DATA SAFEGUARD INC. WHITE PAPER

At Market Research Future (MRFR), we enable our customers to unravel the complexity of various industries through our Cooked Research Report (CRR), Half-Cooked Research Reports (HCRR), Raw Research Reports (3R), Continuous-Feed Research (CFR), and Market Research & Consulting Services.

MRFR team have supreme objective to provide the optimum quality market research and intelligence services to our clients. Our market research studies by products, services, technologies, applications, end users, and market players for global, regional, and country level market segments, enable our clients to see more, know more, and do more, which help to answer all their most important questions.

In order to stay updated with technology and work process of the industry, MRFR often plans & conducts meet with the industry experts and industrial visits for its research analyst members.

For more information kindly visit our website www.marketresearchfuture.com or contact us at info@marketresearchfuture.com

CONSUMER CONFIDENCE IN AN EVER-INCREASING PRIVACY REGULATIONS ENVIRONMENT

For the last four years, data privacy restrictions have become increasingly important. Consumers are growing increasingly worried about the disclosure and use of personal data, and trust is an important factor. According to a Salesforce poll, 48% of customers claimed they had lost trust in businesses owing to abuse of personal information during the epidemic. As the world grows increasingly technology driven and individuals worry more about their personal privacy, data privacy legislation are rapidly forming all over the world to protect the consumer.

In Europe, GDPR was the first major data privacy policy that went into effect in 2016. It was swiftly followed by the California Consumer Privacy Act (CCPA) and Brazil's General Data Protection Law (LGPD), all of which took effect in 2020. Other states and nations are swiftly following suit; for example, in the United States, Colorado and Virginia have approved privacy legislation that will go into force in 2023. While India is in the midst of enacting privacy legislation, the Joint Parliamentary Committee's report for the Data Protection Bill was delivered in December 2021. Growing rules, legislation, and compliance – as well as the increased danger of data breaches – are among the most significant concerns affecting data security in organizations today. All data must be recognized, classified, and safeguarded in order for an organization's data to be secure and comply with rules.

When the EU's GDPR and the California's CCPA were introduced several years ago, they caused quite a stir. (The California Privacy Rights Act, which went into effect on January 1, 2023, amends and expands the CCPA.) Multinational organizations now face a flood of disparate data protection and security laws from nations with competing interests. To navigate them successfully, one should begin planning now, taking into consideration several factors.

China's Data Security Law and the Cross-Border Data Transfer (CBDT) law under its Personal Information Protection Law are two examples of **proliferating rules.** This legislation already makes it risky to transfer or access personal data beyond China's borders. It necessitates completing a cybersecurity examination by March 1, 2023, with consequences for failure to do so. India, Brazil, and Russia are also exploring data protection legislation.

WHY DATA PRIVACY MATTERS IN 2023?

The regulatory focus on data, which was heightened in 2022, is expected to reach fever pitch this year. China's Cyberspace Administration recently issued privacy certification standards, while India's government recently published a draft of its data protection bill, which will likely be voted on in 2023. We may anticipate more from both of these countries, as well as data regulations from Russia, Ukraine, Brazil, Japan, and others.

Companies, aided in part by breakthroughs in artificial intelligence analytics, are discovering new ways to use the data they collect: to run more effectively, manage risks, improve customer services, build and support new business models, and so on. Data security is more important than ever. According to a recent IBM report, the average cost of a data breach across ASEAN countries is currently USD 2.87 million. The researchers considered not only technical expenditures, but also legal and regulatory costs, as well as brand equity loss, customer churn, and a drain on employee productivity. Above all, the irreversible harm to the organization's reputation, eroding stakeholder confidence, and jeopardising data privacy must be considered. More and more businesses are realising that incorporating privacy into their products and services from the start is not only the moral thing to do, but it can also be extremely profitable. For instance, Singapore has promoted the use of a privacy-by-design approach to ensure the proper use and protection of personal information.

The growth of privacy-focused technology will come next. As customers become increasingly worried about their online privacy, there will be a boom in demand for privacy-focused solutions. Secure chat applications and browsers, as well as virtual private networks (VPNs) and encrypted email services, are examples. It's crucial to remember that, while these technologies can help companies safeguard their data, they're not a panacea. Companies must be watchful and take precautions to protect their data. Regulations are also becoming more stringent. Governments throughout the world are taking note of the rising concern over data privacy and are beginning to take action. Since the European Union's General Data Protection Regulation (GDPR) went into effect in 2018, there has been a continuous increase in additional limitations. This trend is expected to continue as more countries seek to enact data protection rules.

More transparency is also essential. The growing awareness of the need of protecting personal information, as well as the necessity for companies to be more accountable for their data collecting and use policies, is driving the trend towards more transparency in data privacy. By providing individuals greater control over their data in 2023, corporations will become more open about their data practices. Individuals should be able to view, modify, or delete their personal information, as well as opt out of some forms of data collecting. This is a win-win situation for both customers and businesses since it creates confidence and a feeling of openness and responsibility.

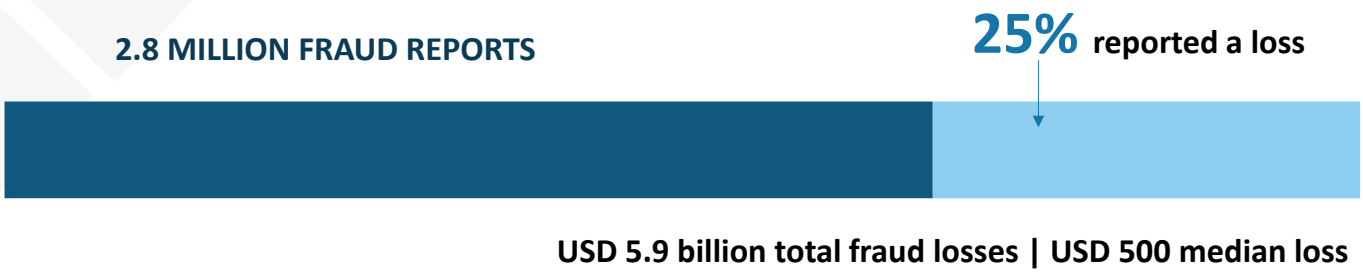
IMPACT OF DATA BREACHES

The ramifications of data breaches for corporations are serious and growing. This is mostly due to the increasing regulatory burden associated with notifying individuals whose data has been hacked. Notification procedures and sanctions for firms affected by a data breach vary by jurisdiction, both inside and outside of the United States and Canada. Businesses that suffer a data breach involving their customers must determine where their clients live and which regulatory entity has jurisdiction. Rules specify the types of data that must be disclosed following a breach, as well as who must be contacted, how the notification must be carried out, and if certain authorities must be alerted. Personal, financial, and health data breaches are often subject to notification obligations, however specific definitions vary by state. Businesses undertaking international commerce may have consumers in several jurisdictions and must meet a number of standards. The costs of such a procedure, including legal fines, potential reimbursement for damages, and any related litigation, might be too expensive for certain businesses. Data breaches involving different sorts of data can have a significant impact on a company's reputation and economic status. In addition to contractual requirements, a data breach might jeopardize a company's planned sale, as happened recently with Verizon's acquisition of Yahoo.

The fact that authorities look beyond the continuous management of personal data adds to the issues as businesses respond to new privacy rules. Data leaks and breaches are becoming increasingly regular. As a result, regulatory organizations scrutinize not just how a corporation maintains personal data prior to a breach, but also how it responds thereafter. Follow-up audits determine if a corporation improved the practices that resulted in the data breach. Authorities apply higher fines if they believe the company's efforts to avoid the original breach and future incidents were insufficient.

In 2021, the Consumer Sentinel Network took in over 5.7 million reports within US, an increase from 4.7 million in 2020.

- ***Fraud: 2.8 Million (49% of all reports)***
- ***Identity Theft: 1.4 Million (25%)***
- ***Others: 1.5 Million (27%)***



Source: Federal Trade Commission Data 2021

In 2020, there has been a flurry of frauds and fraud activities. Data breaches have exposed personally identifiable information (PII) of customers at an alarming pace, placing over 300 million people at risk of identity theft and fraud. Cybercriminals are also concentrating their efforts on more lucrative hacks such as ransomware, credential stuffing, malware, and VPN exploitation. These tactics not only expose consumer information to the risk of being sold on the Dark web, but they also come at a high cost to organizations, particularly Financial Institutions (FIs), which are targeted by cyberattacks **300 times** more frequently than other industries due to the sensitivity of the personal information they store.

Data breaches are an everyday occurrence in both our personal and professional life. Therefore, whether we shop at Walgreens or Barnes & Noble, bank with Capital One, communicate with T-Mobile or Zoom, or have Tufts Health Plan medical insurance, if your data is included as part of the transaction, it has the potential to be exposed. The Dark Web — an unsearchable part of the Internet — is proof of this. Inside those unindexed sections of the Internet, there is a buyer waiting to enjoy the benefits of any stolen piece of your identity. But not every breach in the news is reason for concern, and it's critical to avoid breach fatigue by understanding what information to look for when breaches occur.

PRICE OF YOUR IDENTITY

- Passport - $18
- PayPal Login - $11
- Driver's License -$28
- Online Banking Details - $100
- Credit Card Details - $32
- Social Media Login - $8
- Full Online Identity - $1,200

Source: Dark Web Market Price Index 2021

SYNTHETIC IDENTITY FRAUD: THE EMERGING THREAT

Investigating the data trails people leave behind can assist banks in determining if their clients are real or not, hence reducing losses from this rapidly rising financial crime. Because of their investments in technology, banks have been considerably more adept at avoiding many sorts of fraud, but crime has developed in response. Many fraudsters now employ bogus, synthetic Identities rather than a stolen credit card or identity (ID). Indeed, synthetic ID fraud is the fastest-growing kind of financial crime in the United States, accounting for 10 to 15% of charge-offs in a typical unsecured loan portfolio, according to our calculations. Synthetic ID fraud has also lately been recorded in other countries. Worryingly, far larger losses are amassing behind these Identities like buried time bombs.

SYNTHETIC IDENTITY FRAUD

The use of a combination of personally identifiable information (PII) to create a person or entity for the purpose of committing a dishonest act for personal or financial benefit.

A synthetic identity fraud (SIF) profile is basically a fictitious persona made up of identification pieces (usually taken from actual persons) such as a name, social security number, and address. In order to assist banks in standardizing SIF reporting, the Federal Reserve developed the following definition in April 2021. While the definition is simple, the method of creating SIF profiles is very complex, requiring automation and machine learning.

Although SIF shares certain characteristics with "conventional" identity theft, its origins, behavior, and impact are fundamentally distinct from previous generations of financial crime.

SCALABILITY	▪ SIF has become one of the fastest-growing financial crimes by bringing scale to fraudulent theft. ▪ Criminals collect identification components from the dark web and create millions of fake profiles using automation.
EVASION	▪ Criminals use a thorough grasp of the US payment system in conjunction with sophisticated software to construct profiles that are exceedingly tough to detect. ▪ In contrast to typical identity theft, there is no victim who will detect a fake charge and notify their bank.
VIRALITY	▪ Once a SIF profile has established a moderate amount of credit, it normally establishes five trading lines at various institutions. ▪ Criminals are on their way to establishing their next set of synthetic identities by "piggybacking" extra SIF profiles to an account as approved users.
HARM	▪ The revenues of cyber fraud are funneled towards weapons proliferation, human trafficking, and other severe crimes by global fraud organizations and rogue regimes.

A BRIEF HISTORY OF SYNTHETIC FRAUDS

In the early 2000s, fraud investigators began to identify trends in credit card applications where the applicants' social security number (SSN) did not match the name to which the card was issued. While there was no official term for it at the time, fraud historians consider secured credit cards as the first assault point for synthetic identity fraud, while others see patterns of Frankenstein identities mostly in the unsecured credit card and telecommunications industries. But Frankenstein identities erupted onto the scene, and a huge number of fraudsters began creating new credit card accounts, which they utilized to swiftly rack up balances and then leave without ever making a single payment. The issuing banks wrote off the great majority of these charge-offs as credit losses. This technique evolved as criminal actors demonstrated more patience by making on-time payments for card transactions. They would then charge the card past the credit limit and "bust out" (max out the card without ever paying another dime), allowing them to accumulate illicit proceeds more than the credit limit.

To build an identity, legitimate information is blended with fraudulent information in synthetic identity fraud. The resulting artificial — or synthetic -identity has enough verifiable information to appear authentic, allowing it to be used to create bogus accounts, make fraudulent purchases, and swindle shops, government organizations, and financial institutions.

IDENTITY THEFT BY NUMBERS

RIGHT NOW – 2 new victims every second

PREVALENT – 1/3 of U.S adults victimized, 65% of breach victims experience ID theft, and 32% of families have been affected by identity fraud

COSTLY – average $1,343 per incident

REPETITIVE – 20% of victims experience ID theft more than once; 73% of victims have fraudulent accounts opened at financial institutions where they already have accounts

CONCEALED – takes 3 months to 3 years to discover

ALL AGES – 1 million+ children are victims annually, mostly under 8-years-old

GROWING SIF LOSSES

Synthetic identities account for a small percentage of consumer accounts yet are responsible for enormous amounts of theft. According to FiVerity's Cyber Fraud Network, SIF losses among US FIs increased to $20 billion last year.

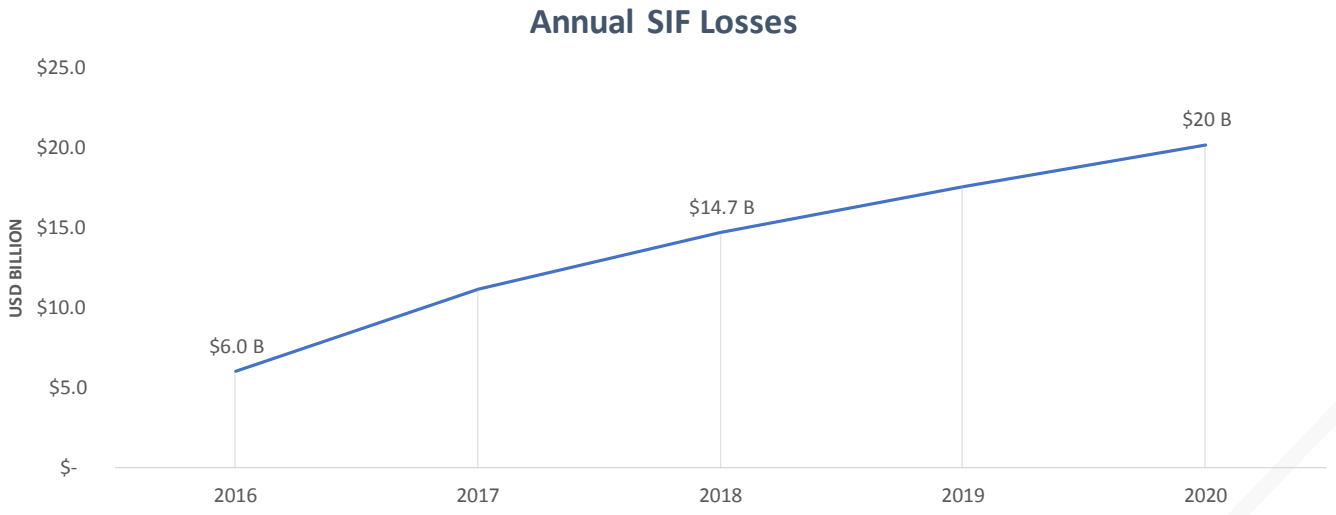
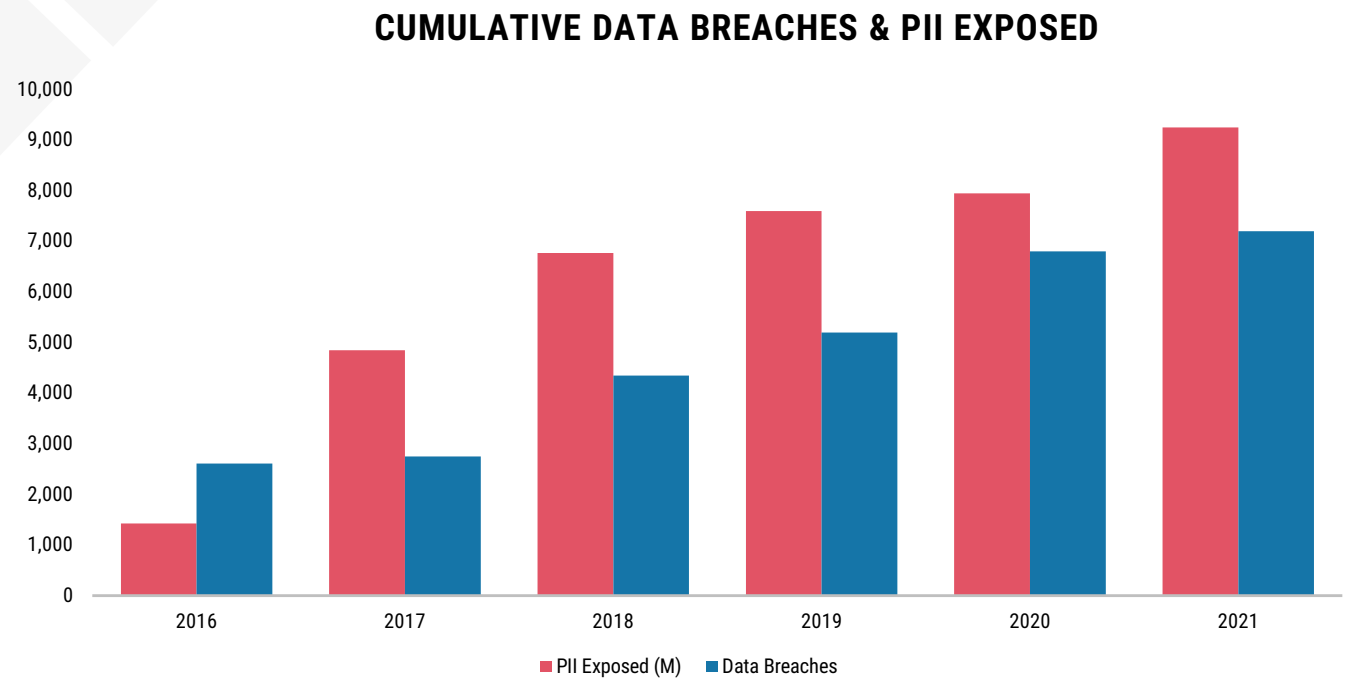


FIGURE 1 CUMULATIVE DATA BREACHES & PII EXPOSED (2016-2021)



Source: Identity theft resource center (January 2021), 2020 in review: Data Breach Report

Identity thieves can not only obtain access to checking, savings, and 401(k) accounts, but they can also use this information to piece together new phony identities, which costs US lenders between $10,000 and $15,000 each occurrence, or $6 billion yearly. Data breaches can have a substantial impact on corporate productivity and revenues. Employees who need to authenticate the integrity of their identification — or who must go through the arduous process of mending a stolen identity — are expected to be out of work for six months and 100 to 200 hours. This has a huge impact on employees' mental states and can lead to health problems such as considerable personal stress, persistent anxiety, and dissatisfaction. Employees may be on edge and wary of how effectively they secure their personal data, causing your clients' business outcomes to suffer. Data breaches can have a substantial impact on corporate productivity and revenues. Employees who need to authenticate the integrity of their identification — or who must go through the arduous process of mending a stolen identity — are expected to be out of work for six months and 100 to 200 hours. This has a huge impact on employees' mental states and can lead to health problems such as considerable personal stress, persistent anxiety, and dissatisfaction. Employees may be on edge and wary of how effectively they secure their personal data, causing your clients' business outcomes to suffer.

The unfortunate truth: **HACKERS MAKE A LOT OF MONEY FROM SMALL BUSINESS IDENTITY THEFT. These attacks come at a high cost, with SMALL BUSINESSES PAYING MORE THAN $200,000 EACH FRAUD INCIDENT.** Furthermore, they can harm employees' and company owners' reputations and generate stress.

CHALLENGES IN MEASURING SIF

- **Stealth -** Unlike ransomware, which requires the targeted company's attention, SIF only succeeds when it goes undiscovered. SIF operates under the radar by posing as actual low-credit applicants, asking modest loans, and making timely payments if accepted. SIF accounts are frequently kept secret even after they have been compromised, since FIs ascribe the theft on poor underwriting.
- **Reporting -** Apart from the apparent difficulty that banks cannot disclose a crime of which they are unaware, procedures for recognizing and reporting SIF have yet to be created. Because SIF is a relatively new offence, there is no official database in place to catalogue each instance, such as the FTC's Sentinel.
- **Evolution -** Criminals have made SIF programs more difficult to detect over time by utilizing AI and machine learning. AI systems learn from loan applications that are accepted and refused, which give vital input to machine learning models. This feedback loop effectively assists fraudsters in identifying the thresholds for each of the older systems' fraud detection criteria and developing new profiles that are even better at dodging them.

According to McKinsey & Company, synthetic ID fraud is the fastest increasing financial crime in the United States, accounting for up to 15% of charge-offs in typical unsecured lending portfolios. The insidious nature of synthetic ID theft is that it is extremely difficult to detect—even after massive financial losses have occurred. Financial institutions (FIs) are frequently unaware that they have been targeted by operators using synthetic ID fraud, instead presuming credit losses are simply due to clients being unable or unwilling to repay and then writing off the losses in accordance with usual practice. The fact that these fake consumers appear to pass the initial identification sniff test is simply one of the many issues that contribute to significant financial losses. The other is that synthetic ID fraudsters can spend up to five years to cultivate Frankenstein account identities, creating confidence with financial institutions before using what is known in the industry as a "bust out," in which credit lines are maxed out and then abruptly abandoned.

GLOBAL PROBLEM

Data Privacy

- **Enterprises are unable to protect their customer's sensitive and personal data(PII) and meet data privacy compliance.**

Global penalties are over $10 billion and increasing.

Synthetic Fraud

- **Significant financial losses are being incurred with the advent of synthetic fraud; the fastest growing financial crime inflicted using Frankenstein identities.**

Global synthetic fraud losses are over $1 trillion and increasing.

Data Privacy Fines

300+ companies fined for non-compliance in 30+ countries.

Company	Fine
Amazon	$888M
British Airways	$26.5M
Marriott International	$23.9M
Ticketmaster	$1.7M
Salesforce + Oracle	$10B

Additional companies fined in the past three years

Equifax, Home Depot, Capital One, Uber, Morgan Stanley, Tesco Bank, Target & Anthem have been fined significant amounts

Synthetic Fraud Losses

Category	Loss
Child victims	$2.7B in 2017 (CNBC-4/24/2018)
Synthetic Identity Fraud(CC)	$800M in 2017 (CNBC-6/7/2018)
Synthetic Identity Fraud(CC)	$1.3B in 2020 (CNBC-1/16/2020)
Synthetic Identity Fraud	$56B (CNBC-3/23/2021)
Synthetic Investment Fraud	$100M (CNBC-3/29/2021 (Robinhood/TD))
Synthetic BNPL Fraud	$6.5B (CNBC-11/28/2021 BNPL)
Synthetic Identity Fraud	$100B (CNBC-12/21/2021-Covid Relief Fund))

Attacks are showing up Paycheck Protection Plans, Medical Fraud, M&A Fraud, Unemployment Insurance, Wire Transfers, Social Security and Insurance Claims.

When the risk of false identification grows, it is no longer as simple as obtaining various kinds of identification to authenticate an identity. Companies must comprehend these new threats, know where to go for solutions, and revise their fraud-prevention procedures. Since fraudulent accounts seem real, conventional fraud detection techniques may miss synthetic identities. Rather of abandoning existing fraud protection systems, experts advise maintaining them while supplementing them with new security measures.

Synthetic identity fraud accounts for up to **20%** of credit losses and costs lenders roughly **$6 billion** annually.

So, how does one identify synthetic fraud?

Experts say that investigators should presume that every identification is potentially fraudulent and act accordingly. They should consider whether they have access to a complete repository of public records in order to validate that their subject's full data exists in multiple data sets, such as all three credit bureaus, utility files, work records, and bank account records, to name a few examples of sources evaluated by businesses performing identity checks today. Investigators should determine if they are acquiring enough personally identifiable information to completely authenticate the subject's existence in records. It is not sufficient to have only a subject's name and date of birth. Searches should provide their phone number, address, email address, and so on.

Researchers should try to determine how long the subject's identity has existed in the data to determine whether their subject is a newly generated identity. They should see whether comparable identities are found in public record databases when they conduct searches on the issue. Investigators should seek for indicators that the target person or business was created when evaluating search results. Simply said, as artificial intelligence technologies and tools improve in completing identity verification and know your customer checks, compliance professionals should leverage the capability they provide to dive deeper, supply up-to-date data, and weed out irrelevant discoveries.

CAN AI SOLVE THESE ISSUES?

The European Commission released its draft suggested rule on April 21, 2021, approximately five years after the EU GDPR went into effect. It provided a set of guidelines for the usage of AI systems and the data they collect. This ruling, like the GDPR, would apply to firms based in or linked with the European Economic Area. While dealing with compliance, the authorities set out to avoid many of the regular loopholes. These, for example, apply to AI information used in the EEA even if it is acquired and created outside the EU.

As organizations expand, their workforce becomes more global, diverse, and distributed, and enterprises adopt new cloud, on-premises systems, and deploy intelligent devices, the old model of static policies based on a fixed set of contexts (for example, in the case of access management, Time, geo-location, device OS, and so on) begins to fail. Policies become more numerous; context does not account for user history; and protecting against future attack routes becomes difficult. Here is where AI-powered security begins to truly shine. These security systems use previous actions, events, and breaches to construct their own models independently and without continual human monitoring. They are intelligent in the sense that they can make judgements on their own, and perceptive in the sense that they can look at data extensively and profoundly. They are easy to maintain and proactive in nature since they continually learn and adapt by using fresh data. This field has advanced rapidly in recent years and is crucial in the identification and prevention of assaults and breaches. Some of the use cases are described here.

AI and machine learning have been utilized extremely well in filtering through massive volumes of data to create identity profiles, which are subsequently used to detect not only abnormal but also malevolent conduct. Based on this, administrators can install "adaptive" authentication rules, such as just-in-time privileges/rights, to reduce the risk of access-related assaults, which are vulnerable to permanent/longer-lasting policies.

AI is all about data quality, comprehensiveness, and data science, which determines how successfully it is examined (also known as the Model). Quality relates to how thoroughly the data has been cleansed, processed, and wrangled for downstream consumption. The tool's comprehensiveness relates to the numerous settings and sources from which it collects data. When a user accesses an app, he or she uses an endpoint device (such as a mobile phone) from a location, navigates a network with firewalls, is authorized, takes a role, and then conducts some action. A competent IAM platform can collect data from all of these contexts (device, location, time, network, directory services, roles-based access, and so on) and then "learn" about access patterns over time. The lessons learned are then applied to essential resources via adaptive/proactive policies. This method goes a long way towards preventing data breaches.

Contrary to its core premises of total autonomy, AI is really going from isolated, in many cases unsupervised learning to hybrid - mixing human intellect and inputs (supervised) alongside unsupervised. This leads to more strong policies, which implies fewer false positives!

To decrease the transmission and severity of breaches, artificial intelligence is being utilized to manage the configuration of adjacent and damaged systems. Notifications and mitigation procedures are automated (for e.g., blocking access or reducing to least privilege). RPA (Robotic Process Automation) also improves efficiency in this field. AI applications for role engineering and identity governance. Some of these include automated separation of tasks implementation and risk-aware access workflow management.

DATA SAFEGUARD

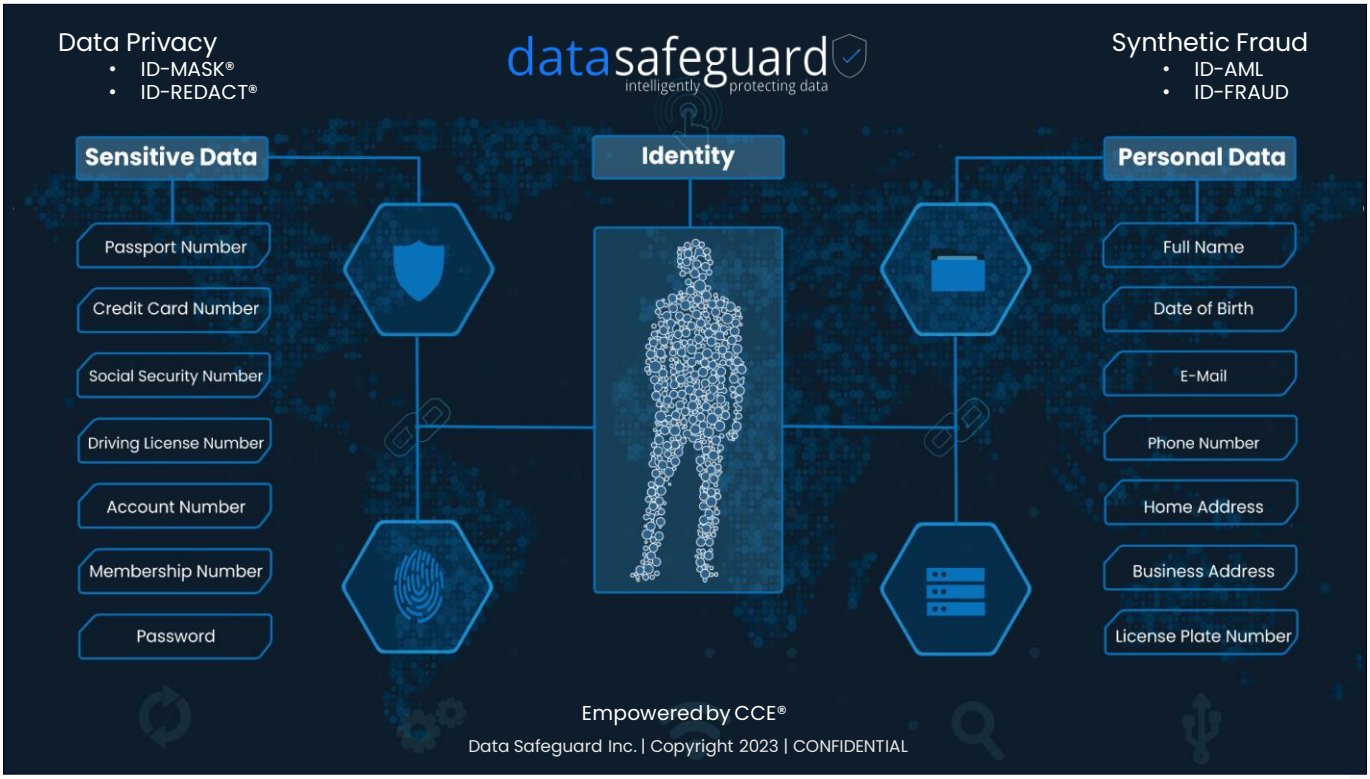
Data Safeguard is an Artificial Intelligence company with Data Privacy and Synthetic Fraud solutions. Its solutions are enterprise class, component modeled, and architecturally scaled to meet global, federal, and state-level compliance mandates as well as prevent significant financial losses caused by Frankenstein identities.

Data Safeguard solves Data Privacy and Synthetic Fraud challenges that were previously unsolvable and humanly impossible. It's AI/ML based solutions employ advanced models and algorithms with supercomputer-based data accelerators that improves efficiency and accurately control predict PII data elements in vast amounts of in complex data environments. Company's SaaS products are available on 5 major channels namely: Enterprise on Premise, Enterprise Cloud, Customer API, Marketplace API and eCommerce platform covering global as well as individual customers.

Data Safeguard's products ID-REDACT®, ID-MASK®, ID-FRAUD, ID-AML are empowered by its patent pending platform – Cognoscible Computing Engine (CCE®). CCE® is built with models and algorithms that harnesses the hyper-accuracy power of artificial intelligence and machine learning technology to make its products most effective Data Privacy and Synthetic Fraud solutions in today's challenging market.

Data Safeguard continues to gain market share and continues to actively hire staff at its locations across the globe to prepare for immediate future growth.

FIGURE 2 DATA SAFEGUARD INC.



9th | Data Safeguard Inc. was ranked 9th in the top 50 thought leading companies in the Artificial Intelligence space for 2023 by Thinkers360

THE DATA SAFEGUARDERS

A global team of seasoned business and technology professionals with an enriched experience of 300 years. The team has a unique blend of entrepreneurship, product development, customer implementation management, and other skills. The team has been collaborating to respond to the Universe's demand to tackle ever-changing data privacy and synthetic fraud concerns. Our passionate team members have held VP through C-level positions and are experts in the financial services, healthcare, retail, technology, telecom, cloud services, logistics, supply chain, and public sector domains' business and technology ecosystems, complex customer environments, and regulatory compliance landscape. The team has global expertise in data privacy, compliance, governance, confidentiality, and protection. Years of industry experience in some of the world's best firms in the financial services, healthcare, retail, and technology segments in the areas of data privacy, as well as synthetic fraud, risk management, artificial intelligence, and machine learning, led us to believe we can resolve the Data Privacy and Synthetic Fraud challenges.

The solution was named a 2020 Banking Tech Awards Finalist (Best Banking Tech Solution category) and was praised for being a game changer in assisting clients with data redaction compliance.

CONCLUSION

Financial crime is growing more sophisticated and prevalent as the digital economy and the ramifications of the data-first society evolve. Synthetic identity theft, one of the fastest growing types of financial crime in the United States, is a particularly sophisticated security problem that is contributing to the rising risk environment and redefining financial services businesses' technical investment objectives (FSOs). Fraudsters who do not appear to be fraudsters provide a problem to businesses all over the world. These synthetic identities not only appear authentic in many ways, but they also contain characteristics of legitimate clients. Companies must grasp the difficulties and limits of exclusively examining static identification features in order to combat this developing and ever-growing class of fraudsters. Businesses may better prepare for synthetic identity theft by seeing each client or transaction through a multidimensional lens that incorporates dynamic identity qualities and their links to one another. Businesses must also examine their fraud-prevention systems comprehensively to verify that no holes exist for criminals to exploit.

There is no question that synthetic identity theft is a rapidly expanding crime committed by unscrupulous actors who blend genuine and fabricated personal information to create an authentic-looking digital identity. Data breaches are not limited to businesses in the United States; businesses all around the world confront similar difficulties. Personal information disclosed in data breaches is frequently sold on dark web marketplaces, where fraudsters can purchase the data required to perform synthetic identity theft. At the moment, the most promising method of combating synthetic identity theft is to use advanced Identity Verification software integrated with AI technologies, which validate ID papers and persons using facial recognition.

DATA SAFEGUARD FOUNDER AND CEO

Data Safeguard's founder and CEO, Sudhir Sahu, a serial entrepreneur with IT engineering and MBA background, founded the company in June 2021. During the pandemic, when companies were shutting down and economy wasn't supporting business growth, Sudhir partnered with his co-founders (Elliott Lowen, Keertana Suresh, Lee Nocon, Praful Parekh and Swarnam Dash) to start a journey that seemed difficult every step along the way.

Sudhir says Data Safeguard was started to enable global as well as small and medium-sized customers to meet Data Privacy compliance, avoid paying hefty penalties and deter the hackers from stealing PII data elements and creating havoc in consumer's lives. Global penalties are over already $10B and increasing, Data Safeguard is the global solution to this global challenge.

Sudhir takes special interest in the Synthetic Fraud solutions to protect the financial institutions from significant losses caused by Frankenstein identities. Global Synthetic Fraud losses are over a trillion and increasing, Data Safeguard is the global solution to this global challenge.

Sudhir traveled to different parts of the world to gain first-hand experience of the hacker community, understand their usage of technology to collect and mine personally identifiable information, combine different data elements to create Frankenstein identities and mode of business operation. He is committed to detering hackers from stealing personally identifiable information and preventing financial crimes.

DISCLAIMER

Market Research Future strategic analysis services are limited publications containing valuable market information provided to a select group of customers in response to orders. Our customers acknowledge, when ordering, that Market Research Future strategic analysis services are for our customers' internal use and not for general publication or disclosure to third parties. Quantitative market information is based primarily on interviews and therefore, is subject to fluctuation.

Market Research Future does not endorse any vendor, product or service depicted in its research publications. Market Research Future strategic analysis publications consist of the opinions of Market Research Future' research and should not be construed as statements of fact. Market Research Future disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Market Research Future takes no responsibility for any incorrect information supplied to us by manufacturers or users.

For information regarding permission, contact:

Tel: 1-646-845-9349

Email: info@marketresearchfuture.com