOCIATED WITH AI AND ML IN FINANCE SERVICE OFFERING

The positive uses and impacts of AI and ML on the financial sector could be limited by some of the risks discussed below:

A. Data Privacy and Security: This concern is common to all emerging technologies compelling robust data protection measures to prevent privacy and security breaches. These risks could be mitigated through the implementation of data governance practices that leverage the benefits of encryption, access controls, data anonymization, etc. to safeguard

Currently, the transformative influences of these technologies are being experienced and deployed at an increasing rate across all industries and financial service is not an exception.

the confidentiality of financial records.

B. Bias and Fairness: Largely, the algorithms underlying AI and ML systems may inherit biases present in their training of data and how assessments are made which may lead to discriminatory outcomes. To deal with this, ethical considerations must be incorporated into the design, development, and deployment of AI and ML systems to ensure fairness, transparency, and accountability in algorithmic decision-making.

C. Regulatory Compliance: Globally, regulators are responding to the emerging concerns and risks of AI and ML. New regulations have been enacted and several ones are under consideration to manage, supervise, and regulate the use of AI and ML systems across the financial sector. Navigating the evolving regulatory landscape and ensuring compliance with legal requirements pose challenges for the deployment of AI and ML systems in the finance sector. Continuous monitoring and auditing of AI systems to identify and rectify biases, security vulnerabilities, compliance, and performance optimization will offer comfort for regulators and restrain them from stricter regulations.

D. Understanding AI and ML models: Generally, technology is complex and inhibits ordinary understanding. The complexity of AI and ML models may hinder the understanding of their use cases and the explanation of the reasons behind their decision outcomes. Striving for transparency in AI decision-making processes and developing models that are easily understood and explainable to stakeholders, regulators and consumers will enhance their uses in the financial sector going forward.

CONCLUSION

The use of technology in any form has become the mainstay of the financial sector globally. The opportunity to integrate AI and ML into financial service offerings holds immense promise for innovation and efficiency. While the pursuit of this is encouraged, innovators, regulators, and end users must ensure balanced and ethical considerations underpin any design, development, and deployment of AI and ML-enabled financial services or tools.

INCLUSIVE FINANCIAL TECHNOLOGY (FINTECH)

04

A SPOTLIGHT ON THE CYBER SECURITY AUTHORITY (CSA)

Cybercrime has become an increasingly pervasive threat in our digitally unified world. With the rise of the internet and digital technologies, criminals have also upgraded their game and equally exploring new avenues to exploit the vulnerabilities to carry out illegal activities. From hacking and identity theft to fraud and malware distribution, cybercriminals employ various tactics to compromise digital systems, security, and privacy of individuals, companies, and even governments. These actions can have severe consequences, including financial loss, data breaches, and damage to one's reputation and privacy.

Ghana, like many other countries, faces its share of cybercrime challenges. It is for this reason that the government and law enforcement agencies are actively working to address this issue through the implementation of cybersecurity measures and regulations.

The implementation of the Electronic Transactions Act, 2008 (Act 772), the Cybersecurity Act, 2020 (Act 1038) and other interrelated legislations serve as the legal backing in Ghana's quest for combating cybercrimes. In addition, the battle against cybercrime will require the deployment of technological tools, legislative initiatives, cybersecurity awareness campaigns, and the expertise of cybersecurity authorities to achieve any desired results.

By understanding the nature of cybercrimes, the mechanisms in place to mitigate them, and the expertise of cybersecurity authorities, individuals and organizations can better protect themselves against the ever-evolving landscape of cyber threats.

In this write-up, we will explore the licensing regime, and policies as well as efforts being made to combat these cybercrimes and highlight the importance of cybersecurity in safeguarding our digital lives.

CYBERSECURITY IN GHANA

In this digital age where technology lies at the heart of our daily lives, cybersecurity takes center stage as a shield against cybercrimes. Cybersecurity is the means of warding off cyberattacks and safeguarding our precious data from the clutches of unauthorized access. It details a wide range of protective measures and strategies aimed at ensuring the confidentiality, integrity, and availability of digital resources to combat cybercrimes.

To effectively protect against cyber threats, cybersecurity professionals employ various proactive measures. These include the implementation of firewall systems to control and monitor network traffic, encryption techniques to secure sensitive information, and intrusion detection systems to identify and respond to potential breaches promptly. Regular security updates also address vulnerabilities and help stay ahead of emerging threats.

In Ghana, the Cyber Security Authority (CSA) assumes an overseeing and coordinating role across the country. It acts as a central authority responsible for implementing the provisions outlined in the Cybersecurity Act, 2020 (Act 1038). By enforcing regulations and promoting cybersecurity best practices, the authority fortifies the nation's digital infrastructure and ensures a secure online environment for individuals, businesses, and government entities.

Cybersecurity authorities, whether individuals or organizations, are recognized as esteemed leaders in the field of cybersecurity. Equipped with extensive knowledge and expertise, they possess the necessary skills to defend computer networks, systems, and data against online attacks. These experts often have backgrounds in information technology, computer science, or related disciplines. They may also hold credentials such as the Certified Ethical Hacker (CEH) or Certified Information Systems Security Professional (CISSP), demonstrating their competence and adherence to industry standards.

Given their deep understanding of evolving threats and security best practices, cybersecurity authorities are sought after for their advice and insights on how to effectively defend against cyberattacks. Their continuous engagement with the latest technologies, emerging threats, and security protocols enables them to provide valuable guidance and assistance to individuals, organizations, and government bodies seeking to bolster their cybersecurity defenses.

Cybercrime has become an increasingly pervasive threat in our digitally unified world.

THE CYBERSECURITY ACT AND THE CYBER SECURITY AUTHORITY (CSA)

In 2020, Ghana's Cybersecurity Act, sometimes referred to as the Cybersecurity Act of Ghana, was passed into law to establish a framework for safeguarding Ghana's cyberspace. To effectively implement these goals, the act established the Cyber Security Authority (CSA) as the regulatory body responsible for overseeing and coordinating cybersecurity initiatives throughout the country. To defend against cyberattacks, the CSA is entrusted with creating and executing national cybersecurity policies, strategies, and guidelines. In addition, the act mandates the establishment of the National Computer Emergency Response Team (CERT) to actively monitor and respond to cybersecurity incidents within Ghana. This dedicated team will be detecting, analyzing, and mitigating potential cyber threats, ensuring a swift and effective response to any cybersecurity events. The CERT is in charge of supplying incident response and early warning systems to lessen cyber threats and vulnerabilities.

In addition, the Cybersecurity Act highlights how crucial it is for the public and private sectors to work together to improve cybersecurity resilience. To effectively address cybersecurity concerns, it promotes information sharing, capacity building, and cooperation. All things considered, Ghana's Cybersecurity Act is evidence of the government's dedication to tackling cybersecurity issues and safeguarding the nation's digital infrastructure. Ghana wants to improve its cybersecurity posture and lessen the dangers brought on by cyberattacks by putting in place a legal framework and regulatory body.

The Cyber Security Authority (CSA) is established as a dedicated body responsible for protecting digital systems, networks, and data from cyber threats. The Authority is empowered to acquire and manage property, enter into contracts, and perform other necessary transactions.

The objectives of the Authority include regulating cybersecurity activities, preventing and responding to cyber threats and incidents, overseeing critical information infrastructure, promoting the development of cybersecurity, fostering collaboration between public institutions and the private sector, raising awareness about cybersecurity, and collaborating with international agencies to enhance national cybersecurity.

To achieve its objectives, the Authority is entrusted with various functions. These functions include providing advice to the government and public institutions on cybersecurity matters, promoting the security of computer systems, monitoring cybersecurity threats, establishing standards and codes of practice, certifying cybersecurity products and services, responding to cybersecurity incidents, identifying and regulating critical information infrastructure, supporting law enforcement agencies, promoting online protection for children, issuing licenses for cybersecurity services, supporting research and development, disseminating cybersecurity information, submitting reports on the state of cybersecurity, educating the public, building capacity in cybersecurity, collaborating with law enforcement agencies, maintaining a national register of risks and licensed entities, and performing other functions necessary to fulfill its objectives.

The Cyber Security Authority is governed by a Board composed

In 2020, Ghana's Cybersecurity Act, sometimes referred to as the Cybersecurity Act of Ghana, was passed into law to establish a framework for safeguarding Ghana's cyberspace.

of relevant ministers, the Director-General of the Authority, representatives from the industry, and other appointed members. The Board, led by the chairperson (usually the Minister), is responsible for overseeing the operations and strategic direction of the Authority in accordance with applicable laws and regulations.

THE LICENSING OF CYBERSECURITY SERVICE PROVIDERS

Under the Cybersecurity Act 2020 (Act 1038), it is a requirement for individuals to obtain a license from the Cyber Security Authority in order to provide cybersecurity services.

To apply for a license, an individual seeking to provide cybersecurity services must submit a written application to the Authority. The application should be in the prescribed form and accompanied by the necessary supporting documentation and fees determined by the Authority. Upon receipt of the application, the Authority is obligated to acknowledge its receipt within fourteen (14) days.

If the Authority is satisfied that the applicant meets the requirements for a license and granting the license is not against the public interest, it may proceed to grant same to the applicant. The decision regarding the application must be communicated to the applicant within thirty (30) days. Once granted, the license is subject to specific terms and conditions.

A misuse of a license will result in an administrative penalty.

A license granted under this Act is valid for a period of two (2) years. To continue operating as a cybersecurity service provider, the licensee must apply for a renewal of the license at least one (1) month before its expiration.

In March 2023, the Cyber Security Authority (CSA) introduced new licensing categories for providing cybersecurity services in the Ghanaian market. This, which became effective in September 2023, established three distinct categories, each with its own set of requirements.

1. Licensing of Cybersecurity Service Providers

This category encompasses Cybersecurity Service Providers (CSPs), defined by the CSA as individuals or entities licensed to deliver cybersecurity services. Some of the cybersecurity services include Vulnerability Assessment and Penetration Testing (VAPT), Digital Forensics Services (DFS), Managed Cybersecurity Services (MCS), Cybersecurity Governance, Risk and Compliance (GRC), and Cybersecurity Training (CT).

Foreign CSPs on the other hand are required to register as a business with the Registrar-General's Department. Following this registration, the licensing requirements for both foreign and domestic CSPs are the same. However, if a foreign CSP is unable to meet this

requirement or does not intend to establish operations in Ghana, it must provide evidence of a partnership with a Ghanaian-owned CSP that holds a valid license. The specific legal and financial terms constituting a partnership in this context are yet to be formally defined by the Cybersecurity Authority.

To obtain this license, CSPs must:
a. Complete an online application.
b. Provide a detailed description of the services offered and the technical processes involved.
c. Verify the accreditation status of the cybersecurity professionals employed.
d. Confirm their business registration.
e. Confirm their tax registration and clearance, and
f. Demonstrate their willingness to provide insurance coverage for potential losses.

Upon receiving a complete application, the CSA will notify the applicants of its decision to issue a license within 30 days. The issued licenses are valid for a duration of 2 years.

2. Accreditation of Cybersecurity Establishments

This category applies to new and existing Cybersecurity Establishments, which the CSA defines as organizations formed to investigate cybercrimes and mitigate cybersecurity incidents. For the purposes of the licensing regime, CEs refers to Digital Forensic Laboratories and Managed Cybersecurity Service Facilities. However, if a CE intends to perform other functions that are not covered by this definition, the CE license may still apply at the CSA's discretion.

Due to its nascent nature, there are no specifically outlined rules applying to foreign operators in this category.

The CSA therefore wields power to notify applicants of its decision to accredit within 30 days of receipt of a complete application. Licenses are valid for 2 years and can be renewed.

3. Accreditation of Cybersecurity Professionals

This category of licensing is for individual cybersecurity professionals (CPs). The CSA defines them as persons accredited under the Cybersecurity Act to "perform a cybersecurity-related professional function." Local (Ghanaian) applicants can gain this accreditation/obtain this license by:

a. Completing an online form.
b. Providing national identification.
c. Submitting a resume that demonstrates cybersecurity expertise.
d. Submitting a reference, and
e. Completing a background check.

Non-Ghanaian individuals must:

a. Complete the same online form.
b. Submit a background check from a "competent authority" in the country of origin or the country of residence for the previous five years.
c. Submit the biodata page of a valid travel document (for example, a passport).
d. Submit evidence of a job or consultancy offer with a Ghanaian-based entity for a cybersecurity job.
e. Submit academic and professional qualifications and certifications.
f. Submit proof of insurance coverage, if applicable.
g. Submit proof of membership of in professional cybersecurity body, and
h. Submit any recommenda-

To apply for a license, an individual seeking to provide cybersecurity services must submit a written application to the Authority.

tions from previous employers. The CSA will notify applicants of its approval within 30 days of receipt of a complete application. This Cybersecurity Professional License is valid for 2 years and can be renewed.

SUSPENSION AND REVOCATION OF LICENSE

The Cyber Security Authority has the power to suspend a license for a maximum period of six (6) months if the licensee fails to renew the license or breaches any specified conditions. Before the suspension, the Authority must provide the licensee with a written notice, stating the grounds for the intended suspension. The licensee is given the opportunity to respond and rectify the breach within the specified time. Failure of which the cybersecurity service provider will be notified of the suspension.

In other circumstances, the Authority may completely revoke a license. These circumstances include obtaining the license through fraud or misrepresentation, cessation of the licensed business, conviction of an offense, bankruptcy, failure to meet the requirements, or if it is not in the public interest for the licensee to continue operating. The revocation process follows similar procedures as the suspension. The revocation of a license will be published in the Gazette.

INITIATIVES TO COMBAT CYBERCRIMES IN GHANA

Ghana has launched several programs and policies in addition to the Cybersecurity Act to tackle cybercrime including the enactment of the Electronic Transactions Act, providing for offenses related to cybercrime, including unauthorized access to computer systems and data, etc. Additionally, the Electronic Transactions Act grants legal recognition for electronic transactions.

There has also been introduced the National Cyber Security Policy and Strategy, which provides a thorough framework for tackling cybersecurity issues. To effectively tackle cyber threats, the policy focuses on raising cybersecurity awareness, developing capacity, and bolstering stakeholder collaboration.

The Cyber Security Authority has the power to suspend a license for a maximum period of six (6) months if the licensee fails to renew the license or breaches any specified conditions.

Further, Ghana has created the Cybercrime Unit under the Ghana Police Service's Criminal Investigation Department (CID) to investigate and prosecute offenses relating to the illegal use of the internet. To effectively combat cybercrime, the unit has been collaborating closely with other law enforcement organizations and foreign partners in its bid to curb the increasing menace of interest fraud.

Also, to create a workforce with the necessary skills to combat cyber threats, the government has invested in cybersecurity education and training initiatives. The National Cyber Security Awareness Month and cybersecurity workshops are two examples of initiatives that are aimed at educating the general public about cyber risks and best practices for staying safe online.

In general, these initiatives among others are testaments of Ghana's dedication to defending its digital infrastructure and shielding its people from online dangers.

EMERGING PRODUCTS AND BUSINESS MODELS

05

COMPLIANCE-AS-A-SERVICE

The ever-changing regulatory environment has grown more complex and demanding for companies to navigate and comply with non-compliance bringing about severe consequences, including fines and reputational damage.

In response, the Compliance-as-a-Service (CaaS) model has surfaced as a beneficial solution for organizations aiming to uphold regulatory compliance and reduce risk. As an increasing number of organizations adopt CaaS solutions to handle their compliance needs, understanding the intricacies of this business model has become essential for maintaining a strong compliance posture and mitigating risks in a modern regulatory environment.

"Compliance-as-a-Service (CaaS)" is a model that involves service providers giving client organizations the means to access managed services, tools, and expertise to assist them in maintaining compliance standards and lowering risks. It combines technology, expertise, and services, providing a tailored approach to ensure businesses meet regulatory standards.

It includes everything ranging from evaluating risks to establishing policies and ensuring businesses operate within legal parameters offering a cost-effective, scalable solution to regulatory compliance, making it a key tool for businesses to navigate the ever-growing regulatory compliance landscape with confidence.

HOW COMPLIANCE-AS-A-SERVICE WORKS

Today, as businesses are grappling with the ever-expanding regulatory landscape, Compliance-as-a-Service (CaaS) is emerging as a lifeline, streamlining regulatory adherence, and helping companies meet their compliance responsibilities through the use of technology, expertise, and an understanding of the local regulatory regime.

Despite the substantial responsibilities involved, CaaS serves as a valuable and controllable service. The system is typically implemented within a private cloud, ensuring that data remains under the secure control of a single entity and transactions are audited for enhanced security.

Compliance-as-a-Service, a component of Business Process as a Service (BPaaS), integrates software, shared services, and proven frameworks to guide enterprises through the framework of regulatory adherence.

CaaS are designed based on the unique compliance requirements of a business, considering industry-specific compliance demands and regulations. This enables CaaS providers to tailor a compliance program that is aligned with the goals and regulatory obligations of a business and updated in response to evolving regulations.

As regulatory dynamics persistently transform, the demand for CaaS is poised to grow, presenting businesses with a practical solution to navigating the regulatory compliance hurdles.

KEY COMPONENTS IN A COMPLIANCE-AS-A-SERVICE OFFERING

In every Compliance-as-a-Service (CaaS) system, there are several key components, each playing a crucial role in upholding regulatory compliance:

1. **Compliance Management:** This involves the development and execution of a comprehensive compliance program tailored to meet the specific regulatory requirements of a business.

2. **Risk Assessment:** CaaS providers regularly conduct risk assessments to pinpoint potential compliance risks and devise effective mitigation strategies.

3. **Audit Management:** This encompasses the oversight of both internal and external audits to ensure steadfast adherence to regulatory standards.

4. **Policy Management:** CaaS providers extend support in formulating, implementing, and overseeing compliance policies.

Together, these components form a cohesive strategy for regulatory compliance, mitigating the risk of non-compliance and allowing businesses to channel their efforts toward core operations.

Other major services that are additionally provided in a CaaS include the following:

a. Database access control
b. Separation of duties
c. Application management
d. Change control
e. Data discovery
f. Data masking
g. Incident response
h. Real-time data protection
i. Repair of vulnerabilities
j. Personnel training
k. Service configuration

ADVANTAGES OF COMPLIANCE-AS-A-SERVICE

CaaS business models offer several benefits some of which include:

CaaS are designed based on the unique compliance requirements of a business, considering industry-specific compliance demands and regulations

1. **Reduced Costs:** CaaS providers aid organizations in reducing costs by diminishing the necessity for internal compliance teams and resources. Outsourcing compliance duties to a specialized provider is notably more budget-friendly, particularly for small to medium-sized enterprises. This move eliminates the need for extensive internal research and implementation of compliance processes, freeing up time and resources for core business activities while experts handle compliance management.

2. **Enhanced Security:** Many CaaS providers extend cybersecurity services, fortifying an organization's defense systems and safeguarding sensitive data.

3. **Scaling:** With organizational growth or market expansions, CaaS providers assist in scaling compliance efforts accordingly. This ensures consistent compliance across all business operations, regardless of the scale or complexity.

4. **Specialized Expertise:**

CaaS providers typically employ seasoned compliance specialists who stay updated with the latest regulations and best practices. Organizations benefit from the provider's expert knowledge to maintain compliance even in the face of changing regulations.

5. **Risk Mitigation:** CaaS providers play a key role in identifying and rectifying possible compliance gaps, and curbing the risk of fines, legal disputes, or damage to reputation due to non-compliance. This aids businesses in managing their risk exposure effectively.

6. **Tailored Support:** CaaS providers can customize their services to meet each organization's individual needs, ensuring they receive the right level of assistance and guidance concerning their specific compliance requirements.

As regulatory dynamics persistently transform, the demand for CaaS is poised to grow, presenting businesses with a practical solution to navigating the regulatory compliance hurdles.

LIMITATIONS OF COMPLIANCE-AS-A-SERVICE

While Compliance-as-a-Service (CaaS) offers significant advantages, there are several drawbacks and obstacles organizations need to take into account when considering this model:

1. **Overdependence on Providers:** Organizations using CaaS may become overly dependent on their chosen service provider. Downtime or issues with the provider can directly impact the organization's compliance status and overall functioning. Additionally, transitioning between providers may require careful planning and effort.

2. **Integration Hurdles:** Integrating solutions from CaaS providers could demand additional time and resources, especially when aligning with the organization's existing systems and tools.

3. **Variability in Provider Quality:** The effectiveness of a CaaS solution hinges on the expertise and quality of the chosen provider. Not all CaaS providers offer the same levels of support and guidance.

4. **Regulatory Changes:** CaaS providers must constantly stay updated with evolving regulations. Ensuring that providers keep pace with new and changing regulations is crucial to avoid compliance issues for the organization.

Organizations should conduct in-depth research when selecting a CaaS provider to overcome these challenges. It's essential to choose a trustworthy, experienced, and dependable partner to meet the compliance requirements effectively.

BUSINESSES THAT COULD USE CaaS

Numerous businesses stand to gain from adopting a Compliance-as-a-Service (CaaS) model, especially those facing regulatory demands or operating within sectors where compliance holds utmost significance.

Any organization that contends with regulatory requirements or functions in a regulated industry ought to explore the benefits of the CaaS model. However, it is crucial for each organization to meticulously evaluate its distinct compliance needs and confirm that a chosen CaaS provider can effectively meet those specific requirements.

Various businesses are well-suited for the CaaS model, including:

1. **Financial Institutions:** Entities such as banks, investment firms, and credit unions are heavily governed by regulations like Anti-Money Laundering (AML) rules and Know Your Customer (KYC) requirements. CaaS is invaluable in helping these entities maintain compliance while relieving internal resource pressures.

It's essential to choose a trustworthy, experienced, and dependable partner to meet the compliance requirements effectively.

2. Healthcare Organizations: Hospitals, clinics, and other healthcare providers must comply with stringent regulations. CaaS providers offer crucial support in safeguarding patient data and ensuring adherence to privacy and security standards.

3. eCommerce and Retail Businesses: Entities processing payments, storing customer data, or functioning online must comply with data privacy and protection regulatory demands. CaaS providers help these businesses ensure compliance with payment processing and data protection standards.

4. Data-Centric IT Companies: Tech firms managing sensitive customer data or operating in regulated industries must comply with data protection and privacy regulations, and other regional and industry-specific norms. CaaS services can assist these entities in managing their compliance requirements.

5. Energy and Utility Entities: Organizations in the energy sector must adhere to environmental, health and safety, and cybersecurity regulations. CaaS providers offer essential assistance in handling these regulatory obligations.

6. Startups and Small Businesses: Smaller businesses and firms might require additional resources or expertise to manage compliance internally. CaaS presents an affordable solution for maintaining compliance while enabling them to concentrate on business expansion.

CONCLUSION

Compliance-as-a-Service (CaaS) has emerged as an essential solution for businesses maneuvering through the evolving regulatory environment. Functioning as a cloud-based approach to regulatory adherence, CaaS brings forth advantages like cost efficiency, scalability, and access to expert guidance. According to a PwC analysis, businesses leveraging CaaS witnessed a reduction in compliance risk by as much as 60%.

The significance of CaaS is projected to amplify, propelled by anticipated market trends and the continuously evolving regulatory sphere. Businesses must regard CaaS as a pivotal element in their compliance strategy. It offers a means for companies to meet existing compliance prerequisites more efficiently and prepares them for the future by providing a versatile, adaptable solution that can accommodate evolving regulations.

In summary, CaaS serves as a substantial leap in how businesses handle regulatory compliance. By embracing CaaS, companies can effectively navigate today's ever-growing regulatory demands and brace themselves for the challenges of tomorrow.

HEALTH-TECH REMITTANCE - COMESO

COMESO, an innovative digital platform developed by Glory-HealthCare, is reshaping healthcare accessibility by promoting financial inclusion. The platform is driven by a mission to save lives through enhanced access to healthcare services.

COMESO, which is an acronym for "COmmitment for a MEdical SOlution", is specifically designed to tackle the issue of providing medical care for people who live far away from their families. It ensures the secure, accessible, and transparent facilitation of health-related financial transactions.

In regions where medical assistance and insurance can be prohibitively expensive, healthcare payments are crucial for many families. COMESO addresses this by allowing senders to guarantee that the financial support sent for health-related reasons is utilized for prescribed medicines and healthcare expenses. This is achieved by earmarking credits specifically for medical purposes, ensuring that the financial aid sent abroad is dedicated exclusively to the healthcare needs of the recipients.

Employing cutting-edge technology, COMESO prioritizes the security and protection of all transactions. Its user-friendly interface facilitates easy access and management of medical funding for loved ones residing in different geographical locations. Transparency is a hallmark feature of the platform, offering users a clear overview of their healthcare-related expenses.

The utilization of COMESO is a straightforward process. Typically, users register and add funds to their accounts, subsequently transferring health credits to their intended recipients. These credits can then be utilized to settle medical service bills at authorized healthcare facilities.

Beyond being a mere platform, COMESO serves as a vital link connecting people across borders. It ensures that funds designated for healthcare purposes are secure and directed toward their intended use. For families in Germany and the Ghanaian diaspora, COMESO stands as an innovation in remittance services in the health sector.

COMESO therefore represents a transformative solution within the healthcare sector, fostering access to healthcare through the prism of financial inclusion. It stands as a testament to GloryHealthCare's unwavering commitment to prioritizing health for all, irrespective of their geographical location.

TRENDS AND INNOVATION

06

BUY NOW PAY LATER (BNPL) AND SAVE NOW BUY LATER (SNBL)

BUY NOW PAY LATER

BNPL

Buy Now Pay Later is a consumer financing model that enables individuals to make purchases and defer payments to a later date. Unlike traditional credit cards or loans, BNPL services often do not involve interest charges if the payment is made within a specified period, typically ranging from a few weeks to a few months. This flexibility has resonated with consumers who seek more control over their cash flow without the burden of long-term debt. At its core, BNPL is a testament to the evolution of consumer-centric finance. This model enables users to make immediate purchases and defer the payment over a predetermined period, often in the form of interest-free installment plans.

Buy now, pay later (BNPL) is a widely adopted payment method, especially among younger shoppers who value convenience, flexibility, and affordability. The global BNPL market was projected to reach $100 billion in transaction value in 2023, according to Juniper Research. With the ability to customize payment schedules, choose interest-free installments, and seamlessly integrate with various shopping platforms, consumers experience a newfound sense of financial empowerment.

However, this flexibility has critics concerned about the potential for BNPL to encourage impulsive spending habits and accumulate debt. Regulatory bodies are closely examining issues related to consumer protection, data security, and the fairness of lending practices.

HOW THE BNPL MODEL WORKS

Selecting BNPL as a payment option - when purchasing from a retailer that supports BNPL, customers can opt for BNPL as a payment method. The BNPL provider settles the full amount, and the customer reimburses them, usually through interest-free installments over a brief fixed payment period.

Making a Down Payment - If approved, customers make a small down payment, such as 25% of the overall purchase amount. They then pay off the remaining amount in a series of interest-free installments, usually over a few weeks or months.

Automatic Deductions - payments can be automatically deducted from a debit card, bank account, or credit card. Some BNPL providers may enforce autopay.

No Interest Charges - BNPL apps usually do not charge interest or fees, and they have a

fixed repayment schedule. unlike credit cards, BNPL typically does not charge interest or fees, and it adheres to a fixed repayment schedule.

Credit Scoring - BNPL services rely on smart algorithms to evaluate risk, enabling quick and smooth approval processes. When an individual applies for BNPL credit, most services usually perform soft credit checks, which help to determine the individual's creditworthiness. BNPL services often make instant approval decisions based on minimal credit checks or sometimes without any credit checks at all. However, over time, BNPL services will provide credit agencies with information on payments and missed payments. Hence, if payments are overdue or not made at all, an individual's credit score can be affected.

SAVE NOW BUY LATER (SNBL)

Save Now Buy Later (SNBL) combines saving, spending, and investing in a single platform. It allows consumers to set aside money regularly for specific purchases while earning rewards such as discounts, cashbacks, market returns, and brand co-investments.

SNBL aims to leverage the existing trend of saving for purchases instead of using credit. SNBL platforms partner with merchants to offer rewards when customers reach their savings goals, promoting financial responsibility. SNBL potentially benefits consumers, merchants, and brands by fostering loyalty, reducing cart abandonment, and attracting new customers seeking alternative payment methods.

Importantly, SNBL offers several advantages over BNPL including avoiding debt and interest by paying upfront for purchases; helping consumers achieve savings goals faster with incentives and gamification; facilitating the growth of savings by investing in financial products and providing access to better deals and offers from partner merchants.

HOW "SAVE NOW BUY LATER" WORKS

Setting a Goal - here, users can set specific objectives for their savings, visualizing progress, and staying motivated. Goals are often related to products or significant purchases, with a set value and deadline.

Creating a Savings Schedule - SNBL apps break down a user's savings schedule into equal parts until the purchase deadline. Users plan to deposit fixed amounts monthly or fortnightly.

Saving Consistently - users save consistently to reach their desired goals, supported by SNBL apps.

Incentivizing Saving - SNBL apps employ features to help users reach savings goals effectively, discouraging spending elsewhere.

Partnering with Retailers - some SNBL apps partner with retailers, linking user savings directly to the retail store. This benefits both parties, with merchants making sales and customers obtaining what they want without incurring debt.

CONCLUSION

The emergence of "Buy Now Pay Later" (BNPL) and "Save Now Buy Later" (SNBL) payment models represent a paradigm shift in consumer finance, providing individuals with more options to manage their money effectively. These fintech innovations empower users to make purchases on their terms, whether by deferring payments for immediate needs or cultivating a savings habit for future desires. As these models continue to evolve, their impact on the financial landscape is likely to shape new attitudes toward spending, saving, and financial well-being.

The emergence of "Buy Now Pay Later" (BNPL) and "Save Now Buy Later" (SNBL) payment models represent a paradigm shift in consumer finance, providing individuals with more options to manage their money effectively.

PERSONALIZED CONTENT CREATION AND MONETIZATION IN WEB 3.0

Alphabet (the parent company of Google) generated a significant portion of its revenue, approximately 80%, through web-based advertisements, while Meta generated about 98% of its income through ad placements last year. These tech giants collectively contributed to 64% of all digital ad spending in the United States in 2021.

Emerging strongly is the discussion of a potential shift in this monopolistic business model due to Web3, prompting conversations about the emergence of a "new web". Web3 has the potential to serve as an underlying structure that can facilitate the introduction of innovative tools, products, and diverse methods of generating revenue within the tech industry, including the advertisement and monetization of content in the hands of users.

There is speculation as to whether the changes will genuinely revolutionize the digital landscape or merely present a rebranding of existing concepts in a new format.

Web3 is not merely a substitute for Web2. In the current Web2 system, user-generated content typically remains the property of the platform hosting it. However, Web3 envisions significant elements such as decentralized content, AI support, and the metaverse. This new framework will embrace open-source solutions, applications directly owned by their developers, and a structure devoid of intermediaries.

Web3 introduces a paradigm where content is not just static information but a dynamic, personalized experience. This is achieved through innovative technologies like AI-driven algorithms, machine learning, and decentralized applications (dApps).

By collecting and analyzing user data securely stored on decentralized ledgers, these systems create custom-tailored content for individual users. From web design, articles, and videos to social media feeds, every element adapts to user preferences, behavior, and interests.

DISTRIBUTION OF CONTENT

Web3 technologies have revolutionized content sharing, introducing efficient peer-to-peer (P2P) networks through platforms like InterPlanetary File System (IPFS) and Filecoin. For example, IPFS draws over 13 million active users monthly, offering decentralized file storage and bypassing centralized servers for better content distribution.

Decentralized platforms offer creators the ability to share content without fear of censorship, hosting over 400,000 websites on IPFS. Leveraging blockchain technology, these platforms give creators greater control over their work, ensuring content reaches audiences without unnecessary restrictions.

Web3 employs decentralized algorithms and user-generated metadata, enhancing content discovery and recommendation systems. These systems boast of a 20% higher click-through rate compared to centralized platforms, providing personalized content recom-

mendations while prioritizing user privacy and control over their data.

The decentralized nature of Web3 not only bolsters efficient content distribution but also empowers creators and users with greater content control. The ongoing growth of Web3 platforms and decentralized file storage systems promises further innovations in content sharing and discovery.

OWNERSHIP AND MONETIZATION

Monetization within Web3 is equally transformative. Traditionally, content creators relied on ad revenue or subscription models, often controlled by intermediaries. In Web3, the introduction of blockchain and smart contracts has revolutionized monetization methods. This change introduces a profound shift in power dynamics within the digital space, paving the way for creators to take control of their creative output.

Creators can directly engage with their audience, leveraging tokenization and Non-Fungible Tokens (NFTs) to monetize their content. NFTs can be linked to content allowing creators to sell unique pieces of digital work in ways previously impossible. The introduction of NFTs means that creators can sell the same piece of content multiple times, or even sell fractional ownership of it.

Furthermore, through smart contracts, creators can distribute unique content, and digital collectibles, or access exclusive direct experiences with their audience, eliminating the need for intermediaries and providing creators with more control and revenue.

IMMEDIATE PAYMENT OPPORTUNITIES WITH SMART CONTRACTS

In the age of Web3, creators no longer have to wait for periodic paychecks or depend on advertisers for income. Smart contracts have revolutionized payment methods, allowing creators to receive instant compensation for the use of their content. Leveraging blockchain technology, these contracts operate autonomously when specific conditions are fulfilled, eradicating middlemen and delays in payment.

Creators now have the liberty to design their payment structures, establish their business models, and engage directly with their audience. The shift to Web3 holds significant promise in enabling creators worldwide to earn more swiftly and gain greater autonomy, fostering a more sustainable and empowering environment for content producers.

USER EMPOWERMENT AND PRIVACY UNDER WEB3

Web3 represents a transformative shift for creators and users, offering a sense of empowerment and bolstered privacy.

Unlike the current Web2 landscape, where platforms frequently exploit user data for tailored ads, Web3 promises a user-focused system, giving individuals control over their data. Users can now choose whether to share their data and, should they decide to do so, can also benefit from it financially.

Web3 introduces a paradigm where content is not just static information but a dynamic, personalized experience.

Beyond this enhanced control over personal data, Web3 shows the potential to fortify user privacy. With features like data decentralization and encryption, users now can keep their personal information secure. This focus on user privacy stands as a notable advancement from the privacy breaches and data misuse common in the Web2 era.

DECENTRALIZATION OF SOCIAL MEDIA

The current landscape of social media platforms is rife with challenges such as oversaturation, biased algorithms, and limited visibility for content creators. The present model often favors mainstream content, leaving newer or specialized creators struggling to reach their audience or gain attention.

In response to these issues, Web3 introduces decentralized social media as a solution. This framework moves away from the centralized platform model, shifting towards a peer-to-peer network that distributes content more equitably, offering a fairer playing field for creators of all kinds, irrespective of their popularity or niche status.

Decentralized social platforms also promise better visibility for creators. By sidestepping platform-imposed rules, content value is gauged by the community itself, fostering an environment where engagement and feedback determine content recognition and rewards more equitably.

Moreover, the decentralized approach enables AI technologies to enhance the user experience. Rather than controlling content visibility, AI can curate more personalized feeds for users. This tech can also create new revenue channels, such as ethical and precise ad targeting based on user-consented data sharing.

THE INTRODUCTION OF MICROTRANSACTIONS

Microtransactions are reshaping how content creators earn revenue and how consumers access premium content or specific features. Unlike traditional payment models that require users to pay a fixed subscription fee or make a large upfront purchase, microtransactions offer a granular payment structure.

Recent reports show a significant 40% rise in microtransaction adoption on media platforms, signaling both creators and consumers recognize the value and convenience this method offers in monetization.

This tailored approach offers a more personalized experience, giving users more control over their spending and supporting content aligned with their interests. This flexibility leads to increased engagement, encouraging users to explore a broader range of offerings and benefits content creators, who can monetize their work more individually.

Recent reports show a significant 40% rise in microtransaction adoption on media platforms, signaling both creators and consumers recognize the value and convenience this method offers in monetization.

Microtransactions offer access to new markets that traditional payment models might miss. The pay-as-you-go structure breaks down the barrier of high initial costs or subscription fees, making premium content accessible to users on limited budgets or hesitant about long-term subscriptions. This

approach widens the audience for content creators, creating additional revenue streams that might have been missed without this payment model.

HOW BUSINESSES CAN LEVERAGE THE EMERGENCE OF WEB3

The following essential tips are recommended for companies to keep in mind as they navigate this new frontier:

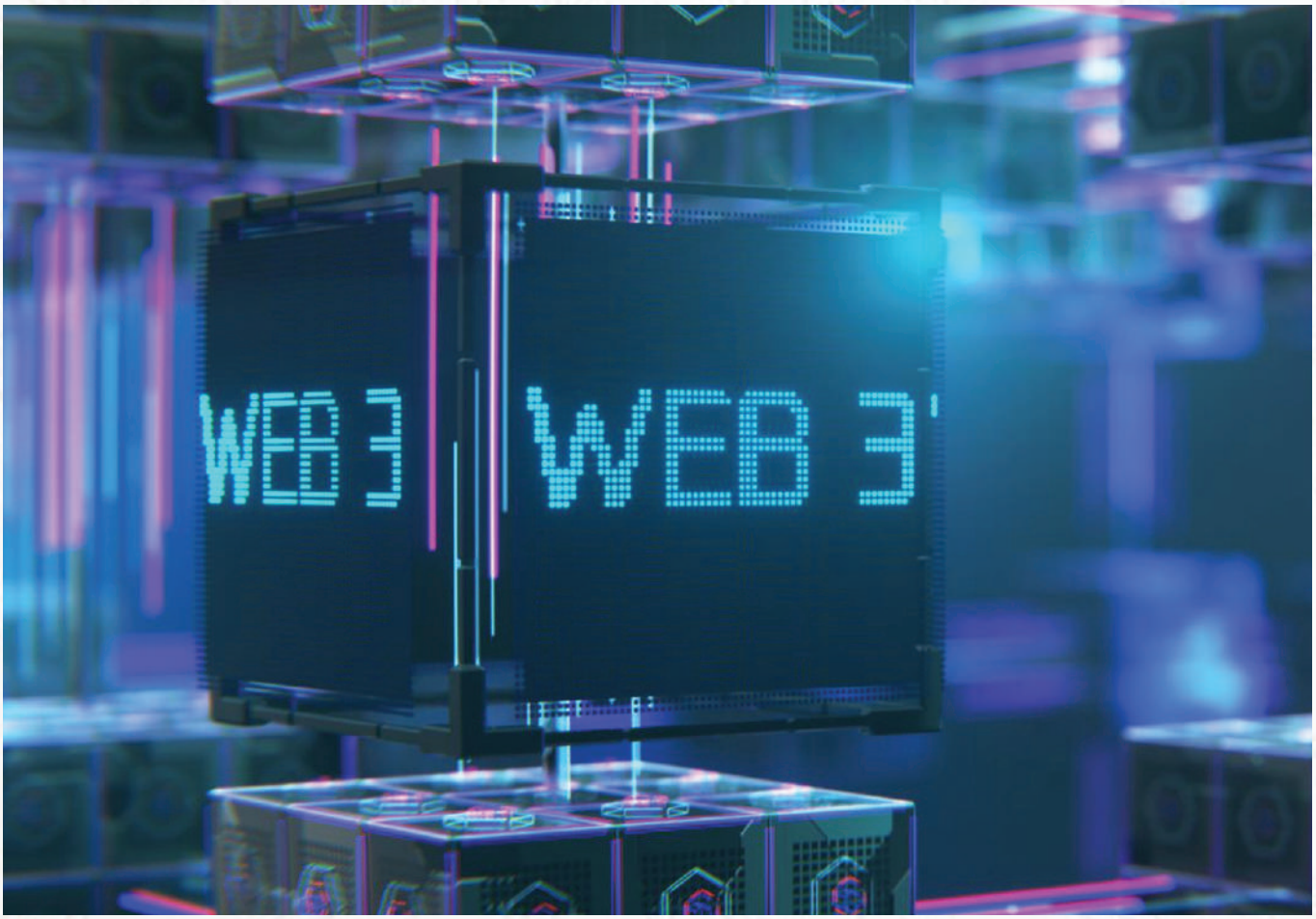
1. Have a Clearly Defined Goal: In the Web3 space, the focus is on community-driven products. Although technological development remains vital, emphasizing a solid community is equally crucial. Prioritizing community development over the tech stack should be considered.

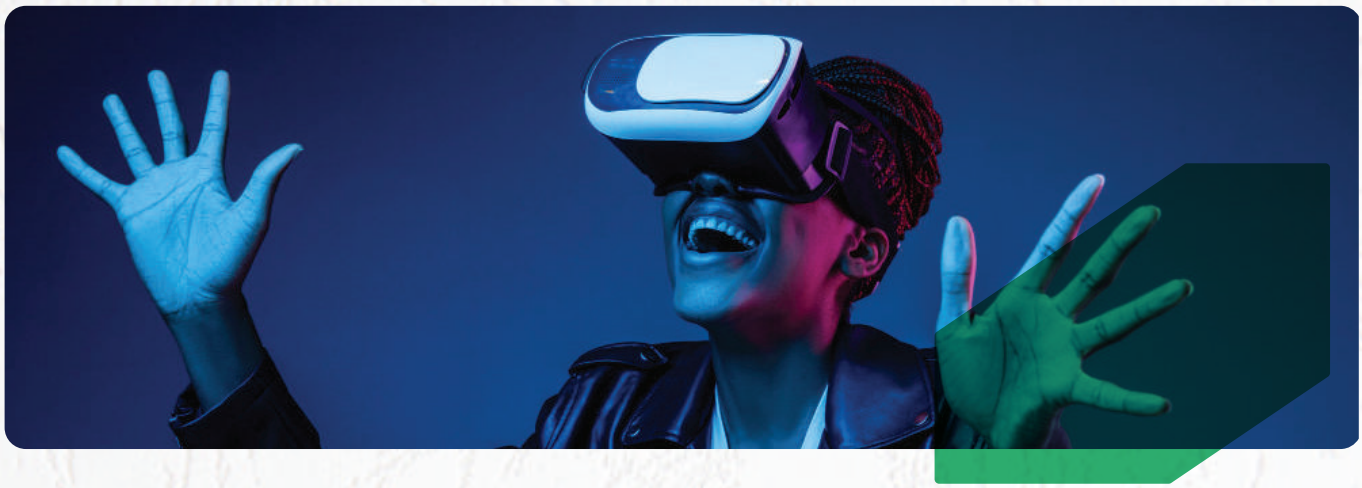
2. Embrace Decentralization: Traditionally in Web2 business strategies, and customers were the primary focus of marketing efforts. However, in Web3, equal importance is placed on the team, product developers, investors, and partners. For Web3 startups, the community roles are as significant as traditional sales and marketing efforts.

3. Motivate Your Audience: Rather than pouring large budgets into conventional marketing strategies, Web3 teams can entice initial users by offering tokens and follow-up reward systems. These incentives encourage the community to attract more users and generate higher interest in the product. Creating a strong incentive system helps in fostering a dedicated community and driving growth.

CONCLUSION

Web3 is reshaping the media and entertainment industries by redefining monetization models. The potential is immense, with decentralized advertising, microtransactions, and tokenization of content offering exciting opportunities for content creators and consumers. As we navigate this new era of revenue generation, stakeholders need to embrace the power of Web3 and leverage its transformative capabilities to orchestrate success in the media landscape.





TECHNOLOGY TRENDS TO WATCH IN 2024

A. AI and ML: Innovation across various sectors is being driven by AI and ML. Noteworthy trends include the emergence of Generative AI contributing to the creation of multimodal AI models capable of processing diverse data types. Additionally, advancements in deep learning and neural networks are on the rise. The use of AI-driven platforms is expected to improve data security, while the use of synthetic data, generated by AI for training machine learning models, is anticipated to see substantial growth.

B. Blockchain: The technology is experiencing increased adoption and exploration by businesses, leading to transformative changes in the financial landscape. This includes a rise in asset tokenization and the prevalence of digital transactions. Key trends will include the adoption of central bank digital currencies (CBDCs) and the integration of AI with blockchain to enhance automated processes.

C. InsurTech: The insurance sector is poised for significant impacts from predictive analytics and AI. Trends such as expanding self-service options for policyholders, the development of custom insurance apps, and the introduction of customer portals are expected to become prevalent as regulatory guidelines for service providers are rolled out.

D. Regulatory Technology (RegTech): RegTech is projected to undergo significant evolution in Ghana and globally. The increased adoption and scaling of AI in regulatory intelligence are expected to enhance regulatory processes. Prominent features include autonomous delivery and a data-first approach in process intelligence, providing exciting opportunities for regulatory professionals. The regulatory compliance landscape will evolve in tandem with changes in business and regulatory environments.

E. Sustainable Technology: Crucial in designing tailored solutions, sustainable technology plays a pivotal role in safeguarding past and future investments. It is expected to optimize energy consumption, reduce waste, and promote sustainable living. The integration of advanced sustainable solutions is crucial for efficiently navigating environmental challenges.

F. Internet of Things (IoT): Anticipated developments in IoT include increased adoption of edge computing, the growth of white-label IoT platforms, integration of AI and Machine Learning, and the expanding scope of IoT platforms in industrial applications.

G. Buy Now Pay Later (BNPL): The BNPL market is set for substantial growth, particularly with increased adoption and use of e-commerce platforms. The flexibility of this model will lead to increased integration by businesses into their payment software, enhancing their products and service offerings.

H. AR, VR & MR: Rapid growth is expected in immersive technologies. AR is becoming more accessible and popular in various industries and government organizations. MR, a combination of VR and AR, offers sophisticated data processing. The VR market is projected to grow significantly due to technological advancements and increased adoption. The current digital transformation initiatives suggest a promising environment for the adoption of these technologies, gradually becoming integral to daily life.

CONSUMER INSIGHTS – WHAT CONSUMERS NEED TO KNOW

07

"CONSUMER CENTRICITY" AND "CONSENT" – PROTECTING CONSUMERS IN THE NEW TECHNOLOGICAL ERA

Ordinarily, no business or enterprise should be told or be encouraged to put the "consumer first" in all it does. This is because typically, each business exists to serve a consumer need presupposing the primary consideration of the interest(s) of the consumer in any development of products or services.

However, the lack of attention demonstrated by many businesses over the years to the needs of consumers and largely, the declining customer service experiences, etc. are compelling the emergence of a spirited advocacy to get businesses, service providers, and innovators to put the consumer first in their entrepreneurial pursuits – consumer centricity.

This advocacy is timely due to the growing integration of technology into every sphere of the consumer's life with exposure to inherent risks of breach of personal data, theft, and impersonation, among others.

The concept of "consumer centricity" requires developers and promoters of new products or services to prioritize and put the ultimate interest of intended users at the core of any development and deployment phase of their innovations. It requires ticking the box on all checklists that promote ethical and responsible design, testing, and use of developed products or services and seeking to ensure the consumer is not exposed but protected on all fronts.

The promotion of the consumer interest may include ensuring an innovation serves a pain point; promotes the safe and ethical use of technology; protects against breaches of personal data supplied by end-users; prohibits the unconsented use of collected data; accommodates and incorporates consumer feedback into product or service upgrades among others.

Further, the commitment to consumer centricity must ensure user experiences are consistently enhanced in a secure and user-friendly manner over the product or service use period.

Today, the need to be deliberate about consumer needs is growing due to the increasing development of new technologies, the fast-paced transition from offline to online, and the growing list of associated risks – taking control of consumer data and use cases to new levels.

With limited consumer influence on the development process of new innovations, innovators must ensure greater control is granted to consumers at the deployment phase of their innovations. To achieve this, end users should always maintain the right to opt in, use, and out of innovations without restrictions through consent.

Due to the critical role of "consent" by consumers to their participation in innovation

deployments, it has become imperative to enhance onboarding, use, and exit processes for consumers as a way to achieve the freedom to join, use, and exit or opt out of innovations.

Consent expressed in any form is central to the practical enforcement of the rights of end-users in this regard. Personal data should not be collected, processed, stored, or used without the consent of the related person. Equally, participation in innovations should not be encouraged without the express permission of the targeted participant.

To further enhance the consent regime, innovators must seek to simplify in plain language consent processes that enable the consumer to opt in and permit the use of their data, experiences, and preferences as insights for their continued use of developed innovations and upgrades.

Nonetheless, consumer consent needs to be precise and relative. No innovator should be allowed to procure blanket consent from consumers for the use of their data beyond the intended purposes. At best, consumers must ensure they are granting consent specifically for the intended use only as same is the only way to ensure innovators do not abuse collected data for other unilateral use to the detriment of the end-user.

As a consumer your consent is your approval for the use of your data and you must ensure you understand the scope of the consent being sought by innovators before ticking, clicking, and signing off in approval.

DATA PROVISION TO 3RD PARTIES AND THE LEGAL REGIME

Within the current financial landscape characterized mainly by digital transactions and technological innovations, financial consumers across the globe commonly deal with 3rd party service providers to access a host of services. As this exchange of personal and financial information becomes commonplace, it is imperative for consumers to be well-informed about the potential risks and protective measures associated with sharing their data, especially with 3rd party service providers.

UNDERSTANDING THE PERSONAL DATA REGIME

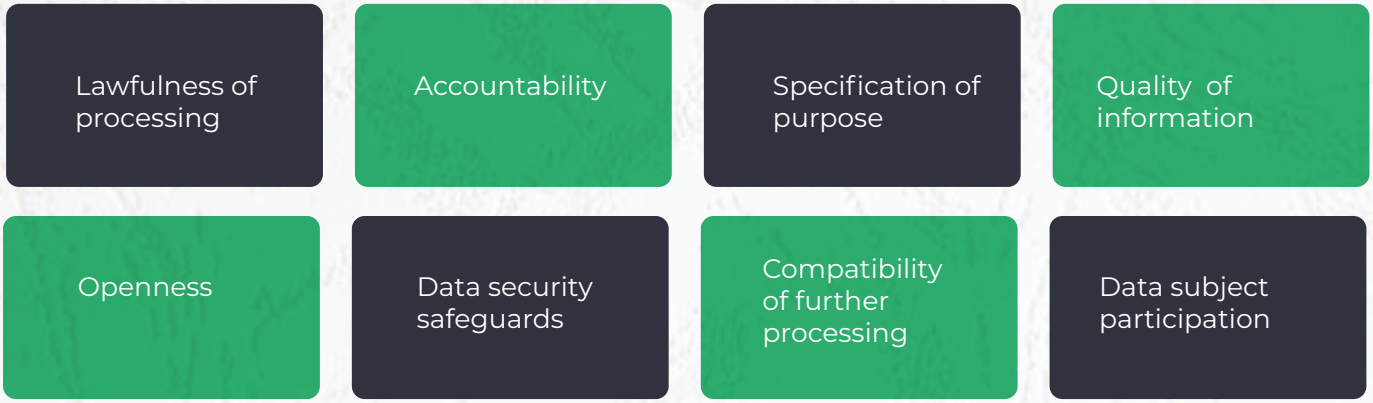
At the core of data protection lies the need for an understanding of personal data, and the principles governing the collection and processing of personal data. Personal data ordinarily encompasses a broad range of an individual's information, including names, addresses, contact details, financial specifics, and identification numbers. The sensitivity of financial data, including account details and transaction histories, necessitates a heightened awareness of the potential consequences of unauthorized access.

THE LEGAL FRAMEWORK

Ghana, recognizing the significance of data protection, has enacted the Data Protection Act, 2012 (Act 843), which serves as a regulatory framework governing the processing of personal data. It is therefore important for financial consumers to familiarize themselves with this legislation, understanding the rights and obligations it confers upon both data subjects and data controllers.

Underlying data protection are some principles governing the collection, storage, and processing of personal data by data processors and or data controllers. These principles serve as guide to data processors when dealing with personal data collected from individuals for any purpose.

Image 1.0. Principles governing Data Protection



CONSIDERATIONS BEFORE PROVIDING PERSONAL DATA

A. Purpose of data collection and compliance with regulations: At all material times, consent by a data subject (consumer) should be explicit and informed, with consumers understanding the purpose of the data collection and processing to appreciate the full scope of the use of such data by the third party. A further step towards this will be the customer confirming that the 3rd party service provider has procured a data protection registration. Understand your rights regarding data access, correction, and deletion.

B. Basic due diligence: Before engaging with third-party entities, consumers should conduct due diligence to verify the reputation of these entities. Trustworthy entities typically exhibit transparency in their privacy policies and have robust security measures in place. The assessment should extend to scrutinizing the security protocols implemented by third parties, such as encryption, secure transmission methods, and authentication processes. It is important to understand the security measures implemented by the third party to safeguard sensitive financial information.

C. Scrutiny of Privacy Policies: Consumers should carefully scrutinize the privacy policies of entities they engage with. These policies elucidate how personal data is collected, processed, stored, and protected. Red flags may include vague or overly broad privacy policies, as well as clauses allowing the sharing of data with other entities without explicit consumer consent. Consumers should inquire about the third party's data retention policies and ensure they align with their expectations, and also clarify how long such data will be stored.

D. Monitoring and Control: Proactive monitoring is crucial in the digital age. Financial consumers should conduct regular audits of permissions granted to third parties and promptly revoke access for entities that no longer require such information. Additionally, consumers should be aware of their right to request a copy of their data from third parties and the ability to have same transferred to another service provider if necessary.

E. Incident Reporting: In the unfortunate event of a data breach, financial consumers have the right to be promptly informed. It is essential to report any suspicious activities or unauthorized access to relevant authorities. Continuous consumer education is paramount, enabling individuals to stay informed about the latest cybersecurity threats and best practices for protecting personal data.

CONCLUSION

The onus is on consumers to safeguard their personal and financial data when engaging with third-party entities. By comprehending the legal framework, critically assessing third parties, and actively monitoring data usage through privacy policies and control measures, consumers can navigate the digital landscape with confidence. Empowered consumers play a pivotal role in cultivating a secure and trustworthy digital ecosystem, ensuring that the benefits of technological advancements are enjoyed without compromising privacy and security.

INSIGHTS

08

THE BATTLE FOR ONLINE SAFETY – THE ROLE OF TECHNOLOGY

The world is rapidly evolving into a digitally interconnected space, with cybercrime emerging as a significant threat to millions of online users worldwide including individuals, businesses, and governments alike. The once expansive digital ecosystem, offering endless explorative possibilities, has transformed into an arena where individuals, businesses, and governments are grappling with the complexities of safeguarding the virtual space.

Specifically, in today's world where we effortlessly surf the web, carry out transactions, share personal experiences, and engage with a worldwide community, the danger of cyber threats has never been more prominent. To this end, the adoption of technology to combat cyber threats has become not only crucial but imperative, as malicious actors continually exploit the vulnerabilities within digital systems and/or virtual spaces.

The aim of this article is to explore how technology can be harnessed to prevent, detect, and respond to cybercrime.

THE STATE OF ONLINE SAFETY

In today's digital age, Ghana, like many other countries, is undergoing a significant transformation in its use of technology. The internet has become a vital part of daily life for communication, commerce, and education, opening up numerous opportunities but also introducing substantial challenges when it comes to online safety and security.

A noteworthy trend is the widespread adoption of mobile technology, with a large portion of the population accessing the internet through smartphones. However, this shift to mobile devices comes with increased risks related to mobile-centric cyber threats, making it essential to prioritize the security of these platforms and connected devices to safeguard personal and financial information.

Recent times have seen the nation grappling with a surge in cyber threats and online attacks. The statistics indicate a significant rise in various types of cyber incidents, ranging from individual-focused phishing attacks to complex cyber espionage campaigns affecting both businesses and government entities. The National Cybersecurity Advisor reported a total of 11,550 cybercrime cases since the launch of the Cybercrime Incident Reporting Points of Contact (PoC) in October 2019. This system was created to facilitate the reporting of cybercrime and cybersecurity incidents by the public, strengthening the efforts of the National Computer Emergency Response Team (CERT) operating under the National Cybersecurity Centre (NCSC).

Cyberfraud, such as credit card fraud, identity fraud, or romance fraud, remains the most prevalent form of cybercrime in Ghana. Perpetrators typically create fake online profiles or websites to deceive victims into sharing their

money or personal information. Significantly, the financial sector has become a particularly attractive target for hackers who exploit vulnerabilities in online banking systems. The Bank of Ghana's Fraud Report for the year 2022 highlighted cyber email fraud as one of the top five fraud categories significantly impacting the banking industry. Notably, this form of fraud resulted in losses of GHC4.3 million in 2022 alone, representing a 65.5% increase from the previous year.

Recognizing the severity of cybercrime, the government has taken a proactive approach, working in collaboration with the Cybersecurity Authority and related institutions such as the Bank of Ghana and the Securities and Exchange Commission to address concerns related to online safety. Several initiatives have been launched to raise awareness among citizens about the importance of cybersecurity. Prominent efforts include the National Cyber Security Awareness Month and the Child Online Protection Portal, designed to educate the public on how to protect themselves online. Additionally, regulating agencies have implemented regulations and rolled out initiatives requiring businesses, particularly in critical sectors like finance and healthcare, to adopt stringent cybersecurity measures.

THE IMPACT OF CYBERCRIME

The repercussions of these cyber threats transcend the digital world and have tangible impacts on individuals, businesses, and the nation's economy. Discussed below are some of these impacts:

A. Individuals: For individuals, cybercrimes like phishing, identity theft, and online fraud pose significant financial risks, leading to unauthorized bank transactions, stolen credit card information, and fraudulent charges. Furthermore, these digital invaders can breach personal privacy by accessing sensitive information, emails, and documents, causing emotional and psychological distress. Identity theft is particularly devastating, resulting in long-lasting damage to one's credit, reputation, and overall well-being. The psychological toll of such crimes is profound, inducing stress, anxiety, and a sense of helplessness.

The once expansive digital ecosystem, offering endless explorative possibilities, has transformed into an arena where individuals, businesses, and governments are grappling with the complexities of safeguarding the virtual space.

Moreover, there is a growing awareness of the internet's threats to children and young people, who are exposed to various risks such as sexual and violent content, cyberbullying, harassment, hate speech, online grooming for illicit activities, and more. These online experiences can harm children's self-esteem, psychological well-being, and personal development, leaving them vulnerable to physical harm, exploitation, and abuse.

B. Businesses: Businesses face their own set of challenges, including financial losses, damage to their reputation, and potential legal consequences. In our interconnected global economy, a cyber incident affecting one entity can trigger a domino effect impacting others. Cyberattacks on businesses result in substantial financial losses,

including costs related to breach investigation, data recovery, customer compensation, and legal proceedings. Such attacks tarnish a business's reputation, eroding customer trust and loyalty, often making it challenging to recover.

Ransomware attacks and other cybercrimes disrupt business operations, leading to lost revenue, decreased productivity, and even the closure of smaller enterprises - some are unable to bounce back from the disruption. Additionally, businesses may face legal ramifications and regulatory fines for failing to adequately protect customer data, further escalating the financial impact.

C. National Economy: A country like Ghana relies heavily on the Internet across various sectors such as education, healthcare, agriculture, finance, tourism, trade, and governance. Nevertheless, the absence of robust online safety measures can jeopardize the growth potential, competitiveness, and resilience of these sectors. Cyberattacks on government entities can threaten national security by compromising sensitive data and systems, including critical infrastructure like power grids, water systems, telecommunications networks, and government institutions.

Cybercrime carries the potential to disrupt the country's economy by impacting critical infrastructure, causing financial losses, and deterring foreign investment. Government agencies must allocate substantial resources to address cyber defense and recovery, diverting funds from other essential public services. Intellectual property theft is also a concern, undermining the nation's competitive advantage and innovation. Government agencies play a pivotal role in responding to and preventing cybercrimes, necessitating considerable resources for law enforcement and national defense, which can have ripple effects on other crucial public services.

THE ROLE OF TECHNOLOGY IN COMBATING CYBERCRIME

A. Advanced Security Systems: One of the primary functions of technology in combating cybercrime is the development and implementation of advanced threat detection systems. Machine learning algorithms, artificial intelligence (AI), and behavioral analytics play pivotal roles in identifying abnormal patterns and potential security breaches. These systems continuously evolve, learning from new threats and adapting to changing attack vectors to detect even the most subtle indicators of malicious activity. By automating threat identification, these systems offer a proactive defense, allowing organizations to stay one step ahead of cyber adversaries.

B. Encryption Protocols: With data as the new currency in this digital age, encryption protocols act as secure vaults, protecting sensitive information. Tools such as end-to-end encryption, secure sockets layer (SSL), and virtual private networks (VPNs) play a crucial role in safeguarding sensitive data during its transfer. These protocols make any intercepted data worthless

Cybercrime carries the potential to disrupt the country's economy by impacting critical infrastructure, causing financial losses, and deterring foreign investment.

to cybercriminals, guaranteeing the confidentiality and integrity of information during both transmission and storage. As these communication channels become increasingly secure, the likelihood of interception and unauthorized access diminishes.

C. Biometric Authentication and Access Controls: To counter the rising threat of identity theft and unauthorized access, technology has embraced biometric authentication methods. Fingerprints, facial recognition, and iris scans provide a higher level of security compared to traditional password-based systems. Moreover, access controls, including role-based access and multifactor authentication, add additional layers of defence against cybercriminals.

D. Incident Response and Forensic Technologies: In the aftermath of a cyber attack, technology plays a crucial role in incident response and digital forensics. Automated incident response systems enable organizations to quickly detect and contain threats, minimizing the potential damage. Forensic technologies, including digital evidence gathering and analysis tools, assist law enforcement agencies in tracing cybercriminals and building legal cases against them.

E. Blockchain Technology: The decentralized and impermeable nature of blockchain technology can be leveraged to boost cybersecurity. Blockchain-based systems provide a secure transactional framework and can be employed in securing critical infrastructure, supply chains, and financial transactions. The immutability of blockchain records adds an extra layer of protection against data manipulation and unauthorized access by creating transparent audit trails and establishing secure communication channels.

F. Endpoint Security Solutions: Potentially, every device acts as a gateway and serves as the initial line of defence against cyberattacks. Nevertheless, these devices are not left vulnerable; they are secured by advanced endpoint security solutions. These comprehensive solutions encompass cutting-edge antivirus software and advanced intrusion detection systems that provide real-time protection against malicious entities like malware and ransomware. Through reinforcement of each device, entities can construct an impenetrable security system, effectively deterring threats attempting to breach their networks, ensuring a secure digital environment, and granting organizations the confidence to operate amid the evolving space of cyber threats.

CONCLUSION

As our reliance on digital infrastructure continues to grow, the ongoing development and integration of advanced technologies remain crucial for fortifying our defences and preserving the integrity of the digital realm. While technology can play a role in enhancing online safety, it is not a silver bullet that can solve all the problems. Technology solutions need to be carefully designed, evaluated, and regulated to ensure that they are effective, reliable, transparent, accountable, and respectful of users' rights. Through a combination of innovation, collaboration, and vigilance, we can navigate the digital landscape with confidence, knowing that technology is working tirelessly to keep our interconnected world secure.

GENERATIVE AI: MANAGING THE CORPORATE USER RISKS

An insurance company in Kenya has deployed billboards in the city of Nairobi with the inscription "Someone tell ChatGPT that GA Insurance is the 3rd largest General Insurer in Kenya". Similar copies of the company's acclaimed position in various insurance categories are dotted across the city.

This could be seen as a marketing campaign seeking to take advantage of the craze and buzz of "ChatGPT" - and everything may be right with it context-wise.

However, inherent in this "call to action" are risks users of ChatGPT particularly corporate ones may be exposed to due to the kinds of data either confidential or otherwise they input into the interactive chatbot or any underlying source data.

Therefore, this article seeks to highlight some of these risks and propose ways companies can promote the use of emerging technologies while safeguarding their proprietary data from disclosures.

ARTIFICIAL INTELLIGENCE (AI), GENERATIVE AI AND CHATGPT REVOLUTION

The rollout of ChatGPT by OpenAI in November 2022 amplified the general consumer interest in the emerging technology of Artificial Intelligence (AI). Although ChatGPT is not the first use case of Artificial Intelligence, its ability to 'humanize' the use of technology particularly in a conversational manner has heightened the applicability of AI to many human endeavors.

Through iterative processes, AI leverages machine learning techniques to learn from large volumes of data to produce reasonable, predictive, and near-human cognitive information. Using publicly available data sources, AI is able to produce and create its own data sets (information) from these existing ones although not always accurate and current due to the time gap in its data sources.

The iteration process combines large volumes of data with fast and intelligent algorithms to allow the underlying software to learn automatically from patterns or features in its source data to produce results that have grabbed the attention and curiosity of many - thinking and acting like humans in its processed responses.

This cognitive ability of AI represents computerized machines with comparable human intelligence using machine learning, and deep learning among others to perform various tasks with ease.

The power of Machine Learning to feed on large volumes of data using different statistical techniques combined with the influence of deep learning using artificial neural networks to process information, solve complex problems, etc has enabled AI to discover various patterns in data and learn through high volumes of unstructured data in varied forms including text, images, and videos.

Comparably, Generative AI has

emerged as a category that uses high volumes of raw data in iterating and learning patterns within same to generate the most likely accurate responses when prompted with a question.

This form of AI relies on large language models (LLMs) to produce natural language outcomes and generate texts and other language-based mediums. The potential of Generative AI to do this is what has enabled OpenAI's revolutionary chatbot - ChatGPT.

Simply, ChatGPT is an AI-powered chatbot that uses natural language processing and machine learning algorithms to understand user queries and respond with relevant information in a conversational manner equal to human cognitive responses.

Its processes are optimized for dialogue using the Reinforcement Learning with Human Feedback (RLHF) method which uses human demonstrations and preference comparisons to guide Generative Pretrained Transformer (GPT) models toward desired behaviors.

To achieve the desired results, the models are trained on vast amounts of data from the internet including conversations, news items, articles, etc to enable human-like responses.

As part of its core functionality, ChatGPT analyses data, token by token, by identifying patterns and relationships; an ability that has enabled its superhuman responses and generated a worldwide craze within the shortest period of its launch.

This cognitive ability of AI represents computerized machines with comparable human intelligence using machine learning, and deep learning among others to perform various tasks with ease.

THE CALL TO ACTION

By the advertisement, GA Insurance is asking the general public to provide data in confirmation of its positions within the insurance sector in Kenya in a manner that could become a source of data for subsequent iterations by ChatGPT and become responses to queries about which insurance company holds the positions the billboards seek to embed.

This call to action is for people to feed ChatGPT with data that enables it to one day produce responses in confirmation of GA Insurance's claims. This desired outcome by GA Insurance is possible because of the way ChatGPT and every other Generative AI works. Generative AI as indicated earlier processes data from identified sources particularly online and based on processed data, makes predictive outcomes of the best possible answer based on the data sets.

Therefore, should people including workers need to the call and take to online platforms acknowledging GA Insurance for the various advertised positions, over time, ChatGPT and other Generative AI will come to learn and process such claims as correct positions of GA Insurance in respect of queries related to same.

Such marketing campaigns could be effective in helping the company establish itself and be validated somehow by emerging technologies such as Generative AI - as many may without more take as accurate responses from these chatbots.

THE ASSOCIATED RISKS

Every Generative AI tool needs data for its iteration process. As of now, they do not generate their own data sets - they process what is available. Therefore, the call to action is a call to provide or feed these Generative AI tools with data.

The temptation in doing this is to provide more than what the call to action requires. And anyone who has used any of the Generative AI tools will attest to the temptation to be specific and particular with queries because of the near-perfect responses one gets from these chatbots.

Over time, people could begin to input or ask queries or have conversations that border on confidential information relating to themselves, others, or the companies they work for.

In a FAQ by OpenAI on whether such conversations will be used for training, the developer of ChatGPT answered in the affirmative saying "Yes, your conversations may be reviewed by our AI trainers to improve our systems". (Don't be mistaken by the use of the word "may". It means "it will be used" as that's the only way the technology could be improved).

Also, on the question of whether specific prompts can be deleted, OpenAI said, "No, we are not able to delete specific prompts from your history. Please don't share any sensitive information in your conversations".

This is the clearest warning any technology developer could give. It's plain black and white. Anything you input as part of your conversation with any chatbot will not be deleted. It will become part of the new dataset that the system will be trained on as part of its improvement process.

The risks therefore can be quantified. There is no guarantee for the protection of the confidentiality of the prompts you input into any chatbot. Eventually, such prompts will be processed and iterated. It could form part of an answer or response a chatbot will be providing a user asking similar questions in the future.

So, whether personal or company information, confidential or otherwise, once inputted into a chatbot, such information will become subject matter data for processing by the chatbot and made widely available on request by others.

And as such information are not capable of deletion from the memory of these chatbots, the unintended consequences of exposing hitherto confidential information to disclosure, and use can be avoided by implementing some of the recommendations below.

WHAT NEEDS TO BE DONE

AI and its use cases such as Generative AI have tremendous opportunities to improve the productivity of workers. Therefore, companies should not seek to ban its use in workplaces despite its risks.

To mitigate the risk, the following initiatives could be instituted.

1. **Policy rollouts:** As first steps, companies must redefine employee conduct and expected uses of these emerging technologies through policy initiatives and procedures. Such policies and procedures must clearly define the scope and permitted use cases to limit the compromising company confi-

dential information and prevent the breach of the intellectual properties of others.

Companies must ensure all stakeholders participate in the design of these policies to ensure their respective concerns are accounted for. Additionally, companies must adopt a feedback loop for the measure of policy impacts and reviews that accommodate new updates/upgrades in these emerging technologies.

2. Training and re-training of staff: With employee conduct defined, companies must ensure comprehensive training and refresher programs are instituted to build employee capacities on the use of emerging technologies such as Generative AI. The training programs must leverage the benefits of theoretical and practical sessions to test and confirm employee understanding and appreciation of these technologies.

Where internal resources exist for this training, companies must use them or procure the services of external people with demonstrated expertise and practical ways of safeguarding the use of these technologies.

3. Intermittent audits and compliance checks: Compliance remains the surest way to ensure employees use these AI tools in accordance with defined conducts. Compliance checks such as intermittent audits or spot checks will help build and measure employee compliance. Additionally, initiatives such as compliance awards, the establishment of helpdesks, departmental champions, etc will help promote a strong compliance culture among employees.

4. Adoption of company-wide AI tools: Some companies have the resources to adopt company-wide AI tools built to the specific use cases of such companies. Where such capacities exist, such companies must invest in their own AI tools with control over the confidentiality of data or information uploaded or shared via such platforms. Companies may explore this option as an add-on productivity tool that enables new ways of working in a secure environment.

CONCLUSION

Increasingly, we are recognizing the immense importance of AI tools and Generative AI to drive greater productivity across many industries. This provides greater justification for their uses than their complete ban despite their risks. Therefore, the adoption of some of the recommendations in this article will help safeguard the use of these emerging tools and must be highly considered by companies to ensure their proprietary or confidential information is not exposed unintentionally to disclosures and breaches.

INDUSTRY PLAYERS' SPOTLIGHT

09

eCAMPUS

eCampus LLC, a pioneering Ghana-based company, is spearheading a transformative educational movement across Africa with its innovative online learning solutions. Since its inception in 2015, eCampus has been at the forefront of e-learning, reshaping the educational landscape to be smarter, more accessible, and customized to meet the diverse needs of learners throughout the continent.

Founded with the mission of promoting self-paced education in Ghana, eCampus has emerged as a comprehensive educational hub. Through an intuitive web platform and a mobile app, the company offers a broad spectrum of courses, prep tests, microlearning modules, and corporate training programs, addressing a range of subjects and skills. This adaptability positions eCampus as a dynamic educational force, addressing the evolving demands of learners in a rapidly changing world.

A key differentiator for eCampus is its integration of artificial intelligence (AI) into the learning experience. By leveraging AI technology, the company optimizes assessment, evaluation, and reporting processes, resulting in enhanced teaching and learning outcomes. This not only streamlines educational experiences but also ensures a personalized and effective approach to learning, catering to individual needs.

Beyond traditional educational boundaries, eCampus actively supports learners in exam preparation, aids job seekers in navigating the competitive job market, and facilitates employee compliance with industry standards through targeted training programs. The incorporation of AI into these processes not only enhances efficiency but also fosters a more adaptive and responsive learning environment.

In a unique twist, eCampus recognizes and rewards the endeavors of learners through a points system. Learners accumulate points throughout their educational journey, which can then be redeemed for exciting prizes or discounts. This gamification aspect adds an engaging element to the learning experience, motivating individuals to actively participate and excel in their educational pursuits.

Moreover, eCampus is not only shaping the future of individual learning but is also playing a pivotal role in the compliance efforts of financial service providers. By offering tailored corporate training programs, eCampus supports financial institutions in ensuring that their employees are well-versed in industry regulations and compliance standards. This strategic alignment with financial service providers underscores eCampus' commitment to delivering not only quality education but also contributing to the overall compliance and regulatory landscape.

Overall, it serves as a driving force for beneficial societal transformation through education, and a crucial partner for financial service providers in achieving their compliance goals. eCampus is more than just an educational platform; it is a companion in the pursuit of knowledge, development, and regulatory compliance.

PAST INDUSTRY EVENTS

BANK OF GHANA eCEDI HACKATHON

The eCedi Hackathon 2023, a joint initiative by the Bank of Ghana and EMTECH Solutions Inc., recently ended. The event which spanned a period of 12 weeks, was aimed at providing a platform for FinTechs, developers, and innovators to devise innovative solutions that explored the diverse use and applications of a Central Bank Digital Currency (CBDC).

The hackathon brought together innovators in technology and finance, with the goal of exploring the potential of CBDC. It was structured to encourage innovation, drive technological advancement, and create solutions that could transform the financial landscape of Ghana.

In 2022, the Bank of Ghana successfully assessed both online and offline applications of the eCedi, showcasing its potential to broaden financial inclusion. The hackathon presented an opportunity to introduce innovative solutions in the domain of digital currencies.

The Hackathon posed challenges that required innovative ideas utilizing CBDC tokens and APIs to prototype solutions or develop tools that tackle a technical issue. The use cases encompassed eCedi usage in merchant transactions (C2B), government payments (G2P), agriculture and trade (C2B, B2B), maintaining data privacy during eCedi transactions, preventing the use of eCedi for illegal transactions, ensuring eCedi interoperability, KYC models/solutions for eCedi, and potential models for cross-border payments and transactions.

The hackathon drew over 200 applications, with the regulator selecting the top 10 innovators - AgroEcedi, Applicase, David Archer, Forward Titans, Libeara x SCB Ghana, Nokofio, Moolre, Paycode, Team AutoCedi, and Team CreditLink for the Demo. Their solutions spanned a wide range of areas, including farmer empowerment, crowdfunding, taxation, digital payments for businesses, investment in government securities, eCedi interoperability, eCedi back-end infrastructure, and credit scoring.

The Hackathon serves as an important component of the regulator's eCedi research project, providing the regulator with the avenue to explore emerging technologies, drive creativity, and promote the development of eCedi.

SINGAPORE FINTECH FESTIVAL 2023

The 2023 edition of the Singapore Fintech Festival (SFF), a yearly event that brings together fintech firms from around the world, concluded on November 17, 2023. The event, which attracted over 60,000 attendees from more than 100 countries, served as a key forum for global leaders to explore significant technological developments in financial services. The theme of this year's event was "Inclusive, Resilient and Sustainable," emphasizing the importance of collaboration and outlining key requirements for shaping the future of the global financial ecosystem.

The event recorded at least 3.5 million session views and counting, with over 60,000 participants. It featured more than 500 exhibitors and over 560 renowned speakers from around the world. Participants from over 160 countries attended the event, which also included more than 100 startup pitches. The conference provided a critical examination of various aspects, including the current instability in the global macroeconomic environment.

Live broadcasts played a crucial role in the global programs that took place during the SFF 2023.

Important announcements were made, such as the winners of the MAS Global FinTech Hackcelerator and the launch of the Global Fintech Hackcelerator for green finance. There was also anticipation for an announcement on the MAS Global CBDC Challenge.

Highlights of the event included the Innovation Lab Crawl and the World FinTech Festival, which featured forty-five (45) satellite events hosted worldwide by partner cities.

TECH IN GHANA 2023

This biannual event, hosted in both London and Accra since 2017, continues to play a pivotal role in fostering and fortifying Ghana's tech ecosystem.

Encompassing a diverse array of subjects such as FinTech, AgriTech, HealthTech, ClimateTech, Gig Economy, Gaming, Policy, Investment, Entertainment, EdTech, and more, the conference served as a crucial platform for the burgeoning tech community to converge. It facilitates global knowledge exchange, encourages networking among industry peers, and provides a stage to showcase innovative solutions.

The Tech in Ghana Conference empowers the nation's entrepreneurs, enabling them to make a substantial impact on the global tech arena while garnering the essential support and recognition they deserve. To elevate Ghana's tech ecosystem on the world stage, this year's conference created a platform for those at the forefront of the technology industry to share their experiences, emphasizing the country's technological prowess.

It took place at the Accra Digital Center from November 28th to 29th, with distinguished headliners and speakers from the tech industry.

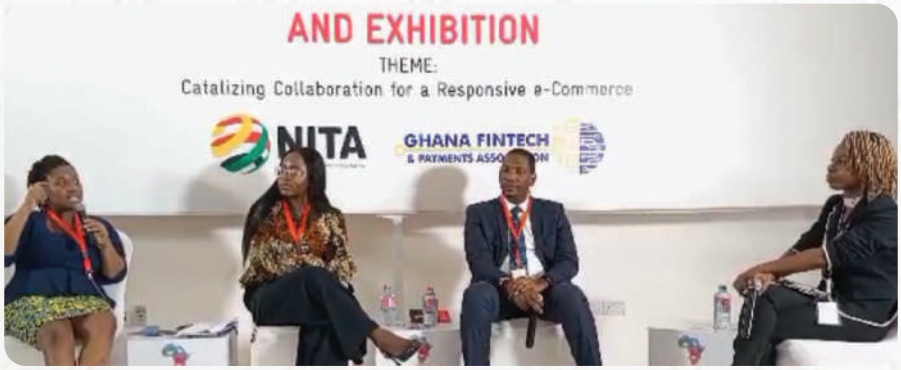
2ND NATIONAL E-COMMERCE FORUM AND EXHIBITION

The 2nd National e-Commerce Forum and Exhibition was organized by GIZ as part of their dedicated initiatives to enhance the country's e-commerce ecosystem.

This forum not only celebrated the achievements of Ghana's e-commerce landscape but also catalyzed the forging of a collective vision for its future development. By bringing together government leaders, private sector representatives, industry practitioners, SMEs, academics, research scholars, ecosystem enablers, intermediaries, and international development partners, the event fostered a collaborative environment.

Aiming to mobilize diverse stakeholders toward more inclusive and cooperative development, the forum featured extensive multi-stakeholder discussions throughout the day. The culmination of these discussions resulted in a comprehensive communique, outlining key outcomes, and charting a course forward. This document identified responsible stakeholders tasked with addressing the challenges identified during the forum.

The National e-Commerce Forum and Exhibition had several objectives, including providing a platform for participants to exchange ideas, share best practices, and discuss lessons learned in navigating the challenges and opportunities within Ghana's e-commerce sector. Additionally, it sought to stimulate discussions among various sector actors, inspiring and expediting interventions in response to their needs. A crucial aspect was advocating for inclusive value chains and market systems to support women in e-commerce in Ghana.



GIZ, through the Pan-African E-Commerce Initiative-Boosting Digital Trade project, has been actively involved in promoting an enabling environment for e-commerce in Ghana. This regional project extends its activities beyond Ghana to Rwanda, Kenya, and the East Africa Community. With a focus on unlocking the economic potential of e-commerce, the interventions showcased in the 2nd National e-Commerce Forum and Exhibition emphasized the ongoing efforts to facilitate stakeholder interaction, understanding, and collaborative problem-solving in the sector.

CTO MIXER

The Ghana FinTech and Payments Association, Qucoon Limited, and AWS collaboratively hosted an Exclusive Mixer event for Startup CTOs on October 5th, 2023. This remarkable event, dubbed "the Cloud Tech Mixer", was spearheaded by Qucoon, a reputable AWS-certified partner. The event catered exclusively to Startup CTOs in Ghana, offering them a chance to explore the cutting-edge developments in cloud technology.

Attendees were able to learn about the latest innovations in cloud technology, connect with industry leaders, and acquire practical insights that could benefit their businesses. The event was a valuable opportunity for participants to adapt and excel in a rapidly changing world.

As a reliable AWS-certified partner, Qucoon Limited played a key role in creating an event that not only promoted knowledge sharing but also enabled meaningful relationships among Ghana's Startup CTO community. The Exclusive Cloud Tech Mixer was a memorable event that contributed to the ongoing advancement and dialogue within the tech ecosystem in Ghana.

GHANA TECH SUMMIT 2023

The 5th Annual Ghana Tech Summit which took place on December 14th as a virtual-only event.

Regarded as the largest tech conference in West Africa, the Ghana Tech Summit annually attracts thousands of global technology leaders, providing a platform for learning and business interactions. The 2023 summit was organized to usher in the "Ghana@100" Edition, exploring the future of Ghana in a post-modern world".

This summit is a 13-year initiative spearheaded by the Global Startup Ecosystem (GSE), recognized as the first and largest digital accelerator propelling 1,000 companies to market annually across 90 countries through entirely online means. The extensive GSE network hosts 25-30 programs yearly, spanning diverse tech realms such as Ai Tech Summit, Blockchain Tech Summit, Space Tech Summit, VR Tech Summit, Nano Tech Summit, Haiti Tech Summit, Her Future Summit, Africa Future Summit, Europe Future Summit, and more.

The event converged hundreds of entrepreneurs, investors, digital marketers, and creatives to collectively address humanity's greatest challenges through the lenses of technology and entrepreneurship. In the past, it drew participation from industry experts representing leading companies such as Google, Facebook, Uber, Twitter, IBM, and Microsoft and the 2023 edition equally rallied thousands for the next era of the internet, featuring keynote speakers such as Ndaba Mandela, Ben Horowitz (Investor in Twitter, Facebook), Tim Draper (Investor in Skype, Hotmail, etc.), Naveen Jain (Founder of Moon Express, Viome, etc.), Jovenel Moise (Current President of Haiti), Vicky Jeudy from Netflix's Orange is the New Black, and Vice Presidents and CEOs from Google, Facebook, Airbnb, Uber, and more.

GHANA HOSTED THE MAIDEN EDITION OF THE GLOBAL CYBER CONFERENCE

The inaugural Global Conference on Cyber Capacity Building (GC3B) took place in Ghana from November 29 to 30, 2023, at the Kempinski Hotel in Accra.

Coordinated by a collaboration among the Global Forum on Cyber Expertise (GFCE), the World Bank, the Cyber Peace Institute, and the World Economic Forum (WEF), this conference attracted over 800 cyber experts globally. Participants included cybersecurity professionals, leaders at high echelons, members of the international development community, and innovators.

Guided by the theme "Cyber Resilience for Development", GC3B was used as a platform for substantive dialogue and the exchange of inventive concepts among policymakers and industry leaders seeking to make substantial contributions to the global advancement of cyber capacity building.

The conference sessions revolved around four key pillars: fortifying international development against cyber threats, fostering collaboration to secure the digital ecosystem, enhancing cyber capacity for stability and security, and putting solutions into practical operation.

A noteworthy aspect of the conference was the unveiling of the Accra Declaration: a worldwide framework fostering collaborative initiatives to aid countries in bolstering their cyber resilience.

The GC3B exemplifies Ghana's commitment to building a robust and secure digital ecosystem.

UPCOMING EVENTS

10

FINTECH ISLANDS 2024

Fintech Islands 2024 is an upcoming global gathering set to unite leaders and innovators from the fintech sector in Barbados. Spanning three days, the event promises a dynamic blend of insightful talks, interactive workshops, networking opportunities, and entertainment, delving into topics ranging from digital banking and blockchain to AI and cybersecurity.

Distinguished speakers at the event include influential figures such as Brian Armstrong, CEO of Coinbase; Ngozi Okonjo-Iweala, Director-General of the World Trade Organization; Jack Dorsey, co-founder and CEO of Twitter and Square; and Richard Nunekpeku, Managing Partner of Sustineri Attorneys PRUC, a fintech-focused law firm.

Adding an exciting dimension, Fintech Islands 2024 will host a startup pitch competition, where 10 selected fintech startups can showcase their solutions to a panel of judges and investors, vying for a prize of $100,000. The event promises a unique and immersive experience, set against the breathtaking backdrop, rich culture, and warm hospitality of Barbados. The venue, the new Sam Lord's Castle Resort, epitomizes luxury, seamlessly blending history, elegance, and modern amenities.

Anticipated as one of the most promising and impactful events in the fintech sector, Fintech Islands 2024 provides a prime opportunity for learning, networking, and collaboration with top minds in the field. Reg-

TECH IN GHANA CONFERENCE

The Tech in Ghana Conference is an annual African technology event held biannually, once in London and once in Accra, Ghana. AB2020 hosts this event as a platform dedicated to fostering UK-Ghana collaboration and showcasing Ghana's vibrant tech ecosystem.

The 12th special edition is set to take place in Accra and London, with the Ghana session scheduled for March 19 & 20, 2024, at the Accra Digital Centre.

Tech in Ghana serves as a leading platform that bolsters Ghana's tech ecosystem by facilitating valuable knowledge sharing, global networking, and innovation.
It offers a space for knowledge exchange and provides an invaluable networking opportunity for the tech community, bringing together professionals from across the country and around the world.

The event promises attendees the chance to explore new trends, projects, innovations, and partnerships, gain insights into Ghana's tech ecosystem, and foster relationships with the country's tech professionals.

TECH IN GHANA

12TH ICT4D CONFERENCE

The 12th ICT4D Conference is set to make a return to Accra, Ghana, taking place on March 19th and 20th, 2024, with workshops scheduled for the day before and after the main event.

Known for its high interactivity and hands-on approach, this cross-disciplinary conference attracts approximately 700 technical advisors and senior executives hailing from public, private, and civil society organizations within the humanitarian and international development sectors.

This global conference delves into the transformative potential of Information Communication Technology for Development (ICT4D) and data innovations, showcasing their tangible impact on the lives of millions. It sheds light on how these technologies enhance the effectiveness of humanitarian relief, development, and conservation projects.

INNOVATE NIGERIA CONFERENCE & EXPO 2024

Prepare for the largest corporate innovation gathering in Nigeria, themed "Accelerate Business Transformation in the Age of AI." The event is scheduled to unfold at Landmark Event Center in Lagos, Nigeria, on February 6th and 7th, 2024. This unique conference zeroes in on corporate innovation and corporate venturing as viable capital sources for startups in Nigeria.

Given the current global market landscape and the challenges faced by Nigerian founders and those in other emerging markets while seek-

ing capital, the platform aims to foster startup-corporate collaborations, partnerships, and investments as a timely intervention to bolster the local startup ecosystem.
Anticipate engaging cross-sector discussions on the future of innovation and artificial intelligence (AI) during the conference.

Exploring how African companies can harness AI's transformative potential for societal good and global competitiveness, the event boasts an impressive lineup of speakers and spans over 12 industry tracks. With over 5000+ attendees and 10,000+ online participants, this groundbreaking conference is the first of its kind in Nigeria.

Attendees can expect a rich array of offerings, including conference sessions, exhibitions, exclusive tours, masterclasses, an investor dinner, innovation pitches, and more. The event's diverse tracks cover AI, Fintech, Foodtech/Agric, Healthtech, Proptech, Smart City & Infrastructure, Energy & Climate, Finance & Trade, Mobility, Ed-tech, Manufacturing & Automation, Future of Work & Talent, Civic Tech & E-Gov, and Corporate venture & M&A.

AFRICA TECH SUMMIT NAIROBI 2024

The 6th Africa Tech Summit Nairobi is taking place from 14th – 15th February 2024 and will connect tech leaders from the African ecosystem and international players under one roof.

Network with key stakeholders including tech corporates, mobile operators, fintech, Web3 ventures, investors, innovative start-ups, regulators, and industry stakeholders driving business and investment forward.

The 2024 edition will host four tracks – the Africa Money & DeFi Summit, the Africa Climate Tech & Investment Summit, the Africa Startup Summit, and The Africa Mobile & App Summit which drive interaction and a future line of sight across the track topics. The event connects over 1000+ industry leaders, 700+ companies, and 150+ speakers via four tracks plus workshops, expos, and multiple fantastic networking opportunities.

Publisher's Notice or Disclaimer ©

The information provided in this document does not, and is not intended to, constitute legal advice; instead, all information, content, and materials are for general informational purposes only.

Readers should contact their lawyers to obtain advice with respect to any particular legal matter. No reader or user should act or refrain from acting on the basis of information in this document without first seeking legal advice from his or her lawyers.

The use of, and access to, this document or any other resources by the firm does not create an attorney-client relationship between the reader or user and the firm, key contacts, and contributors.

All liability with respect to actions taken or not taken based on the contents of this document is hereby expressly disclaimed. The content in this document is provided "as is;" no representations are made that the content is error-free or may be affected by subsequent changes in legislation on the subject matter.

For more information,

visit
www.sustineriattorneys.com

or follow us on **@SustineriAttorneys**

or call **+233302553892**