AnimaTech®
A Revolution In Biometrics

Investors 2018 - Teaser

Legal Information

The information contained in this document is strictly confidential to **AnimaTech LTD** and must not be copied, reproduced, distributed or transferred in any form to any other person or used for any purpose inconsistent with the purpose for which it has been delivered.

While this document has been prepared in good faith, no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by **AnimaTech LTD** or by any of its officers, employees or agents in relation to the adequacy, accuracy, completeness or reasonableness of any assumptions, data, parameters or other content of this document.

This document does not constitute an offer or invitation in respect of any sale or purchase of securities and no information set out or referred to in this document shall form the basis of any contract. This document has been delivered to interested parties for information only and **AnimaTech LTD** gives no undertaking to provide the recipient with any access to any additional information or to update this document or to correct any inaccuracies in it which may become apparent.

By accepting this document, the recipient acknowledges and agrees to be bound by the foregoing limitations.

Executive Summary

Biometrics in Identity Verification

Identity verification has become **a central necessity** in societies and economies of today. This demand has been driven by social and technological changes ranging from the rise of e-commerce, cloud data storage, anti-terror policing and border control, to healthcare and the rapid rise of gaming entertainment.

Over **15 million** consumers are **victims of identity theft or fraud** every year in the US alone, and values of over **$16 billion are stolen**. Corporations targeted had their **share price negatively impacted** and out of 65 companies evaluated the breach cost shareholders over **$52 billion**.

Consequently, **identity theft** has become big business in line with the rise of the Internet of Things (IoT). As the “eyeball test” and “basic paper ID” cannot be used, knowledge-based authentication (KBA) was originally adopted, relying on passwords and PINs.

In attempts to further improve **security protocols**, two-factor authentication (2FA) was developed, which mainly relied on a second device to authenticate the user. However, passwords and pins can be cracked, forgotten, shared inadvertently or lost, making KBA and 2FA approaches no longer highly secure.

Attention, therefore, has shifted to **biometrics** as a way of authenticating identity using an individual’s specific and unique traits and features. Biometric technologies developed until now include face, fingerprint, iris, palm, vein and voice.

Today, biometrics lie on the critical path of the hundreds of billions of dollars in commerce, insurance payments and premiums, averted losses from identity crime, the security of borders and national interests.

Executive Summary

Life Signs – The New Frontier

The **biometric technologies** developed to date – including face, fingerprint, iris, palm, vein and voice all represent a significant improvement in the security industry. However, they each suffer from several imperfections: some technologies are extremely expensive, some are not portable, others are not sufficiently accurate or quick and so forth. The security industry continues to search for a **solution** which will meet its needs but without these drawbacks.

AnimaTech has a new set of biometrics in various phases of development which provide the level of security required by today's societies and economies. This is the set of signals emitted by the body that can uniquely identify an individual – the set of "**Life Signs**".

Medical studies have proved that an individual emits signals in patterns which are **unique** to each individual. Life Signs are, by definition, **live biometrics**, which make them ultimately **impossible to fake**, resolving a significant issue suffered by all the other static biometrics. This, together with a plethora of other unique features, makes AnimaTech's technology **the next-generation biometric.** The AnimaTech solution **combines Life Signs** with other established biometric technologies, most notably **face recognition**, with **powerful algorithms** thereby providing a multi-layered approach which 'ticks all the boxes'.

The technology is also **compatible** with the vast majority of existing systems. Therefore, AnimaTech's solution will provide businesses and other users with a **straightforward** and **cost-effective transition** to a superior technology. To create a further enhanced multi-technology platform, AnimaTech will also combine its multi-layered recognition system with behavioural recognition technology.

The potential number and variety of situations for the **application of AnimaTech's technology**, and therefore the scope for further **development** and **exploitation** of the technology, is vast.

Executive Summary

AnimaTech – Value Proposition

AnimaTech's **unique technology** dramatically advances verification accuracy and reduces fraud risk. **AnimaTech's platform will offer customers the ability to use AnimaTech's technology alone or in conjunction with other verification technologies**.

AnimaTech is entering **Phase 3** of corporate and product development, which will include completion of Proof of Concept and a multi-product development program as well as targeted business development. Phase 1 included core technology development, Phase 2 included development of early product and concept, as well as the establishment of a Service Centre for business development and consulting services.

Initial **adoption of AnimaTech's Life Sign technology is easy** as it does not require development of new sensory reading hardware. For instance, existing cameras on smartphones and laptops are sufficiently sensitive to make readings, strike partnership agreements, begin commercialising the technology and generating initial revenues.

While the firm has a patent strategy in place, the best protection for the firm's intellectual property is **rapid commercialisation**. The compatibility of AnimaTech's technology with the vast majority of existing systems will simplify and speed-up commercialisation.

The firm is currently **retained** as an **advisor** to businesses in target industries**. Early revenue** is currently coming from consulting services, and revenue generation from the core technology is expected within 12-18 months after funding through licensing fees and transaction processing volumes.

The database of individuals' Life Sign readings coupled with AnimaTech's token and the ability to use it in conjunction with other identity verification techniques are together **exponential value creators**.

Executive Summary

AnimaTech – Investment Proposal

Technical team. An experienced and committed team of scientists from the technology and security business sectors have a deep knowledge of the medical basis and data analysis behind Life Signs. A core skill of the group rests in their extensive experience in cyber security and in data cleansing, data processing and algorithmic application development. The team is led by the inventor of the technology, also a founder and co-owner of AnimaTech.

Management team. A multi-disciplinary management team has been assembled to bring the technology and platform to market. The team includes a founder and co-owner of AnimaTech.

AnimaTech's technology. This is compatible with the vast majority of existing systems and therefore it will be straight forward for businesses to include this in conjunction with their incumbent technologies or adopt it standalone.

Patent strategy and IP Protection. A patent strategy has been devised to protect the technology and its applications. The first patent is currently pending in the US. Others are in the pipeline.

Business strategy. A commercialisation strategy has been identified, initially based on developing applications in a few key industries through partnerships with leading industry players. The firm has begun operations through consulting assignments in target industries through which its core technology will be positioned. The technology will produce multiple sources of revenue spread across several industries. Initially revenue from the core technology is expected from the broad payments processing industry and security enablers of commercial platforms.

Funding. AnimaTech is now **seeking €2m** through an equity issue, followed by one or two further equity raises of up to €20m in total, to accelerate its activities by hiring more scientific, technical and commercial staff, enhance the product suite, expand marketing and product positioning and strike distribution partnerships.

Technical Team

Based in Nice, France – Key Members Led by Frédéric Aime

Frédéric Aime French

Founder & CTO

Frédéric is one of the founders of AnimaTech. He has a profound knowledge of the IT industry with extensive experience in several fields including signal processing applied to cardiology, artificial intelligence and large database operations. He is a cyber security expert and has worked with large companies in the protection of data and processes. He has many years of experience leading and motivating technical teams. He has worked at IBM, Amadeus, Sun Microsystems, Oracle, Orange, Gemalto, Google, Airbus and Air France. He graduated from the University Institute of Technology (IUT) and the University of Sophia Antipolis in Nice.

Aurélia Bordas French

R&D Director

Aurélia is one of the founders of AnimaTech. She is a veteran of the telecommunications industry with more than 15 years of experience in project management, team leading, patent filing and operating in major security environments. She is expertly versed in project management in the IT industry and is fluent in the needs and quality processes of a software business. She has previously worked at France Telecom, Mctel, Gemalto and the French National Education. She graduated from the University Institute of Technology (IUT) and the University of Sophia Antipolis in Nice.

Vincent Vignaux French

Technical Director

Vincent is a technical leader, computer scientist, and software architect of many years' experience. His specific experience includes complex projects such as nuclear, hydraulic energy developments included with medical and financial aspects, 3D development display in Google maps and TGV Internet provision using cybersecurity skills and deploying development infrastructures. Amongst others, he has worked for 8 years for Thales Company. He graduated from the Polytech Sup Engineering Institute.

Alexis Rabeuf French

Technical Director

Alexis is a certified IT technician. He has worked for several small to mid sized companies based in Monaco as an external IT consultant, and for 12 years in the energy industry managing technical needs for shipping and trading companies. He holds a degree in Network Design and Administration.

François Zannin French

Technical Director

François is an engineer with extensive technical and customer experience. After several years at Thomson as part of the real-time software development team for the French Navy, he worked for 10 years in the R&D department of Hewlett Packard's core telecom. He then took his expertise to Mctel and Gemalto and developed the Telecom equipment manufacturer business in the areas of management and security of network infrastructures and services provided by Telecom operators. He graduated from the Engineering School in Brest.

Charles Saad French

HR Director

Charles has been working in the human resources and recruitment industry for nearly 15 years. During this time he has developed strong communication and interpersonal skills in negotiation with major companies like Econocom, SII and Proxiad. He has also gained a specific knowledge of the engineering market in France. He is a graduate of the University Institute of Technology (IUT) in La Garde, the University Of London and SUPDECO in Montpellier, France.

Business Team

Based in London, UK- Key Members Led by Sebastian von Bulow

Sebastian von Bulow — Swedish/American

Founder & CEO

Sebastian is one of the founders of AnimaTech. He has extensive experience building and launching business ventures and concepts in the technology and media sectors. He started his first tech based company with a Nordic platform in the 1980's. Sebastian is skilled in product planning, user experience, consumer marketing, product management. He has experience in quality assurance testing and is a branding analysis expert. He has previously worked for international organisations including Ernest & Young and Bang & Olufsen, focusing mainly on international business in New York and Moscow. He holds a B.A in international Business & Marketing from Sweden and New York, USA.

Vinayak Bhattacharjee — Indian

Executive Chairman

Vin is an entrepreneur with extensive experience in the finance industry. He has held prominent management and leadership roles in large financial institutions. During his leadership periods at Barclays and State Street, he created the hugely successful exchange traded funds market in Europe by launching the iShares range of ETFs and then heading the SPDR ETF business in EMEA. Through his personal and professional private equity practice, he has built and advised businesses in financial services, technology and internet ranging from internet gaming in Scandinavia to telecommunications support services in India. He has authored articles on behavioural economics and has an MSc in Economics from London University.

Per Bergkvist — Swedish

CFO

Per has over 20 years experience in international finance gained in a variety of sectors including IT, infrastructure, media and banking. He has held senior positions in global organisations, including ABB and UBS, as well as in corporate finance and private equity firms such as Alfa Capital in Russia. He is also an entrepreneur who has been involved in a number of start-ups and has a solid experience in growing and developing new ventures. He has spent many years in London, New York and Moscow, and holds a MSc in International Business and Economics from Lund University in Sweden.

Matteo Fedeli — Italian

Director Strategy and Innovation

Matteo is an investment professional and a founding partner of Greentale Capital LLP, an infrastructure and private equity business. He has strong commercial, analytical and numerical skills. His experience covers product and partnership development, system and operations solutions and deal management. He has arranged investments and deals for a total gross value of over $1B. He holds a Masters in Engineering from Politecnico di Milano and a Masters in Finance from London's CASS Business School.

Nicola Taylor — Australian

Legal Director

Nicola is a founding partner of Greentale Capital LLP and a lawyer with 20 years of experience in a variety of jurisdictions and practice areas having worked at Herbert Smith Freehills and at Freshfields. Most recently she has specialised in financial services. She has led legal, regulatory and human resources functions in start up ventures and worked closely with commercial and technical colleagues in close-knit multi-disciplinary teams. She has a BA and BL (Honours) from The Australian National University. She is admitted to practice in England and Wales, New South Wales and the High Court of Australia.

Paul Gutteridge — British

Director Communication and Government

Paul is a behaviour analyst who works with government agencies to broker meetings and lead teams in sensitive contexts and with commercial bodies to train leaders to read, assess and influence behaviour in negotiations and project deployment. He has trusted relationships with government, law enforcers and decision makers in financial institutions where physical and cyber security are paramount. He holds a Dip. Behaviour Analysis and Investigative Interviewing, Adv. Forensic Statement Analysis, EIA Facial Action Coding System reader.

Our Advisory Team

A wealth of expertise to draw on

AnimaTech is surrounding itself with an international team of influencers and advisors with a wealth of experience in:

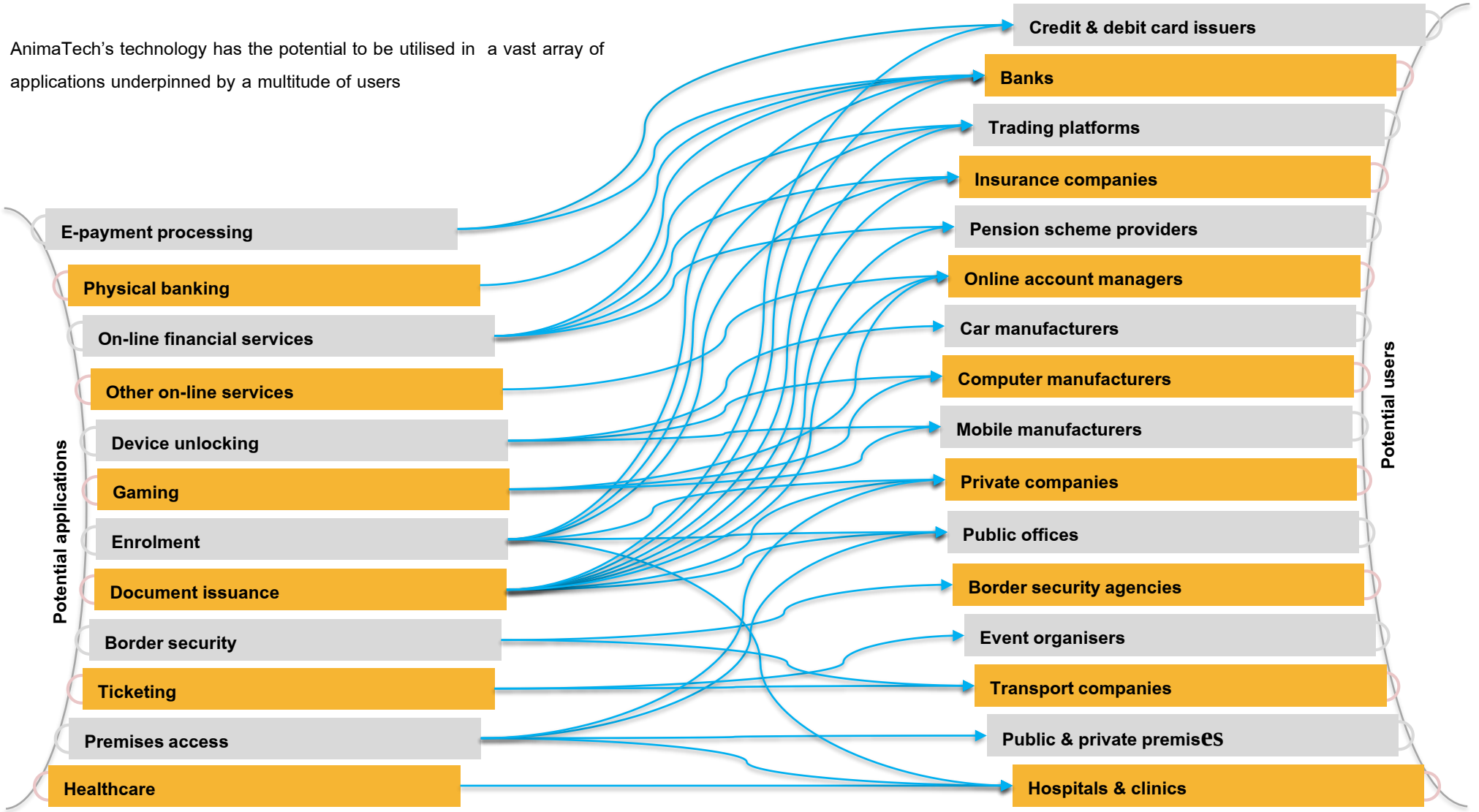
- Financial infrastructure
- Patent law and strategy
- Government relations
- Security services
- Technology
- Behavior analysis
- Biometric industry
- Medical
- Business relations
- Academics

Having a multi-disciplined team enables us to navigate intelligently and respond effectively to the continuing advances in the market.

Our Market Potential

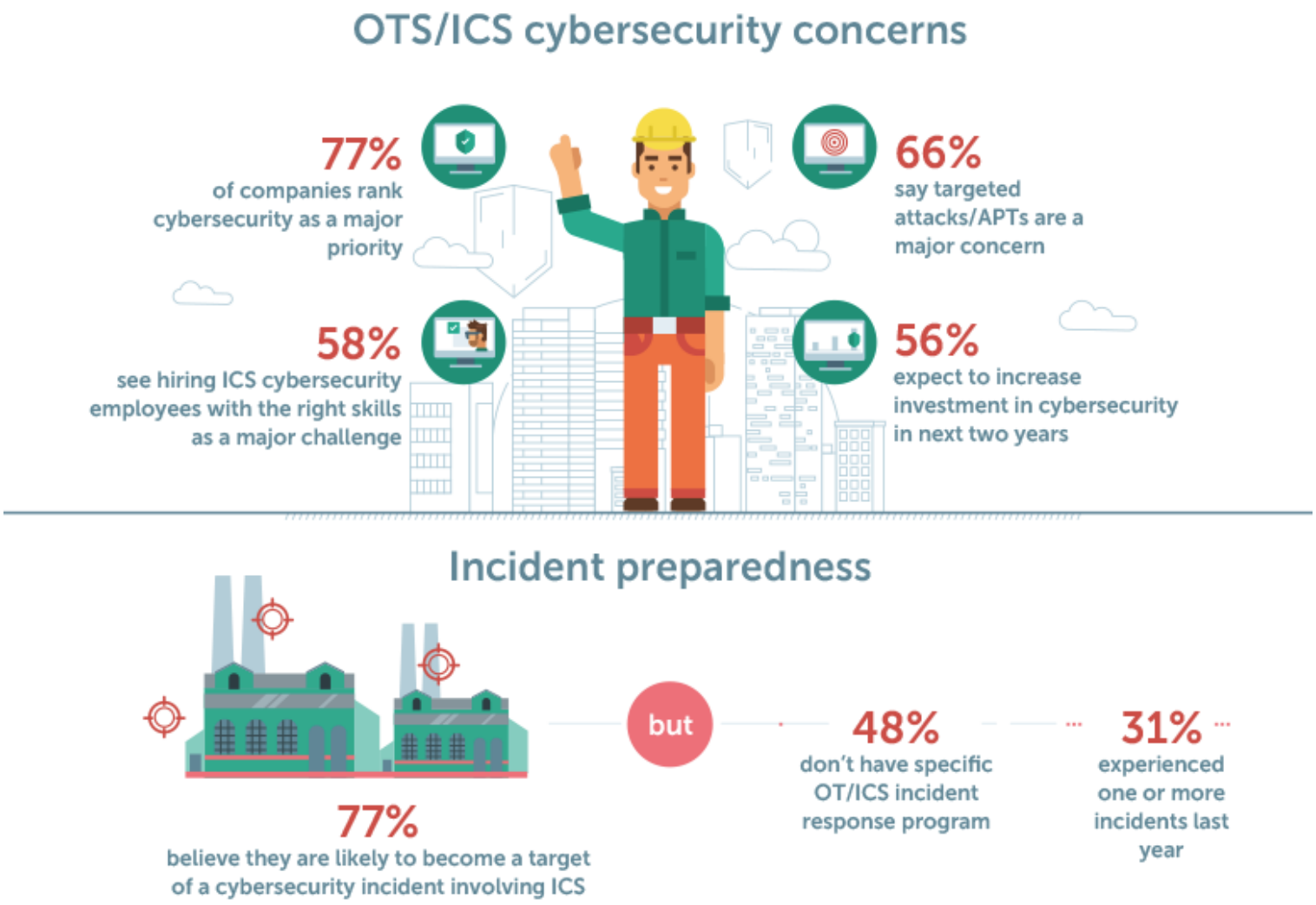
Potential Applications and Users

AnimaTech's technology has the potential to be utilised in a vast array of applications underpinned by a multitude of users



Appendix

The Landscape - Snapshot 2018



Appendix

Data Breaches

A data breach occurs when there is an unauthorized access of a database. Confidential information held on a breached database can be viewed, copied, stolen or used. Typically the information is valuable personal information. Breaches are no longer a binary proposition where an organization either has or hasn't been breached. Instead they are wildly variable and have varying degrees of fallout, from breaches compromising entire global networks of highly sensitive data to others having little impact.

DATA RECORDS LOST OR STOLEN SINCE 2013

9,198,580,293

ONLY 4% of breaches were "Secure Breaches" where encryption was used and the stolen data was rendered useless

DATA RECORDS ARE LOST OR STOLEN AT THE FOLLOWING FREQUENCY

EVERY DAY	EVERY HOUR	EVERY MINUTE	EVERY SECOND
5,153,266	214,719	3,579	60
RECORDS	RECORDS	RECORDS	RECORDS

The Landscape

Data Breaches by Industry in 2017

COMPARING THE INDUSTRIES

From an industry perspective, the greatest number of records compromised between 2016 and 2017 originated from organizations in economic sectors classified as "other." These "other" industries racked up over 1.3 billion breached records in 2017, up from more than 86 million the year before - more than a 1,400 percent increase! That surge notwithstanding, the number of incidents declined in those segments by 57.5 percent from 160 to 68.

RETAIL

The **Retail** sector has taken significant steps to stop cyber attacks - particularly at the point of sale - and perhaps it's paying off. Retailers had 215 data breaches in 2016, down 10% from 239 the year before and accounting for 12% of the total. Also the number of records stolen was down to 32 million from 40 million in 2015, a decrease of 18.8%.

HEALTHCARE

Healthcare: Compromised accounts grew 27.4 percent to 33,717,772 from 26,467,715. Incidents decreased by 11.3 percent during that same period from 531 to 471. Even so, healthcare organizations encountered the greatest number of breaches among all other industries in 2017

FINANCIAL SERVICES

The **Financial services** sector is one of the more fascinating, and gives a good indication of how attacks are resulting in the theft of larger numbers of records. Financial services weathered an increase from 13,364,697 to 235,563,765, with the number of incidents decreasing by nearly 10 percent from 241 to 219. The rise of breached records in

TECHNOLOGY

Technology: With a 3 percent increase in breached files in the technology sector, numbers went up only slightly from 392,727,945 to 404,698,020. Breaches involving technology providers went down during that same period from 203 to 130. There were plenty of industries where the total breached records actually fell but the number of incidents rose

EDUCATION

The **education** sector saw improvements in both the number of data breaches and records. Breaches totaled 157, down 5% and accounting for nearly 9% of the total. Records stolen dropped 78% to 4.4 million.

Insurance

Insurance, whose total number of breached records dipped by 98.5 percent from 9,307,242 to 135,359 and whose incidents increased by nearly a half from 15 to 22.

GOVERNMENT

Government: An 18.7 percent rise in records from 391,795,340 to 465,014,660 occurred in governmental agencies, with incidents declining more than a third from 289 to 193.

HOSPITALITY

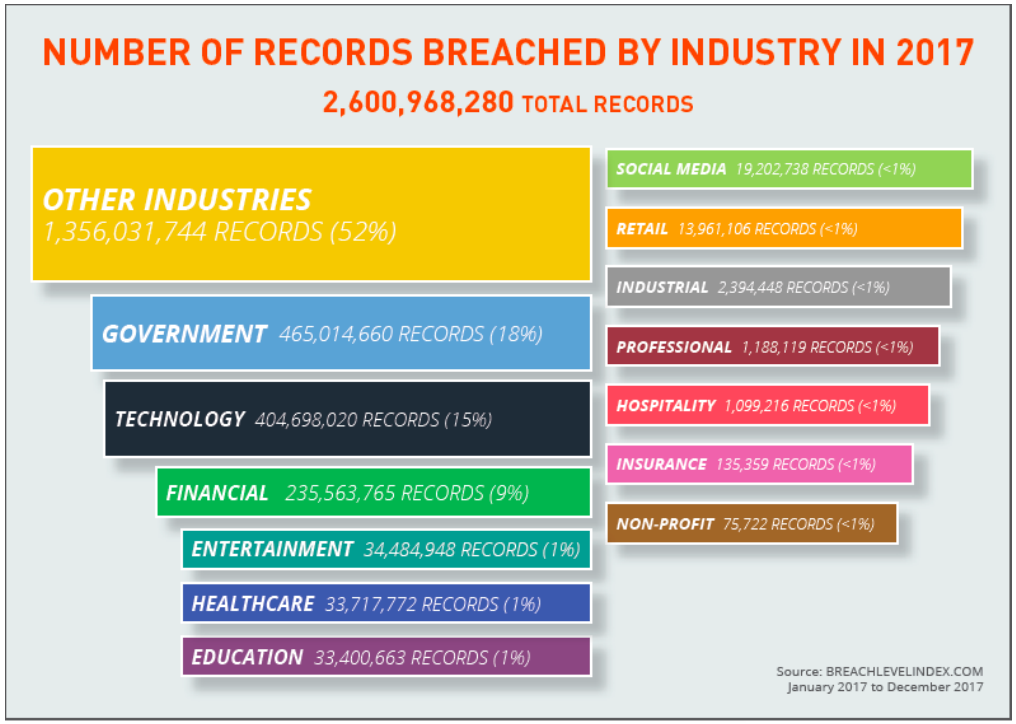
Hospitality dropped 88.5 percent to 1,099,216 from 9,568,998, yet events rose slightly by 2.9 percent from 35 to 36.

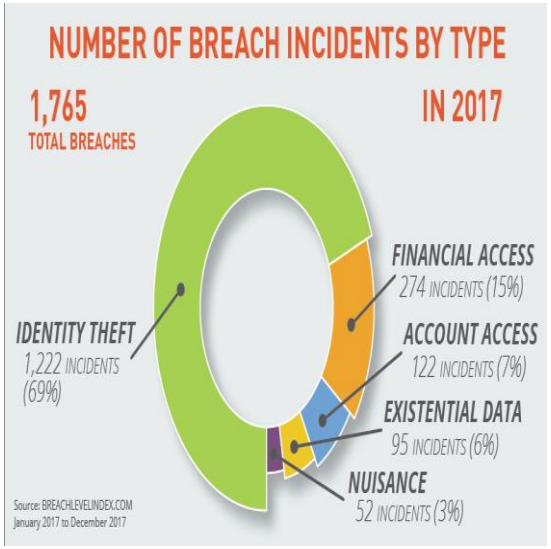
The Landscape

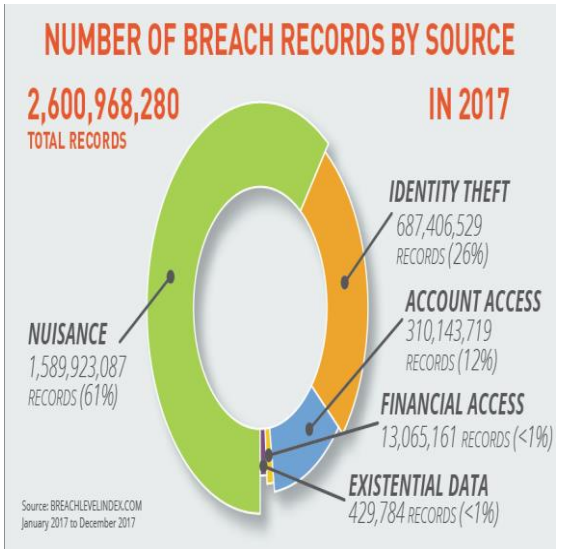
Data Breaches by Industry in 2017 (cont.)

Social Media

Astonishingly, **Professional services and Social media** saw an even greater rate of growth in their number of compromised records over the course of the year. Breached accounts for the former industry increased to more than 1 million from 0. Its number of incidents also experienced monumental gains, swelling from just one case in 2016 to 92 the following year. As for the former, compromised documents pertaining to social media expanded greatly percent from just 1,489 to close to 20 million, whereas the number of incidents grew from 2 to 9.





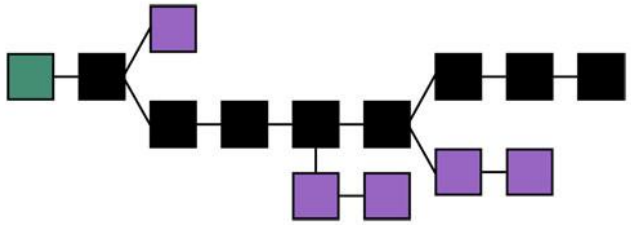


Appendix

Cryptocurrency Security

BLOCKCHAIN

There are security issues with Cryptocurrencies. However, a recurring theme is the fact that these security breaches and issues have **less to do with the protocol itself**, and a lot **more to do with the people and services** handling and storing these currency units.



OWNING CRYPTOCURRENCY IS NOT quite the Wild West experience it was at the beginning of the decade, but investors still face plenty of instability and risk. The threats are not just abstract or theoretical; new scams crop up, and old ones resurge, all the time. Whether it's a fake wallet set up to trick users, a phishing attempt to steal private cryptographic keys, or even fake Cryptocurrency schemes.

Cryptocurrency Wallets

Cryptocurrencies are stored in wallets, but unlike a PayPal account, these “wallets” **do not actually store the currency units themselves**. Despite a number of different implementations and formats, generally wallets will **contain a public key** that is used to receive the currency units (similar to a bank account number). It also contains **a private key** that is used to verify that you are indeed the owner of the currency units that you are trying to spend.

Appendix

Identity Theft

"Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain."

[US Department of Justice]

- Some **15.4 million** consumers were **victims** of identity theft or fraud last year (**+16%** compared to 2015 figures and the highest figure recorded).
- Thieves stole **$16 billion** (+$1 billion compared to 2015).
- Two-thirds of firms breached had their **share price negatively impacted**. Out of 65 companies evaluated the breach cost shareholders over **$52.4 billion**.
- **918** data breaches led to **10 million** data records being compromised worldwide **every day** in the first half of 2017 (+ **164%** compared to the last six months of 2016).

Data breaches typically result in theft of personal information – identity theft – and identity fraud. As statistics reveal, these are large and costly problems – and growing ones. It is also generally accepted that publicly available figures significantly underestimate the extent of the problem because identity theft reporting is largely unregulated and uncontrolled, and private companies prefer to avoid bad publicity so they do not voluntarily report.

As the "Internet of Things" (IoT) continues to grow quickly and relentlessly, more and more data will be at risk of cybercrime, adding pressure on demand for safe and reliable solutions.

A 2016 report from Business Insider's research service (BI Intelligence) estimated **US$655 billion** will be spent on cybersecurity between 2015 and 2020: **US$386 billion** to secure PC's, **US$172 billion** to secure IoT devices and **US$113 billion** to secure mobile devices.

Appendix

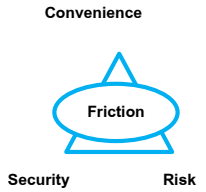
The Growth of Biometrics in Authentication

Biometric authentication can be viewed as having evolved in three phases, each with increased acceptance of their role in everyday life.

1. During the **first phase** the use of biometrics was established through mass-market smartphones and, to a lesser extent, border controls. Functionality mainly included unlocking and security features on a phone and identity validation at some border controls.

2. The **current second phase** is being characterized by increased confidence in biometric technology as more applications are developed such as secure payments and the introduction of biometrics on smart cards.

3. During the **third phase** biometrics will become a part of everyday life. Usage will be on a broad scale though multiple applications via several devices often with interacting biometric systems satisfying increasingly stringent security requirements.



The success of biometric technology also depends on the balance between security level, convenience and risk level. The right balance means greater acceptance of its use.