



Innovation Strategy - Blockchain - AI - RegTech - Cyber Security

# Develop Your Fintech Strategy

2018  
Unbank.Ventures



**Unbank.Ventures** is an education company focused on incubation and accelerator services in the financial industry. We are building a global platform to provide education, advisory and investor connections to startups, financial institutions & service providers.

Our flagship programs are:

Unbank.Incubate

Unbank.Accelerator

Unchain.Ventures

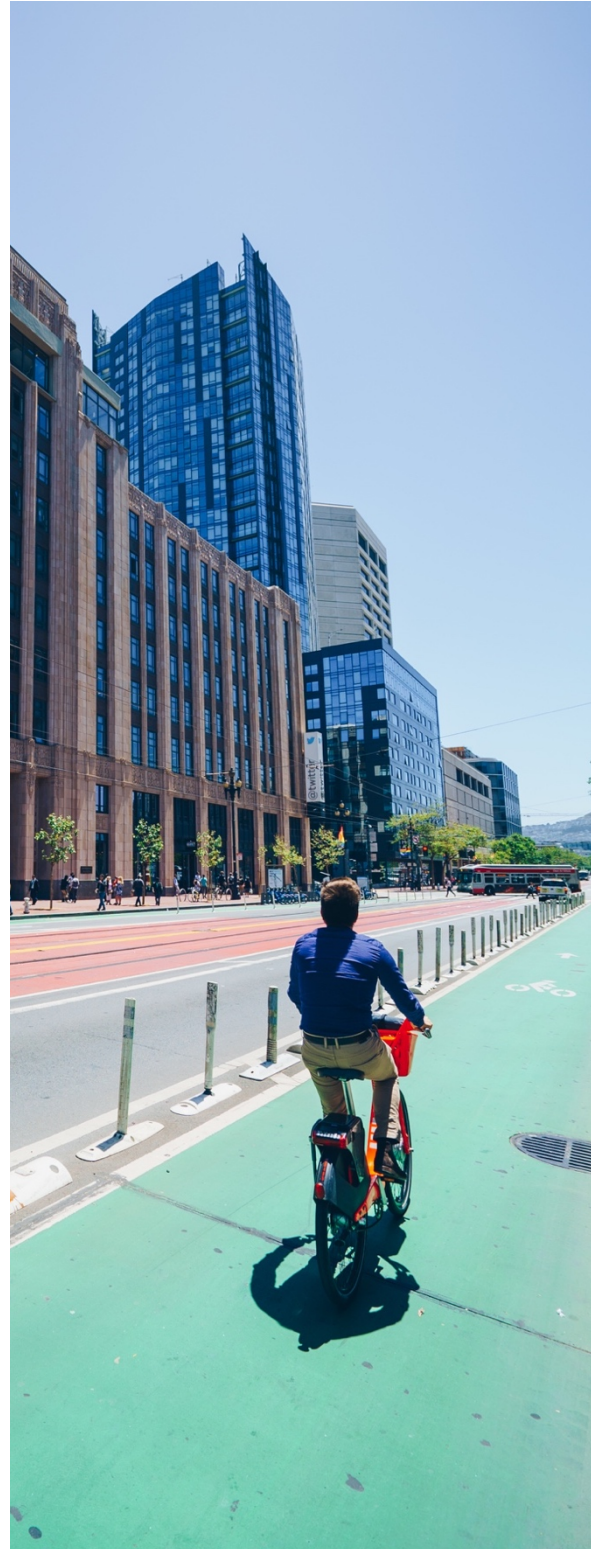


## Table of Content

1.1 Introduction to Innovation Strategy	4	4.4.8 Encompass Compliance Corp.	33
1.2 Innovation Strategy	5	4.4.9 CUBE	33
1.2.1 Innovative Culture	6	4.4.10 IdentityMind Global	33
1.2.2 Innovation Leadership	7	4.5 Should You Invest in RegTech?	33
1.2.3 Tech Adoption	9	4.6 What is the Future of RegTech?	34
1.3 How Innovative is Your Company?	11	4.7 Conclusion	34
1.4 Conclusion	12	5.1 Introduction to Cyber Security	37
2.1 Introduction to Blockchain	14	5.2 What is Cyber Security?	38
2.2 What is Blockchain Technology?	14	5.2.1 Types of cyber attack	39
2.3 Blockchain in Trade Finance	15	5.3 Why Should Financial Institutions increase their focus on Cyber Security?	40
2.3.1 Smart contracts	16	5.4 Cyber Security Trends in the Financial Industry	41
2.4 Blockchain Trade Finance Platforms	16	5.4.1 Proactivity	41
2.4.1 Wave	16	5.4.2 Adoption of More Advanced Technologies	41
2.4.2 Batavia	17	5.4.3 More Advanced Attacks	41
2.4.3 Marco Polo	17	5.4.4 Multi-Factor Authentication	42
2.4.4 Voltron	17	5.4.5 Regulations	42
2.4.5 We.Trade	18	5.4.6 Competence Shortage	42
2.5 Conclusion	18	5.5 Cyber Threats to the Financial Industry	43
3.1 Introduction to AI	20	5.5.1 Changing Landscape	43
3.2 What is Artificial Intelligence?	20	5.5.2 Third- and Fourth-Party Cybersecurity Risk	43
3.3 Where is AI today?	21	5.5.3 DDoS Attacks	43
3.4 How Can AI Be Used in Finance?	21	5.5.4 AI	44
3.4.1 Trading	22	5.5.5 Jackpotting	44
3.4.2 Banking	22	5.5.6 State Supported Attacks	44
3.4.3 Investing	24	5.6 Conclusion	44
3.4.4 Lending	24		
3.5 Conclusion	25		
4.1 Introduction to RegTech	28		
4.2 What is RegTech?	28		
4.3 Technologies Applied in RegTech	29		
4.4 RegTech Solutions	30		
4.4.1 IBM Financial Services & Industry Platform	30		
4.4.2 RIMES RegFocus	31		
4.4.3 Thomson Reuters Velocity Analytics	31		
4.4.4 Asset Control	32		
4.4.5 Bureau van Dijk	32		
4.4.6 Ayasdi	32		
4.4.7 Trulioo	32		

# Part 1

How can companies within the financial industry take advantage of new technological trends?



## 1.1 Introduction to Innovation Strategy

Innovations revolutionize the way we work and new technologies disrupt traditional processes and systems. Since the beginning of the digital revolution, there has been an enormous change in how businesses operate, on the strategic, administrative and operational level. The exponential growth of technology, makes it more important to keep on track with the technological developments than ever before.

In the financial industry, there has been a wave of technological innovations challenging the financial services as we know them. Today, traditional financial services compete with a fast-growing industry, known as Financial Technology or Fintech. Fintech uses technology to improve processes, systems and activities in the financial sector. It is a broad term and concerns everything from payments and loan and money transfers to contracts, insurance, and regulations.

The investments in Fintech have increased remarkably and every player in the financial industry should pay attention to the new fast-growing industry and all the possibilities that come with it. New technologies can simplify working methods and make your business more efficient.

Investing in technology and innovation can give your business advantages in the short and long run, but it requires the right culture

and leadership in order to unleash its true potential.

For this reason, Unbank.Ventures provides this paper, a guide into the world of Fintech. As an education company in the financial industry, we work with Fintech startups and financial institutions all over the world and experience the huge potential that the intersection between technology and financial services creates.

We believe new technologies can give your customers increased value, through simplifications and smarter solutions. In addition, technological innovations can reduce costs. Better services at lower costs will attract new customers and help your company grow.

The question is whether your company has the right base to grow through continuous innovation. And what kind of innovations and technologies you should focus on. There are no general answers to these questions but we will, through this paper, provide the information you need in order to explore the new world of financial technologies.



### Part 1

Are you ready to invest in new innovations?

What kind of Fintech technology should you focus on in pursuit of value?

How should you deal with tech adoption?

## 1.2 Innovation Strategy

A well defined strategy for innovation is more important than ever before. The high number of growing startups, the accelerating speed of technological developments, globalization, and demographical factors lead to a high pace of change, as well as a high level of uncertainty in the environment. In order to stay profitable over time, companies either have to come up with more efficient systems and processes, or create more value for the customers through innovative products and services. On the other hand, if a company stays unchanged in a dynamic environment, it will be outcompeted.

*New technological systems, products and services often lead to a competitive advantage.*

An innovative strategy is a plan to encourage advancements in technologies, products, or services. This form of strategy helps enhance the technology in a company, by enabling creative thinking.

The Financial Industry faces a wide spectrum of new and powerful technologies. In order to successfully adopt and implement these innovations, organizations must have a sufficient strategic approach to innovation. Who in your company has an experimental mindset? Who seeks new opportunities and is willing to take high risks in order to gain high rewards?

In a modern company, these people are located in more than an innovation lab. The innovative thinking must be rooted in the organizational culture, and every division must be able to validate ideas, adopt, and scale them. Employees with an innovative and open mindset simplify the adoption of new technologies and the internal resistance against changes are thus limited.

In startups and small organizations, leaders and employees can sit around the same table and discuss market potential and new solutions. This form of interaction encourages innovation and entrepreneurial thinking. But when companies grow larger, the personal interaction decreases and leaders start using more formal systems in order to share information and keep control. The lack of systems for idea sharing and creative thinking often becomes a huge problem for the fast-growing organizations. That massive growth leads to less creativity and innovation.

There are more than 5000 banks in the US and most of these are already well established with formal systems and processes. Yet only the largest banks have systems and strategies concerning innovation. In today's continually changing technological environment, rigid, backward leaning banks will be out-competed by the largest banks. To remain competitive, smaller banks must establish an innovative strategy and start looking into the fast growing world of Fintech.

But how can companies within the financial industry take advantage of new technologies? And how do they provide a reasonable assurance regarding the achievement of innovation objectives?

### 1.2.1 Innovative Culture

Having a well established innovative culture is the key to create cycles of successful innovations. An innovative mindset must be rooted in the culture if your company aims to stay innovative over time. There is huge uncertainty related to new technologies, and what looks promising today can turn out to be a real disaster tomorrow. Investing in new technologies can be terrifying and some will therefore avoid these investments and keep their current technology. Being a safety-seeker in today's rapidly changing and competitive world is a mistake.

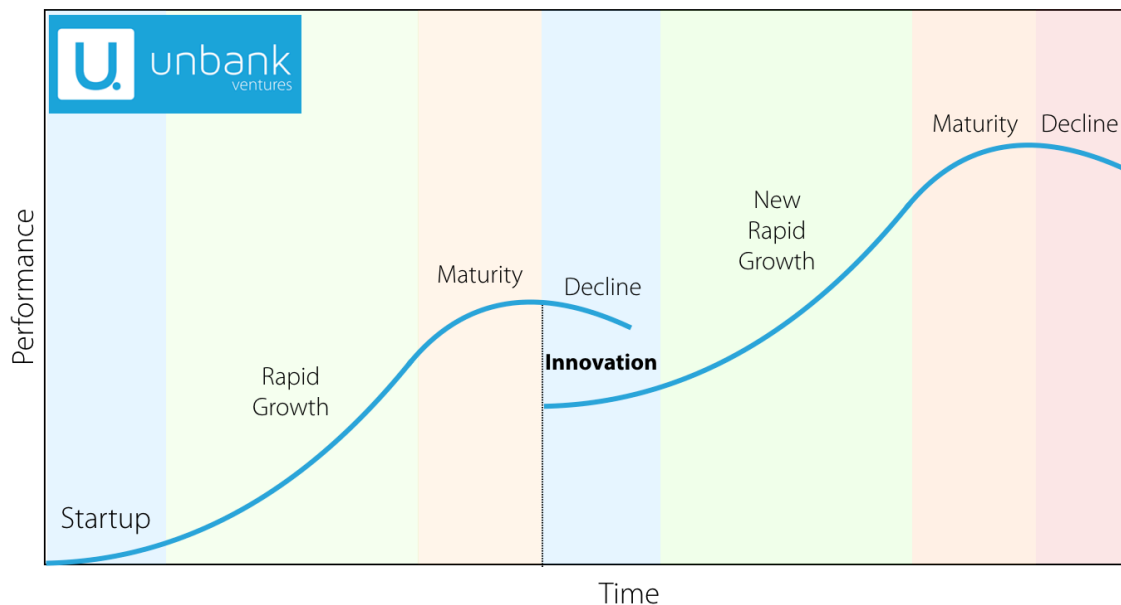
All companies need a culture that encourages the embrace of new

technologies and eases the barriers of creativity.

You do not get an innovative culture by simply defining an innovation strategy. Similarly, employees do not start thinking outside the box just because they were told to do so. An experimental, innovative culture must be formed over time and when you obtain it, the culture will start attracting innovative people. Creative people break things down and think outside the box. They seek improvements and want to solve problems which is particularly important considering the high degree of complex challenges today's businesses face.

*An innovative culture can give great advantages, but is generally difficult to obtain.*

Simply adopting a new technology does not mean you get a long-lasting advantage. In



The life cycle of a company focusing only on one key innovation. In order to avoid the decline period, companies must focus on continuous innovation.

order to keep the advantage, the technology must be successfully implemented and continuously improved. With an innovative culture, employees will look for improvements and potential uses for the technology, instead of being satisfied with the the current state of the company. Without continuous innovation, a company eventually will experience declining performance. To avoid the negative growth, it is important to focus on new innovations so that the company repeatedly experiences new growth periods. That one key innovation will not lead to a lasting competitive advantage.

An innovative culture is undoubtedly important, but equally so is innovation leadership.

### 1.2.2 Innovation Leadership

Creating an innovative culture is in itself challenging. Core values and beliefs are not only difficult to change; they also change slowly. Leaders must combine different styles of leadership in order to encourage innovation and creative thinking. On one hand, they must keep control over the organization so that it works in the right direction, and on the other hand they must empower employees and give them freedom to behave creatively. To balance empowerment and control is particular difficult. If you give employees too much freedom, there is a risk that they act contrary to the underlying business objectives. Boundaries and a high level of diagnostic control systems could damage motivation and the innovative spirit. Being aware of

different forces with impact on the ability to control and motivate employees is necessary before starting the development of an innovative strategy.

How do you attract and keep innovative employees? There is always a risk of losing great employees, but ambitious leaders



For leaders:

1. Define the rules of the game
2. Put innovation on the agenda
3. Find appropriate performance measures for innovation
4. Set targets for innovation
5. Set boundaries
6. Create a team environment
7. Empower employees
8. Manage, track and support

should find ways to satisfy their innovative people.

Other difficulties related to innovative leadership concerns the costumers. How do you explore new markets while keeping existing costumers? The right balance between exploration and serving existing markets can be challenging to find. By testing new products and services, you can

put your core markets at risk. Still, managers with a desire to achieve a high level of innovation, should create opportunities for experimentation and creativity.

Traditionally, managers aimed to keep things on track and reduce the uncertainty to an absolute minimum. As a result, businesses tended to be very standardized, rigid and without an innovative focus. The management usually had a top down strategy, and prioritized control over innovation. Over the years, the traditional approach has become outdated in many sectors, due to the increasing level of dynamics. The financial industry now faces disruptive innovations in almost every financial service and the leadership must change in order to take advantage of the new digital innovations. With a higher degree of dynamics in the sector, the leadership style needs to be more dynamic and flexible. Empowerment, continuous improvements, and adaptations should play a key role in the leadership.

*As a manager in the financial services industry, you shouldn't look at new innovations as threats, but opportunities.*



### 1.2.3 Tech Adoption

Companies holding an innovative culture and style of leadership are likely to invest in innovations. Unfortunately, there is no best practice in terms of adoption method. What works for your competitor, will not necessarily be the best for you. Hence, the question is what approach you should go for when adopting a new technology. Generally, there are two main practices:

- 1) In-house development
- 2) Procurement

Many managers prefer developing technologies in-house. Building your own solution lets you tailor the technology for your own needs and your customers expectations. The technology will also be in line with your strategic orientation and objectives. Even though there are many positive aspects with a self-built solution, it is not an easy task to run the entire process from idea to final solution.

How will the new technology create value for your customers? Which financial service will be improved through the innovation? What should the specifications be? Do you have the right expertise in-house? Who should be part of the team? How much risk is associated with the investment? The financial aspect is naturally also important to take into account when deciding whether you should be building your own technology.

Alternatively, you can procure the technology externally. Like self-development, procurement of Fintech technologies has the opportunity to provide a competitive

advantage in the financial industry. For companies without the right competence in technological development, this will be the preferable strategy in terms of tech adoption. However, the process is simpler than the self-building strategy, with a few matters that must be considered.

The process of procurement is in itself very important for the end result of the tech adoption. Lack of preparation and research can result in suboptimal solutions and adoption of technologies that have to be replaced relatively quickly in order to stay competitive. As a consequence of the fast pace in Fintech development, there are now a great many companies that offer different technological solutions for the financial industry. Some are already well established, while others are still in a startup phase, where experimenting with new and innovative technologies and services.

By emphasizing planning, specification determination, supplier research, value analysis, and valuation, you can provide a reasonable assurance regarding the achievement of tech adoption. Evaluation of alternatives should recognize and determine relative advantages, complexity, compatibility and 'trialability' among others.

Some companies prefer an acquisitions strategy for technological improvements. The purchasing company then uses the purchased company to improve its financial services.

Instead of making a purchase, a collaborative procurement can be an alternative. Entering a collaboration with a supplier can increase the level of innovation and result in ground breaking products and services. Alternatively, a collaboration between equally sized procurement companies can be beneficial. Some financial institutions do not have enough available resources to go into negotiations alone. By forming an alliance with another similar company, they get more power in the negotiations with suppliers, which can lead to lower costs. Whether you develop a technology in-house or obtain the technology through procurement or acquisitions, you should be aware of the benefits and drawbacks with your strategy. What strategy you choose should be based in the type of technology you need and your organizational structure, culture and leadership practice.

## 1.3 How Innovative is Your Company?

Measuring innovation is a challenging exercise due to the high level of subjective factors. Therefore, there is no general way to quantify how innovative companies really are.

To better understand needs and the ability to adopt new Fintech technologies, we are creating a fillable form consisting of both objective and subjective considerations.

Based on general information combined with evaluations of management principles, we want to give companies a score on how innovative we think the company has the ability to be. We base our score on a preselected list of characteristics and our algorithms are frequently improved in order to give the most precise estimates possible.

The algorithm is under construction. Fill out the form and help us create an innovation score tool.

By taking the survey, you help us create a groundbreaking algorithm for innovation assessment. In addition to the innovation score tool, we will make a report concerning innovation in the industry. Both the findings and the algorithm will be available for all participants.



---

Help us develop the model

Click here:

Take the survey

Link: <https://goo.gl/forms/QkSV819jf33EnHrG2>



## 1.4 Conclusion

The first part of our series regarding development of Fintech strategy has focused on innovation strategy. In order to be a successful innovative financial institution, you must exercise innovative leadership and create an innovative culture in your organization. The way you manage your employees and encourage innovation and creative thinking in the workplace will affect your ability to gain a competitive advantage through innovation. Be aware of the benefits and drawbacks with different tech adoption strategies, and find the one that fits best to your needs, culture, and organizational structure.

Having a well-defined innovation strategy will help you stay within the fast-growing Fintech industry and take advantage of the opportunities that comes with it.



# Part 2


How can blockchain improve trade finance?

## 2.1 Introduction to Blockchain

In this part we will focus on the new blockchain technology and discuss how the technology can be applied in trade finance. Trade finance includes financial activities like lending, the issuance of letters of credit, factoring, export credits, and insurance.

Blockchain is about to change the way people and companies work. In brief, blockchain is a digital, public ledger of transactions. The blockchain is continuously growing and new transactions are recorded, added to the chain, and linked to the previous block. This technology makes transactions more transparent and secure.

We believe blockchain has a huge potential in the industry, and the following pages give an introduction to the technology and its advantages in trade finance.



Part 2

What is blockchain?

Why is blockchain interesting for financial institutions?

What is the potential of blockchain in trade finance?

Which platforms for blockchain trade finance exist?

## 2.2 What is Blockchain Technology?

We have all heard that blockchain will be the next huge digital revolution after the internet. But how does it work and why is this particular technology so promising?

The blockchain technology records transactions in blocks of data and every block is added through cryptography and connected to the previous added block. The connection of blocks makes an irreversible chain of blocks and the way they are chained makes it almost impossible to change the data at a later time.

A blockchain can be connected to millions of nodes, which are personal computers connected to a network. All these nodes have a copy of the blockchain, which means the information is decentralized and widely distributed. To change anything in the chain the information in the entire network of nodes must be updated, which requires an enormous processing power. Consequently, it becomes very difficult to manipulate or corrupt data.

Blockchains can have different degree of transparency, depending their purpose. A blockchain that is permissionless is very open, while a permissioned blockchain has a higher degree of controlled access points. This makes it possible to control peoples access and give access permission only to people who need it.

In the financial industry blockchain can be perceived as an opportunity as well as a threat. On one hand, the technology can improve many financial services by making them more reliable, efficient, and secure. On the other hand, blockchain challenges the way today's banks operate and their current business model.

As you may know, the blockchain technology was originally developed for Bitcoin and was used to verify cryptocurrency transactions. Today we see a much wider potential for the technology. In the financial industry, blockchain can be applied in the field of insurance, stock exchange, smart contracts and so on. According to a report from the IBM Institute for Business Value, 91% of their surveyed banks are planning to investing in blockchain technology in 2018. The high percentage indicates a common understanding of the potential this new technology has in the financial industry. But still, there are some banks sitting on the fence, which is remarkable when we observe the benefits and huge field of application.

This paper will focus on the use of blockchain in terms of trade finance.

## 2.3 Blockchain in Trade Finance

Manual processes within the field of trade finance can be both challenging to handle and time consuming. One single transaction could involve lending, insurance, issuing letter of credit, factoring and so on. There are

clearly many parts involved and paper-based documentation must be sent from part to part in order to establish an agreement. Every time a change is made, all parts must be informed and get the chance to review and validate the documentation. As a result of the high number of documents and partners in different countries, the logistics become highly complicated. From exporter to importer, goods must be validated by multiple legal entities and if any unforeseen problems occur along way, transactions can take weeks to complete.

Banks deal with complex processes in terms of cross-border transactions, and the security of tracking of transactions can be problematic. To simplify the process, paper-based transaction records can be substituted with digital transaction records using blockchain technology. This change of technology can lead to a number of process improvements.

First of all, the process in itself becomes more streamlined. Waste in form of waiting time will be markedly reduced and lead to a faster transaction process. Furthermore, the transaction also becomes more transparent since transaction partners are able to see the progress and track the flow from start to end. As initially described, blockchain comes with improved security and beside improved efficiency it results in less uncertainty and higher degree of trust in trade.

Transactions often require multiple signatures and contracts, which can be

handled by integrating smart contracts in the blockchain.

### 2.3.1 Smart contracts

Smart contracts are contracts that are developed using digital code and stored on a blockchain. Since the smart contract is built on the blockchain technology, it is immutable and distributed. Immutable means that the smart contract cannot be changed when it is created and being distributed means it the contract is being validated and stored at a network of computers. This reduces the risk of manipulation and since the data is added through cryptography, only people with access are able to see and sign it.

A smart contract includes all the information you will find in a traditional contract, but it also includes computer code that will trigger an action if a particular condition is met. For instance, if all parts agree on the terms and sign the contract, assets will be transferred automatically. In other words, there are a bunch of built in If-Else statements, which makes the contract process go much more seamless and without an intermediary.

When a part signs the smart contract, the blockchain will be updated and other persons with the right access point can immediately see the updated status of the contract.

As for blockchain, smart contracts have a wide field of application and it can be applied in most industries. In trade, smart contracts can be used in the agreement

between the exporter and the importer, as well as their banks. The importers bank will be able to track the assets, review the contract, and submit obligations to pay the exporters bank. On the other hand, the exporters bank will provide payment obligation and create another smart contract. When the all the conditions are met, the payment will go through.

There are multiple exciting blockchain initiatives in terms of trade finance. In the next section I will briefly discuss some of the most promising platforms that are out there.

## 2.4 Blockchain Trade Finance Platforms

### 2.4.1 Wave

The first blockchain trade finance transaction was made by Barclays and Wave in 2016. The Fintech startup company Wave was a part of Barclays Accelerator program in 2015, and a year later, Barclays and Wave executed the first a global blockchain transaction using their new Wave platform. This was the first time the paper-based process went digital using blockchain technology and Barclays claimed the platform gave substantial cost savings and reduced the transaction time from days to hours.

In November 2017 Wave announced they had successfully conducted a pilot using its application and hence taken another step towards a commercialized solution. The parties managed to execute an export letter



of credit in four hours, a process that usually takes over a week to complete. At that time Wave worked with 57 banks and many more wanted to be a part of the next pilot project.

#### 2.4.2 Batavia

Swiss bank UBS and IBM started working on a global trade platform based on blockchain in 2016. A year later BMO, CaixaBank, Commerzbank and Erste Group joined the team. Their platform is called Batavia and is developed in collaboration with exports from the transportation industry. Their object is to make a well functional blockchain trade platform that is designed to support more efficient, transparent and cost efficient transactions.

Batavia uses a combination of smart contracts and distributed ledger technology. Their platform makes it easy to manage and track the process for all participants in a cross border transaction.

In June 2018 Batavia successfully executed its first live pilot transaction with corporate clients and took another step in the establishment of Batavia as an open system that is built on the IBM Blockchain Platform. The successful pilot transaction indicates that Batavia is a step closer to be a complete, fully functional blockchain solution.

#### 2.4.3 Marco Polo

In collaboration with 13 global banks, blockchain startup R3 and the trade finance tech provider TradeIX are developing Marco Polo – a open-source trade finance platform. It is built with R3's distributed ledger

technology, Corda and delivered over TradeIX's TIX platform.

Marco Polo is a pre- and post- shipment trade finance solution, and includes everything from purchase of orders, to invoicing, shipping and logistics information, to trade assets, financing activities and credit risk.

In late 2017 the group behind Marco Polo launched the project and the first proof of concept was successfully carried out early in 2018, when they launched the first pilot project. In May this year, the French bank Natixis also joined the initiative, which signalize there is an increasing understanding of the benefits these platforms can provide.

R3 is working with Microsoft and integrating Corda with Microsoft's Azure.

#### 2.4.4 Voltron

Beside Marco Polo, R3 is also working on another interesting platform based on their distributed ledger technology, Corda. In collaboration with 12 banks R3 is developing the Voltron platform for improved efficiency in trade finance. Voltron will be a marketplace for exporters and importers. They can use the application for preparation and validation of shipment details, in addition to streamlining the letter of credit process.

Multiple pilot projects have been running and Valtron looks very promising. The time of

paperwork can be significantly reduced using the platform.

#### 2.4.5 We.Trade

Like R3, IBM also work on multiple platforms for trade finance. In 2017 IBM and eight banks began the development of We.Trade, a digital trade chain share platform using distributed ledger technology.

We.Trade can be used to manage, track, and secure cross-country trade transactions.

From February 2018 test clients were able to use the platform, and the commercialization were planned to take place in Q2 2018.

### 2.5 Conclusion

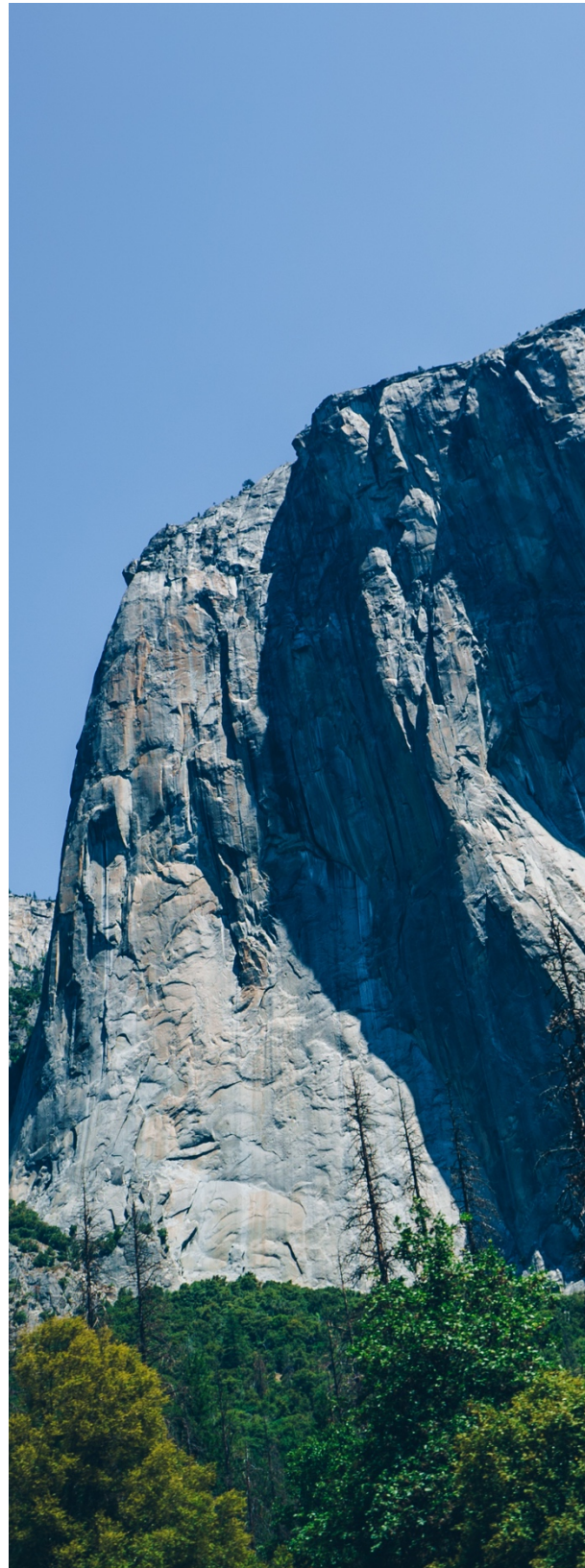
The second part of our series regarding development of Fintech strategy has focused on the blockchain technology in terms of trade finance. Blockchain records transactions in blocks of data and adds them through cryptography to a chain of blocks. The connection of blocks makes an irreversible chain of blocks and the way they are chained and stored makes it almost impossible to manipulate or corrupt data.

As we have seen, the blockchain technology can improve transaction processes in order to be faster, more secure and less complex. The landscape of blockchain trade finance applications is fast growing and several platforms will soon be commercialized. Wave, Batavia, Marco Polo, Valtron and We.Trade are participants in the trade finance

blockchain race. It will be interesting to follow their journey and see how they revolutionize the industry.

# Part 3

How is artificial intelligence (AI)  
disrupting financial services?



## 3.1 Introduction to AI

Today most financial institutions have open their eyes for AI and there is no doubt the implementation of AI can create value for businesses.

The question is rather how financial institutions can make the best out of the technology. There are several use cases for AI in financial services, and keeping track with the fast paced development of AI can be hard. In the following pages we give an insight into some applications for AI in terms of financial services.



### Part 3

What is artificial intelligence (AI)?

What is the state of AI now?

What are the most important use cases for AI in terms of financial services?

## 3.2 What is Artificial Intelligence?

In computer science, AI is a term for intelligent machines. Machines are programmed to “think” like humans and they have the ability to solve different kind of problems without being programmed to solve each particular task. In other words, we want machines to learn, reason, percept and take action in order to achieve a desirable result. The term is applied when machines act independently, without intervention from humans.

Businesses in all industries seek to find new ways to work more cost efficiently. AI gives huge opportunities and disrupts the traditional way people work. Machines today can take over repetitive tasks and let humans focus on composite tasks or tasks that require human interaction. Nearly every industry has tasks that could be done by AI, and the financial industry is no exception.

AI is a wide term, including many different terms and technologies. As a result of the lack of precise definitions and the broad set of techniques, methods and algorithms, it can be difficult to understand what AI actually is and how it works.

Some people will say AI is the intelligence demonstrated by machines in contrast to natural intelligence demonstrated by living creatures. But even though scientists have figured out a great deal about the human brain, we do not fully understand how human intelligence works. However, we try



to make artificial intelligence as close to natural intelligence as possible. The term AI can be separated in two branches, symbolic learning and machine learning. Symbolic learning includes computer vision and robotics, while machine learning on the other hand, includes statistical learning and deep learning. Machine learning uses statistical techniques to train models, and models must be fed with historical data in order to give accurate results.

Furthermore, there are multiple fields of AI connected to each of the two branches. For instance, computer vision is a field related to symbolic learning, while speech recognition, and natural language processing (NLP) use machine learning techniques. When we discuss different use cases for AI in terms of financial services, we will cover all these fields of AI.

There are different degrees of how intelligent AI really is. Most machines we think of as AI today has very specialized intelligence. IBM's Watson, Apple's Siri and DeepMind's AlphaGo is very good at the particular tasks they are set to do, but their intelligence is very narrow and they cannot handle a wide spectrum of different tasks – in other words, their intelligence cannot be generalized in order to solve all kinds of different problems.

### 3.3 Where is AI today?

AI is moving fast and it has been incorporated in service after service. What AI was twenty years ago is not even related to AI anymore. Today, AI has what we call

narrow intelligence. As described in the previous paragraph, this means it performs well at specialized tasks, but we have not obtained what is called general intelligence, which is the intelligence of a machine that can perform every individual, intellectual tasks that a human can perform. It is hard to tell when we first succeed in the development of general intelligence, but when we first do, I think the advancements towards superintelligence will go very fast. By superintelligence, we mean AI that is much smarter than the smartest human brains. The rapid development and the fact that we do not know where we are going, can be both frightening and exciting.

For business today, one of the greatest risks is not having the right strategy to adopt technologies fast enough. In order to keep on track with the advancements, banks should, as described in part 1, have a strategy built on an innovation culture, using an innovative leadership.

### 3.4 How Can AI Be Used in Finance?

AI has huge potential in literally all financial fields. As the AI technologies develop, new applications are discovered and exploited. In this section I will describe the present state of AI in trading, banking, investments and lending.

### 3.4.1 Trading

Even the best experts on financial trading having a hard time identifying all patterns in the stock market. There are always a huge number of factors affecting the fluctuations, and predicting the future is almost impossible due to unpredictable events. However, machine learning can improve predictions, using a large amount of data than humans can't handle. AI can manage trading decisions through well-established algorithms based on historical data.

Using AI in trading is not something new, but the huge advancements in the field of AI has made it much more accessible and interesting. ValueWalk reported hedge funds managed by machine learning algorithms already outperform traditional hedge funds and increasing investments in this field indicate a growing understanding of the importance of machine learning in trading.

There are already multiple AI solutions for trading on the market. For instance, the Fintech startup Kavout has an AI driven investment platform that discovers tradable opportunities and makes informed decisions in order to find stock winners and avoid losers. Modulus is another company that is offering AI trading platforms.

What happens when everyone has prediction machines? Will everyone get the same predictions, leading no one to have an advantage in the stock market? Probably not. I believe there will be an endless race towards the best machine, and the solution

with the most accurate algorithm will achieve best long term results.

Another interesting aspect in terms of AI in trading is related to blockchain smart contracts (described in part 2). Combining these technologies can give great impact on the efficiency in the trade finance industry. AI can be used to analyze historical contracts in order to create new complex contracts, known as intelligent contracts. By looking through a huge number of contracts, the AI comes up with suggestion on terms and clauses, which helps the part come to an agreement. This way of using AI will free up bank staff and consequently lead to cost reductions. HSBC and IBM already developed this kind of solution in 2017, and today there are more companies offering intelligent contracts.

### 3.4.2 Banking

Chatbots, also called interactive agents, have been adopted by many banks. A chatbot is an AI which handles interactions with real humans. Customer service chatbots are increasing in popularity and it is easy to understand why. Replacing human workforce with a machine can lead to significant cost reductions, and due to the advancements in machine learning and NLP, chatbots have become very smart and functional.

They learn from their conversations and follow a complex set of algorithms in order to give accurate answers. Neural networks help chatbots to sort and label data, and to generate responses with a level of certainty

attached. In banking, most inquiries are generic, what makes chatbots very useful. However, most chatbots are not advanced enough to handle all support cases and they can also make mistakes, if the costumers inquiry is unclear.

Does a chatbot create value for customers, or does it only create value for banks through cost reduction? Whether or not your bank should implement chatbot in customer service, depends on the audience. Today, most of the people using chatbots are young and live in the US. Hence, before replacing staff, you should analyze your audience and figure out what their preferences really are. If you have the right audience, adopting a chatbot can give you more efficient customer experience.

Interactive agents fed with customer specific data can open up for new exiting opportunities and machine learning can be used in order to personalize the customer experience. AI is much better than humans at fast processing of data. Consequently, a chatbot will be able to give suggestions based on a better base of information than traditional customer service representatives can do. For instance, chatbots can tell customers how much money they spent on groceries the previous week and come up with suggestions on where a customer should by groceries in order to save more money. In other words, a chatbot can tailor offers and goals based on preferences and needs.

Due to the relatively easy development process and great advantages, there is a high number of different chatbots on the market. Some examples are Bank of America's chatbot Erica, JPMorgan's Coin, Wells Fargo's chatbot and Capital One's Eno.

Like chatsbots, AI assistants have been more and more accessible. This creates new opportunities within the field of banking. People always seek more efficient solutions and as speech recognition get better, people will truly increase their use of virtual assistant. In order to give a better customer experience, banks can offer services through virtual assistants. As an example, a collaboration between a bank and an AI assistant like Alexa, Siri, Cortana, or Google Assistant can enable customer interaction through voice. Hence, AI can simplify the way people interact with their bank and make bank information even more accessible. I will not be surprised if Apple starts working with a bank in order to offer mortgage via Apple Pay through their AI assistant, Siri.

Some banks are using machine learning algorithms in order to find out which customers are most likely to exit the relationship. By undertaking predictions based on a big dataset, banks can obtain valuable information concerning customers, and execute appropriate actions in order to keep them.

Lately, there have been some major advances in the field of deep learning. The technology has become pretty accurate, and

opens up for new fintech opportunities. Image recognition has entered the industry and this form of AI can be used to scan and verify identity documentation, invoices and so on. Consequently, image recognition can avoid identity fraud, as well as it can make more efficient payment processes for customers in terms of paper based invoicing.

Machine learning is also used to detect fraud. Billions of dollars are lost every year due to wrongly rejected customers. By applying machine learning algorithms, banks can detect fraud attempts more accurate and obtain better processes in terms of fraudulent transactions.

### 3.4.3 Investing

AI has also entered the field of investments. Robo-advisors are AI machines that provides algorithm-based financial advices in terms of wealth management and investment decisions. In similarity to AI in trading, Robo-advisors uses machine learning to analyze data and to learn from it. They often analyze portfolios, risk tolerance, market trends and investment history in order to give as good advices as possible.

Humans are still dominating the decision making in investments, but AI is taking a bigger role and much indicate that AI will take an even bigger role in the upcoming time. Partly because the technology develops fast and gives regularly more accurate predictions, but also because the decisions made by machines are not affected by individual incentives and interests.

Another aspect related to the increasing use of robo-advisors is the fact that robo-advisors service comes on a lower price than human investing professionals. This low-cost wealth management let investors earn a higher net profit than they would have done with a high cost service.

The rapid growth in robo-advisors started in 2010 and today there is a great number of fintech startups developing robo-advisors. Wealthfront, EquiBot and Wealthsimple are some of them.

There is no doubt the field of investments will be affected by the technological developments in the following time. What is interesting is to what degree human investments professionals will be replaced by machines and how machines and humans will work together in order to give the very best advice.

### 3.4.4 Lending

AI has a great potential in the lending market. Due to the size of the industry and the many manual processes, improvements in lending can create significantly value. Implementation of AI can lead to cost reductions, increased effectivity and more streamlined processes. Consequently, it is not a question whether AI will take over credit decisions, but when AI will replace all the manual processes related to lending.

Big Data comes with new opportunities. Many banks have huge amount of data about customers pay back history and preferences. Using structured data in

machine learning will increase their ability to assess people's creditworthiness.

Traditionally too many loans default and too many good borrowers do not get loan, due to the default risk. It can be very challenging to assess whether a potential customer will default or not. There are numerous factors affecting whether a borrower will default, and even with perfect information about the customer, there would still be a risk that the person or business not manage to meet all terms and conditions of a loan. By using machine learning algorithms banks can manage risk and reduce both credit losses and losses from fraud. Lenddo, Underwrite.ai, ZestFinance and Quifax are companies using AI and machine learning in order to evaluate creditworthiness.

The loan screening process is often time consuming and AI can reduce the screening period from days to minutes. Today there are several banks that are experimenting with automating credit decisions using AI and Sony Bank Inc., SoftBank, Mizuho Bank and Shizuoka Bank Ltd. are some of them.

Furthermore, AI can be used to improve customer experience, by analyze how fast a loan can be paid back using machine learning techniques. This usage will help customers reduce the down payment period and give them increased customer satisfaction.

Even though AI can improve lending, it is not unproblematic. The lack of transparency makes it hard to understand why some customers are rejected a loan and

regulations regarding equal treatment of customers makes it therefore difficult for AI implementation in lending decisions. Banks must be able to prove that they are not discriminating based on unreasonable characteristics. Since the technology develops fast, it will truly soon be transparent enough and banks should then be able to adopt the technology in order to stay competitive in the lending market.

In terms of debt collections, AI can be applied in order to make the process more efficient. By feeding an AI with data about past due lenders, the AI can optimize the collection process by suggesting contact time and method, or give lenders priority based on their likelihood to pay.

### 3.5 Conclusion

The third part of our series regarding development of Fintech strategy has focused on artificial intelligence (AI) in financial services. There is no doubt the implementation of AI can create value for financial institutions, but it also has its challenges due to strict regulations, limited transparency, and its missing ability to contextualize information.

In trading, machine learning can be used in order to improve predictions, by analyzing and learn from a large set of data. AI can discover tradable opportunities and make informed decisions in order to find stock winners and at the same time avoid stock losers.

In banking, chatbots are growing in popularity. These interactive agents use machine learning and NLP in order to learn from its conversations and generate accurate responses to customer's requests. Machine learning is not only used for chatbots, it is also used in order to avoid fraud and to decide which customers are most likely to exit the relationship. AI assistants built on speech recognition also has a very interesting potential in the field of banking.

In Investments, Robo-advisors have entered the market. They use machine learning to give algorithm-based financial advices at a lower price than human investing professionals.

In lending, machine learning can help banks assess people's creditworthiness, and hence reduce the amount of default and at the same time increase the number of actually good borrowers getting a loan. AI can also speed up the screening process and be used to give each customer useful information regarding their down payment period.

As we have seen, the potential for AI in the financial industry is huge. It has potential in literally all fields of finance, and as a participant in the financial market you should pay attention to the fast growth of artificial intelligence and the new opportunities that follows – they might give you a competitive advantage.



# Part 4

How can businesses within the financial industry benefit from RegTech?

## 4.1 Introduction to RegTech

RegTech is a branch of Fintech, and involves technologies that aim to help financial institutions manage regulatory compliance. In the aftermath of financial crises and scandals, extended requirements and expectations have appeared and led to a more complex environment for financial institutions. As a result of the high rate of change in regulations and laws, the field of compliance has been a big challenge for financial institutions and many are therefore looking into technologies in order to substitute manual risk and compliance processes with new, advanced technologies.

The following pages we will give you an insight into the field of RegTech, and our goal is to give you a better understanding of the advantages that comes when groundbreaking technologies and tools are applied in regulatory compliance and risk management.



### Part 4

What is Regulatory Technologies (RegTech)?

Which technologies are being applied in the field of RegTech?

Should you, as a participant in the financial industry, invest in RegTech?

What will RegTech look like in the future?

## 4.2 What is RegTech?

Any technology or digital solution developed to address regulatory challenges and help financial institutions to manage regulatory compliance, can be characterized as RegTech. The wide spectrum of regulations financial institutions face in today's environment, can be highly difficult to comply. RegTech aims to help businesses stay compliant in an efficient and low costly way.

After the financial crisis in 2008, businesses within the financial industry experienced increasing regulations and the need for better compliance processes became highly applicable. In Europe PSD2, MiFD 2, MIFIR and GDPR have just been implemented, and these regulations can also have impact on American financial institutions. With stricter and a more complex set of regulations, more companies fail to comply, and the cost of non-compliance has shown to be significant. Wells Fargo exposed the failure of regulatory compliance in 2016 and paid \$185 million in penalties. In an increasingly complex regulatory environment, the importance of improvements in the field of compliance are worthy every financial institution's attention. Luckily, the development of Fintech disclosed the huge potential for technology in the financial industry, and as the amount of technology in the sector increase, people start to realize that technology-based systems can give great advantages also in the field of compliance.

Since the entrance of RegTech, a lot has happened in the compliance space and today RegTech is a very promising field of expertise that is about to revolutionize the field of Fintech. Companies providing RegTech solutions are developing rapidly and today we see hundreds of companies offering solutions concerning regulatory reporting, risk management, identity management and control, compliance and transaction monitoring.

How is RegTech different from what has been done earlier in terms of technology in compliance? It is true that technology has been applied in order to improve compliance for a long time, but what is different is the design and the degree of flexibility. In contrast to the traditional, rigid solutions, RegTech aims to create scalable solutions that easily can be implemented and automated. A RegTech solution is built on advanced technologies and has the ability to go fast through large data sets and produce reports and analysis, without human interaction. In order to improve the efficiency and accuracy in the processes, RegTech companies building their solutions on groundbreaking technologies, such as blockchain and artificial intelligence (AI), as well as big data and visualizations techniques.

### 4.3 Technologies Applied in RegTech

AI has a particular interesting potential in the RegTech space. As described in Part 3 of our

Fintech series, Machine Learning, has a wide field of application in the financial industry. Natural language processing (NLP) uses machine learning techniques in order to understand human language. What is very interesting in terms of compliance, is the NLP technologies ability to interpret compliance and regulatory obligations. AI is better than humans at fast and accurate processing of big data, which makes it superior on monitoring regulatory changes in the space. Hence, implementation of RegTech solutions can result in more efficient and accurate compliance processes and reduce the need of human regulators. Machine learning techniques can also be applied in order to identify patterns and to predict relevant outcomes and risks, such as price movements. Beside the advantages of being efficient and accurate, RegTech built on AI can increase the responsiveness, by automatically identifying changes in regulations and further adapt dynamically. It also provides increased security through data encryption in information transmission, or through the implementation of more secure technologies, like blockchain.

As described in part 2, Blockchain can make a great impact on financial services. In the RegTech space, companies have started to build solutions on top of the new blockchain technology, which has its advantages. By using blockchain all actions are getting tracked and distributed. Hence, the process can be monitored in a better and more efficient way. With blockchain it becomes easier to verify compliance and regulators have immediately access to the updated

information on the blockchain without having to collect and update the documentation manually.

Cloud computing let businesses store their compliance data remotely, on an online, open platform, which allows real-time compliance and advanced analytics based on big data. For small institutions with limited available data, this could be particularly interesting, since larger sets of data, increase the accuracy of machine learning predictions.

Advanced data visualization also has an interesting field of application in terms of regulatory compliance. By combining interactive data visualization with analytics, users can easily get an overview of the current state of compliance, which makes the risk and compliance monitoring simpler.

## 4.4 RegTech Solutions

The number of companies offering RegTech solutions has been growing rapidly over the last few years. RegTech businesses deliver solutions with different purposes – from employee surveillance to fraud detection, and they target different customers – from banks to funds. The technologies being applied, differ from business to business, but they all aim to add value to financial institutions by creating innovative solutions for compliance and risk management. Figure 1, on the next page, gives an overview of how insurmountable the RegTech market is. There are hundreds of actors in the market

and some serve one single area, while others deliver solutions in multiple fields of expertise. In the upcoming paragraphs, I will give examples of some of the most influential RegTech businesses in the space.

### 4.4.1 IBM Financial Services & Industry Platform

IBM entered the space in November 2016, after the acquisition of the regulatory compliance firm Promontory Financial Group. IBM combines their advanced artificial technology with Promontory Financial Group's know-how in regulatory areas, in order to give financial institutions better solutions within the field of compliance.

IBM's AI, Watson, can process large data sets fast and make informed decisions based on training data and machine learning algorithms. Watson is able to detect changes in the regulatory environment and learn and improve from these changes.

IBM's six RegTech solutions primarily focusing on four areas:

- Financial Crimes and Conduct Risk
- Financial Risk
- Governance, Risk and Compliance
- Security and Resiliency.

In May 2018 IBM won two awards in the A-Team Group RegTech Awards. One for the best AI Solution for Regulatory Compliance and one for best Regulatory Alert Management Solution. IBM has already been a big player in the field of compliance and it is exciting to follow their further work in the RegTech space.

#### 4.4.2 RIMES RegFocus

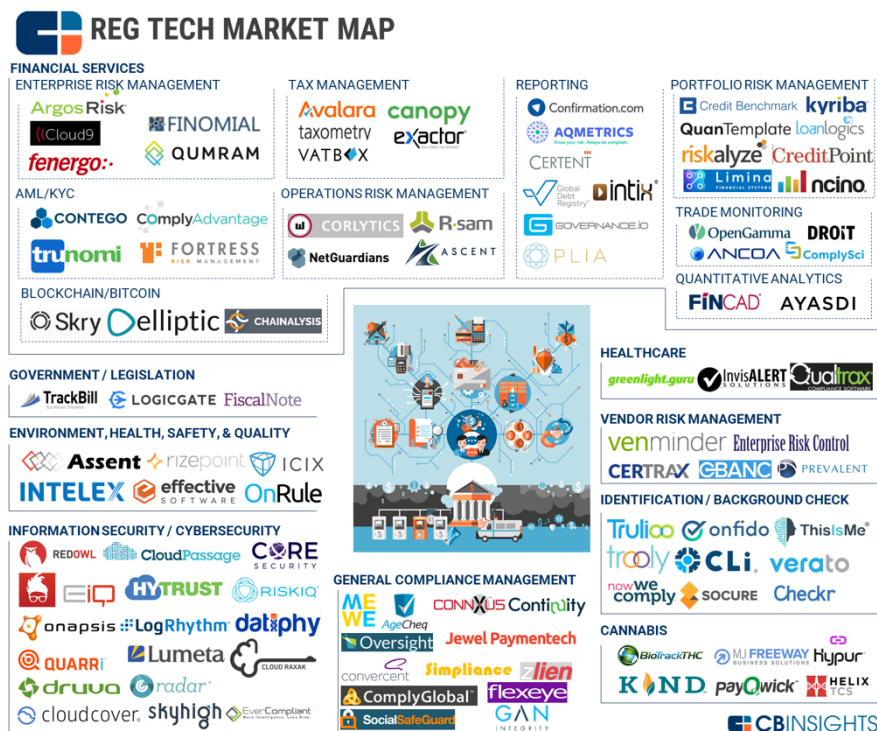
RIMES is an American company with more than 20 years experience with financial benchmarking and RegTech solutions. Their award winning solutions are built to streamline compliance and manage risks.

RIMES offer three RegTech solutions. RegFocus BMR Control aims to help asset managers, banks and insurance companies to comply EU's landmark Benchmark Regulation. RegFocus MAR handles the many complex challenges of Market Abuse, including the Market Abuse Regulation and MiFID 2 compliance. And RegFocus Market Surveillance is designed to deal with the risk of insider dealing and market manipulation.

#### 4.4.3 Thomson Reuters Velocity Analytics

Thomson Reuters Velocity is a market data analytics platform. The platform analysis financial and risk data and provides trade opportunities and risk management. In terms of compliance, it performs a real-time market monitoring and regulatory compliance checks for current and upcoming regulations. Reports for MiFID 2 compliance are created automatically.

Velocity Analytics is an advanced tool covering the entire trading lifecycle from market impact estimates to transaction cost analysis.



Figur 1: RegTech market map. Source: [CBinsight](#)

#### 4.4.4 Asset Control

Asset control are financial and data management experts, and has been working with Fintech since 1991. Today Asset Control delivers solutions to banks in 23 countries and they aim to help chief data officers and chief risk officers stand behind the integrity of the data they share in house, as well as to external stakeholders.

Asset Control deliver solutions for dealing with market data, risk and compliance. AC Plus enables financial institutions to meet the requirements of FRTB, MiFID 2 and BCBS 239. Lately, Asset Control was awarded best data management solution for regulatory compliance, by A-Team RegTech.

#### 4.4.5 Bureau van Dijk

Bureau van Dijk was established in 1991 and focuses on private company information, corporate structures and M&A deals. They have a wide spectrum of solutions, among them their solution for compliance and financial crime. Their compliance solution captures, analyzes and monitors data about approximately 300 million companies across the globe, and automatically creates reports in order to help managers with their decision making.

Their platform helps clients with compliance in terms of EU directives, anti-money laundering, FATCA and OFAC. Bureau van Dijk also provides an award winning data solution for tax compliance.

#### 4.4.6 Ayasdi

In contrast to the latter companies, Ayasdi is a more recently established company, founded at Stanford in 2008. They are working in the intersection of AI and Big Data, and has become one of the leaders in the enterprise-class AI. Their solutions are built on machine learning algorithms in order to solve different regulatory and compliance challenges.

Ayasdi's solution for Anti-Money Laundering find subtle patterns across multiple data types to reduce false positives, while their Model Accelerator aims to discover complex relationships, predict, justify, act and learn from its actions. It works by combining unsupervised learning with supervised techniques, which makes their solution very powerful.

#### 4.4.7 Trulioo

Trulioo is a global identity and business verification company that provides secure access to over 400 data sources worldwide in order to instantly verify consumers and businesses. Trulioo's data sources includes credit files, mobile network operators, public records, government data, business registers, mobile applications, consumer marketing and digital data.

GlobalGateway is Trulioo's service to help businesses comply with cross-border Anti-Money Laundering and Know Your Customer rules. They aim to help banks and financial institutions with their compliance, risk and verification problems.

#### 4.4.8 Encompass Compliance Corp.

Are your company performing drug and alcohol testing? If so, you should check out Encompass. Regulations in terms of drug and alcohol testing are complex with more than 10 000 separate laws and regulations. If these regulations are not being met, huge financial penalties can occur. Encompass Compliance Corporation provides real-time monitoring of changes within the space and provides tools to mitigate regulatory and compliance risk. Their service is not industry-specific, and can be applied in most industries in the US.

#### 4.4.9 CUBE

A very interesting company in terms of RegTech is the AI focused compliance company CUBE. They were founded in 2011 and were one of the first RegTech companies to recognize how extensive regulations in the financial industry would become.

CUBE provides a regulatory intelligence and change platform to customers across the globe. Their solution uses AI in order to understand the impact of regulatory change on businesses. The platform captures regulatory changes, figures out whether or not they have impact on a business, and acts by applying regulatory changes to maintain compliance.

#### 4.4.10 IdentityMind Global

IdentityMind Global is a RegTech company established in 2013. Their customers are financial institutions, crypto currency marketplaces and Fintech companies. IdentityMind Global builds digital identities

for risk evaluation and automates compliance in financial transactions. Their platform also maintains and analyzes identities worldwide in order to perform identity proofing, risk-based authentication, regulatory identification, and to detect and prevent fraud.

Their new solution, IdentityMind 2.0, is a digital identity platform designed to provide the industry's most accurate and efficient AML compliance results. IdentityMind Global uses their patented eDNA™ technology in order to securely track transactions and to provide a continual assessment of whether or not an identity should be trusted.

### 4.5 Should You Invest in RegTech?

No doubt, the technologies presented in this paper has a very interesting potential in terms of regulatory compliance and risk management. Still, RegTech solutions are not the right solution for every financial institution at this point of time. As described in Part 1: Innovation Strategy, how successfully a company can adopt new technologies, depends on their culture and leadership. For rigid, backward leaning companies it can be particularly difficult to achieve great advantages by adopting innovative technologies like AI or Blockchain. On the other hand, if your company has the right culture, with employees continuously seeking improvements through innovations, an adoption of RegTech solution will truly be beneficial.

You should also consider a number of factors concerning regulations in your company's environment.

If your company face a highly complex environment, with several regulations that changes rapidly, a RegTech tool can be of great support. However, you do not have to replace your entire human workforce of regulators and lawyers, but technological solutions can support humans and their manual compliance processes.

If your company operates a high amount of manual compliance processes, that has potentially high risk for your company, RegTech solutions will be appropriate.

RegTech will also be preferable if you have limited available data, or if you are struggling to find ways to handle the data in order to improve your compliance and regulatory processes.

## 4.6 What is the Future of RegTech?

Is RegTech just another buzzword? I will say no. Indeed, the future of RegTech looks very promising and if you are in the financial industry, it's definitely worth looking into the fast growing field of RegTech. As we have seen in the previous pages, the field of application is wide and gives great advantages in the financial industry, due to its computational superiority, flexibility, and increased security. Still RegTech is in the initial phase, and even though the solutions,

as they are described in section 4, are good, they will truly become much better, fast.

As AI and the Blockchain technology develop, we will truly experience an expansion in the field of RegTech.

Considering the increasing complexity with stricter regulations and the high amount of manual compliance processes we experience in today's financial industry, the potential is huge, and the RegTech revolution has just began.

## 4.7 Conclusion

The forth part of our series regarding development of Fintech strategy has focused on Regulatory Technologies (RegTech).

RegTech involves any technology or digital solution developed to address regulatory challenges in the financial industry. Financial institutions face a complex environment in terms of regulatory compliance, and RegTech companies aim to help businesses stay compliant, by applying advanced technologies in digital solutions. Their services can help financial institutions deal with compliance processes and risk management in an efficient and low costly way.

Technologies applied in RegTech are mainly artificial technology, blockchain, data visualization and cloud computing. There are hundreds of solutions in the RegTech space, and their use of these technologies varies. As shown in chapter 4, Machine learning is widely used, both for predictions of outcomes and risks, and for automatic

interpretation of compliance and regulatory obligations.

The future of RegTech is very bright, and today most of the solutions are built on early stage technologies. However, adoption of RegTech can already give you great advantages in terms of increased responsiveness, more efficient and accurate processes, and better security. As technologies develop, we will experience even greater benefits from RegTech solutions, and even though your company is not ready to invest in RegTech at this point of time, you should keep up with the rapid growth and developments in this particular space.

For every business in a highly regulated industry – RegTech should be of great interest.

# Part 5

What is the current state of  
cyber security in the financial  
industry?



2014

**JP Morgan Data Breach**

One of the largest data breaches in history with 83 million customers affected.

**Carberp Trojan**

In 2015 Cyber experts discovered a two year long attack, resulting in more than a billion dollars stolen from 100 banks around the world.

2015

2016

**SWIFT Hack**

Mysterious attackers tried to steal \$951 million from Bangladesh's Central Bank.

**Petya Cyber Attack**

A massive attack at government infrastructure in Ukraine. Ukraine's National Bank, airports and state power station were hit by attackers.

2017

2018

**Coincheck**

World's largest digital currency theft. The Japanese currency exchange says attackers stole \$534 million in virtual assets.

**UK banks**

Seven of the UK's biggest banks were targeted by co-ordinated cyber attack. Costed the banks hundreds of thousands of pounds.

## 5.1 Introduction to Cyber Security

We will now focus on Cyber Security in the financial industry. As the timeline on the previous page shows, there has been some major data breaches and cyber attacks in the industry the last few years. Millions of people have been affected and enormous amounts of money has been stolen. Even though most attacks are financial motivated, some are categorized as cyberterrorism, undertaken in order to create chaos and fear. The series of powerful attacks on Ukraine's infrastructure in 2017 is an example of the latter. Cyber attacks with substantial outcome are attracting media's attention, but most attacks have less public interest and are absent in traditional media. That doesn't mean they do no harm to businesses. They still pose a significant risk and innovative challenge for businesses.

As we have pointed out in the previous parts of our series ***Develop Your Fintech Strategy***, Fintech is in great growth. New technologies are being adopted by financial institutions and processes and systems become more accurate and efficient. There are a bunch of positive aspects with technology adoption, but everything has its drawbacks and technology is no exception. Implementation of digital solutions opens up for new possible cyber threats and give hackers more ways to perform a data breach.

Financial institutions are attractive targets for cyber attack. Hence, Cyber Security should

be kept in mind when you establish your Fintech strategy.



### Part 5

Why should financial institutions increase their focus on Cyber Security?

What are today's security trends in terms of Cyber?

What are the most serious cyber threats for financial institutions?

## 5.2 What is Cyber Security?

Cyber Security is all about keeping your data, software and hardware safe from theft or damage. A data breach can result in loss of reputation, assets, and information, which can have huge negative impact on your business. Hence, protection of vital information about customers, employees, operations, products, and systems is highly important in today's competitive world. The field of cyber security aims to provide reasonable assurance when facing malicious actors.

In addition to security in the digital space, cyber security also include security in terms of physical access to hardware systems.

Cyber Security experts often discuss vulnerabilities and even more important, exploitable vulnerabilities. Vulnerabilities in a cyber perspective can be defined as weaknesses with a current digital system, and can be related to design, implementation, processes or control systems. If a particular vulnerability can be exploited by a hacker, we say it is an exploitable vulnerability.

### 5.2.1 Types of cyber attack

Hackers use multiple ways to attack their targets and their methods vary in complexity and sophistication. A brief description of some of the most common types of cyber attack in the financial industry follows.

**Backdoor attacks** are cyber attacks where attackers find a backdoor into the computer system, and manage to avoid the normal authentication and security processes. These attacks usually come as a consequence of weaknesses in the design and configuration.

**Denial-of-service attacks** (DoS) are attacks designed to prevent the rightful user to get access to the system. Common ways to execute DoS attacks are either to enter wrong password for an individual user enough times to lock the account, or the attacker can overload the machine capacity resulting in unavailable login for all users.

When an unauthorized user gains access to a data system, we call it **direct-access attacks**. An attacker can obtain access through physical access to the hardware, or by making operating software modifications

using viruses and bugs like worms, keyloggers and covert listening devices. As soon as attackers have access they are likely to copy information or modify computer systems.

**Malware attacks** involves special designed software that aims to steal or destroy data. Viruses, worms, Trojan horses, ransomware, spyware and adware are examples of malware.

**Man in the middle** (MITM) is a cyber attack where an attacker insert itself in the middle of a conversation between two parties, and manipulate the conversation in order to obtain sensitive information. The two users still think they are communicating with each other, but they are actually communicating with the middle man.

Since passwords still are the most used method to authenticate users, **password attacks** are a common strategy for attackers. There are mainly two methods used for password attack, Brute-force and dictionary attack. The first method involves using a software to randomly guessing different combinations of letters, numbers and commonly used passwords in order to crack the password. Dictionary attacks use combination of words from a dictionary in order to log in.

**Phishing** is a method where the attacker tries to acquire sensitive information from users by using emails and websites. The attacker aims to trick the target to send information such as usernames, passwords,

credit card details etc. These attacks have shown to be pretty sophisticated. The attacker pretend to be a trusted entity, like an employee, friend or another plausible person, and it can be difficult to actually understand it is an attack without talking to the real person.

**Eavesdropping** involves surreptitiously listening to a private conversation. This form of attack can be done over phone, email and chat.

**Jackpotting** involves an attack at an ATM, where the attacker installing a malicious software and hardware onto an ATM. The malware give them control over the ATM and the attacker can then force the machine to dispense cash quickly.

### 5.3 Why Should Financial Institutions increase their focus on Cyber Security?

We live in a digital world, surrounded by digital products, platforms and solutions. Businesses today rapidly adapt new technologies in order to achieve a competitive advantage in a highly competitive environment. Fast development and adoption of new technologies can potentially lead to increasing number of security vulnerabilities and flaws. The risk of cyber attacks cannot longer only be a job for the IT department. It must be a part of the organizational culture and rooted in the strategy.

Beside the increasing number of potential security flaws, there are indications of increasing security threats. First of all, we experience an increasing complexity in the global environment, with great powers trying to strengthen their position through intelligence operations and sabotage in the digital space. Many attacks come from Russia and China, but also North Korea has their own cyber-army, which has become a big cyber threat for western governments and financial institutions.

Another potential threat is the increasing number of internet users. Today more than 4 billion are connected to the internet, which means nearly half of the world's population still live unconnected. The growth rate in internet users are high, and as the number of users increase we can expect increasing number of attacks in the digital space.

Increasing threats and rapid development in technologies makes cyber security to a field every financial institution should focus on in the upcoming time. KPMG's 2018 U.S. CEO Outlook pointing at Cyber Risk as the top risk for today's businesses, no matter industry. And as much as 68% of CEOs believe it is a matter of when and not if. For financial institutions, which are attractive targets for hackers, there is no doubt Cyber Security should be a priority, and kept in mind when new technologies are being considered.

## 5.4 Cyber Security Trends in the Financial Industry

The technology sector has been growing rapidly. New advanced technologies have entered the market and the field of Fintech has increasing importance in the financial industry. As new technologies are adopted, the field of Cyber Security must adapt to new vulnerabilities and attacks. Hence, the rapid growth in technology, is a driving force for the massive growth in the field of Cyber Security. New trends come and go, and the next paragraphs will point out some of the trends we see in the field today.

### 5.4.1 Proactivity

As a result of the major ransomware attacks we have experienced lately, businesses in all industries have opened their eyes for the catastrophic consequences of an attack. Wannacry in 2017 and Petya in 2016 hit thousands of computers and resulted in damages worth billions of dollars. The need for backup routines and regularly updates came into people's mind and forced organizations to go over their routines in terms of cyber preparedness.

### 5.4.2 Adoption of More Advanced Technologies

We have earlier discussed the potential of groundbreaking technologies like Artificial Intelligence and Blockchain to financial institutions. In terms of Cyber Security, AI can be of great support for security professionals. Banks usually have a lot of data, and by applying machine learning algorithms, the

data can be used to discover weak points and vulnerabilities before they are exploited. It can also be used to predict whether a transaction is genuine or not. There are a bunch of AI solutions for fraud detection and identity theft, and there will truly be even more as the technology becomes better and more intelligent.

Also Blockchain has a wide field of application, and it is secure by design. Blockchain is decentralized and distributed, which makes it nearly impossible to manipulate or destroy. It is highly likely that we will see more use of blockchain for transactions in the upcoming time.

### 5.4.3 More Advanced Attacks

Unfortunately, advances in technology also lead to more advanced attacks. Usually hackers are forward leaning and ready to make use of new technologies pretty fast. They always aim to stay one step in front of researchers and Cyber experts, which can be frightening in a security perspective.

We have already seen examples of hackers using AI in cyber attacks. Data scientists from security firm ZeroFox, studied how AI can be used in order to create phishing tweets, and they figured out artificial hackers based on machine learning was better at creating posts with malicious links.

There are several ways attackers can take advantage of rapid developments in AI, and password attacks, phishing, and malware creating is just some of them.

In terms of malware, hackers have started to use more innovative macro tactics, to attack banks. Last year researchers observed a bank Trojan that used malware macros to evade Sandbox detection.

There is also a potential cyber risk in Internet of Things (IoT). IoT uses sensors to collect data, communicate, analyze and act on information. IoT devices can be commanded to undertake a coordinated attack at vulnerable systems. This can possibly lead to very dangerous situations. In the financial industry IoT is still in a very early stage, but the technology can be used for payments, in blockchain smart contracts, for authentication, and for banking at home.

The use of AI Assistants creates another potential vulnerability. Recently, it was discovered that Amazon Echo, which uses “Alexa” software, had recorded and sent a private conversation. This is problematic in a security perspective, since it opens up for a potential eavesdropping attack. Several banks are looking into AI Assistant banking services, and making a hundred percent secure service will be essential.

#### 5.4.4 Multi-Factor Authentication

Password attacks are common, and AI can make it a lot easier for attackers to crack your password. Therefore, it is important to use multi-factor authentication. AI powered biometric authentication can use voice, fingerprint, retina and face scans, instead or in addition to normal passwords.

I believe we will see increasing use of more advanced authentication systems in the financial industry in the upcoming time.

#### 5.4.5 Regulations

New cyber security regulations are being rolled out all over the world and some of them also affect financial institutions in the US.

Last year (2017) China’s Cybersecurity law was put into effect, and the Cyber Security Agency in Singapore proposed their Cybersecurity Bill a month later. General Data Protection Regulation (GDPR) was put into effect in 2018 and gives consumers more rights and ownership over their data. Every organization that store data about European citizens must follow to the new regulations. Many will truly fail to comply with GDPR, which will be very costly.

#### 5.4.6 Competence Shortage

There is shortage on competence in the cyber security industry. As businesses understand the real importance of cyber security and the massive consequences an attack can result in, financial institutions will experience challenges filling their new security positions, due to the relatively high demand.

We experience an increasing interest for Cyber Security among consulting firms. They are collecting highly professional expertise for their advisory services, and educate talent themselves. Due to the shortage of experts in the industry and the increasing priority among consulting businesses, we expect

more outsourcing of Cyber Security in the upcoming time.

## 5.5 Cyber Threats to the Financial Industry

As we already have pointed out, most cyber attacks are financial motivated. The more sensitive data and valuable assets a business holds, the more likely it is to be attacked. Banks and other financial institutions have both sensitive information and money, and they are consequently a major target for financial motivated attackers. Banks are also a naturally target for cyberterrorism, since a successful attack can create chaos and decreasing trust. There is no doubt financial institutions face many threats in the digital space, but what is the biggest threats right now, and where are they coming from?

### 5.5.1 Changing Landscape

Today's banks operate in highly complex environment with rapid changes. The risk landscape in 2018 is quite different than what it was only a few years ago. Attackers experiment with new methods and discover new vulnerabilities as soon as they occur.

Managers have to be up to date, and continuously following the developments in the field of cyber security. To be backward leaning in a constantly changing threat landscape, can be very dangerous and highly costly.

### 5.5.2 Third- and Fourth-Party Cybersecurity Risk

To monitor your vendors can be hard, especially for large financial institutions. In order to protect your data, you should have clear defined routines and control of who has access to your data.

Even though it is hard to monitor your vendors, it is even harder is monitoring fourth parties. Your vendor's third parties can pose a threat, and should, in line with your own vendors, be monitored. If a fourth party is out of play, due to a cyber attack, how will it affect your third party, and further how will it affect your own business?

A well developed vendor management plan can help you manage these threats.

### 5.5.3 DDoS Attacks

Initially, I presented denial-of-Service (DoS) attacks, which aim to disrupt services of a host connected to a network. Distributed denial-of-service (DDoS) attacks are increasing in popularity among hackers. It occurs when a portion of a network is targeted by incoming traffic from many different sources, usually resulting in very slow network or a completely crash and downtime.

Financial institutions can lose enormous amounts of money due to downtime. DDoS attacks are increasing in scale and pose a serious threat since it is relatively easy to execute. In April 2018 seven of the UK's largest banks were hit by a massive DDoS

attack, resulted in reduced operations, downtime, and hundred of thousands of pounds in loss. The attackers used a software that could be rented for as little as 11 pounds. DDoS attacks are cheap, simple to carry out, and therefore a big threat for financial institutions also in the US.

#### 5.5.4 AI

As described in paragraph 4.2, cyber attacks become more sophisticated with more advanced technologies, and there is no way to discuss potential threats without mentioning artificial intelligence. Fintech companies are working hard to come up with groundbreaking AI solutions for security proposes, and the industry fears that skilled hackers can get ahead in the AI technology race. If they do, they can use their AI to discover exploitable vulnerabilities before cyber security experts find them.

#### 5.5.5 Jackpotting

Lately, cyber attackers have started to target ATMs. Earlier this year the first “jackpotting” attack was executed in the US. Criminals have figured out a way to exploit a vulnerability in banking, and just the first week they stole over \$1 million dollars. This shows that cyber attacks are coming n new creative ways, which is problematic in a time were more services become digital.

#### 5.5.6 State Supported Attacks

Intelligence services report increasing focus on cyber warfare. Cyber is both a cheaper and faster method of warfare, and many states have started to use cyber as a way to

attack their enemies. Nation state attacks are not only targeting government infrastructure, they also attack businesses and organizations, in order to create chaos, gain sensitive information, and to finance their activities.

Russia is one of the most active actors in terms of state supported cyber attacks, but also North Korea, China and Iran have dedicated cyber armies that pose a threat for American financial institutions.

## 5.6 Conclusion

The fifth part of our series regarding development of Fintech strategy has focused on Cyber Security in financial services. Cyber is definitely one of the top risks for businesses today, and the consequences of a data breach can be enormous. Since the financial industry is a main target for attack, managers within the financial industry should be aware of the threats and keep up with the fast growing Cyber space.

Many financial institutions today aim to gain a competitive advantage through innovative technologies. Adaption of a new technology can improve business processes and platforms, but also potentially lead to new vulnerabilities, which in some cases are exploitable. Since the beginning of the digital revolution, hackers have detected exploitable vulnerabilities and carried out targeted attacks. As we have seen, millions of

people have been affected and huge amounts of money has been stolen, due to successful cyber attacks.

Cyber Security is an ever changing field of expertise, and it can be hard to keep track with new trends. There is increased proactivity among managers and cyber experts are taking advantage of new groundbreaking technologies, like AI and Blockchain. Cyber security regulations are also being rolled out all over the world, and point out the importance of established routines in the digital space. Even though, the focus on cyber is increasing, there is also a competence shortage in the industry, and as more managers understand the importance of highly competent cyber specialists, we expect there will be more outsourcing of cyber security.

Financial institutions are facing a wide spectrum of cyber threats. One of the biggest threats involve the changing risk landscape. If companies do not keep track with new methods and techniques used by attackers, they will be a more attractive target.

Most businesses monitor their own processes and data flows, but are failing in monitoring third and fourth parties, which can be crucial. If a vendor is put out of play, as a result of a cyber attack, it can have impact on your daily operations. Other potential threats in 2018 are DDoS attacks, jackpotting, AI attacks and the increasing number of state supported attacks.

A cyber attack can be highly costly and end up in new investments, management replacement, public relation expenses, as well as huge marketing campaigns. Being proactive can be very valuable, and cyber security should therefore be taken into count when you develop your Fintech strategy.

## Contact

To learn more, contact:

### **Brett R. Noyes**

Managing Director at Unbank.Ventures

**P** 509-910-3496

**E** [brnoyes@unbankventures.com](mailto:brnoyes@unbankventures.com)

**Skype** noyeslimited

## Author / Photographer

### **Andreas Orset**

Consulting Intern at Unbank.Ventures

**P** 0047 938 29 158

**E** [andreas@unbankventures.com](mailto:andreas@unbankventures.com)

**Skype** a.orset

**Website**

<http://www.unbankventures.com/>

**Headquarter**

San Francisco, California

**Specialties**

Fintech, accelerator, incubator, and venture capital

**Year founded**

2016

**Company type**

Partnership

**Company size**

2-10 employees