



EBOOK

The State of Fintech and Fraud in 2019



SEON Technologies Ltd.
seon.io

info@seon.io
0044-20-351-44790

Table of content

EXAMINING CURRENT AND FUTURE TRENDS FOR THE SECURITY OF ONLINE BANKING, INSURANCE, LENDING AND PAYMENT PROVIDERS.

1 WHAT IS DRIVING THE FINTECH BOOM

- 1.1 Acceleration of the Mobile Economy
- 1.2 Increase in Payment Channels
- 1.3 Meeting Customer Standards
- 1.4 Tapping Into Transactional Data
- 1.5 Reaching Global and Emerging Markets
- 1.6 Investor Interest

2 KEY TRENDS FOR THE FUTURE OF FINTECH

- 2.1 A Shift from Disruptor to Partner
- 2.2 Banks Will Continue to Open Up
- 2.3 Tailored Services Become the Norm
- 2.4 A Race to Reduce Customer Friction
- 2.5 New Regulations Transform the Playing Field
- 2.6 Advanced Technologies Become Integrated

3 FINTECH'S INCREASING RANGE OF DIGITAL THREATS

- 3.1 More Cybersecurity Attack Options
- 3.2 Online Fraud Becomes Costlier

4 FRAUD FIGHTING FOR FINTECHS

- 4.1 A Typical Fraudulent Journey
- 4.2 The Three Key Touchpoints
 - 4.2.1 New registrations
 - 4.2.2 Login Authentication
 - 4.2.3 User Action
- 4.3 Deploying the Right Fraud Fighting Tools
 - 4.3.1 Email Profiling
 - 4.3.2 Device Fingerprinting
 - 4.3.3 Other Data Enrichment for ID Profiling
 - 4.3.4 Machine Learning: Connecting the Data Dots

5 KEY TAKEAWAYS

Introduction

12,000

estimated number of fintech startups worldwide ([Statista](#))

\$ 4,7 T

estimated worldwide fintech market ([Goldman Sachs](#))

\$ 150 B

value of the biggest fintech in the world, Chinese company Ant Financial ([CNBC](#))

88 %

percentage of legacy banking organizations who fear losing revenue to fintech startups ([PWC](#))

\$ 380 B

estimated market value of currently unbanked civilians around the world ([Raconteur](#))

Fintechs are already completely transforming the financial landscape. There are now more than 12,000 fintech startups worldwide, and [Goldman Sachs estimates the worldwide fintech market to be worth \\$4.7 Trillion.](#)

Redrawing the lines of the financial industry, however, does not happen overnight, nor without disruption. Following the 2008 credit crisis, an **increase in regulations, heavy non-compliance fines and penalties created the perfect momentum** to punish legacy banking institutions, and foster innovation with the young newcomers.

In this ebook, we'll examine the disruption caused by fintech startups, the adjustments made by large financial institutions, and the challenges faced by both types of organizations - with a specific focus on the increasing burden of online fraud.

What is Driving the Fintech Boom

THE BROADER FINTECH CATEGORY CAN BE SEGMENTED INTO FOUR VARIANTS

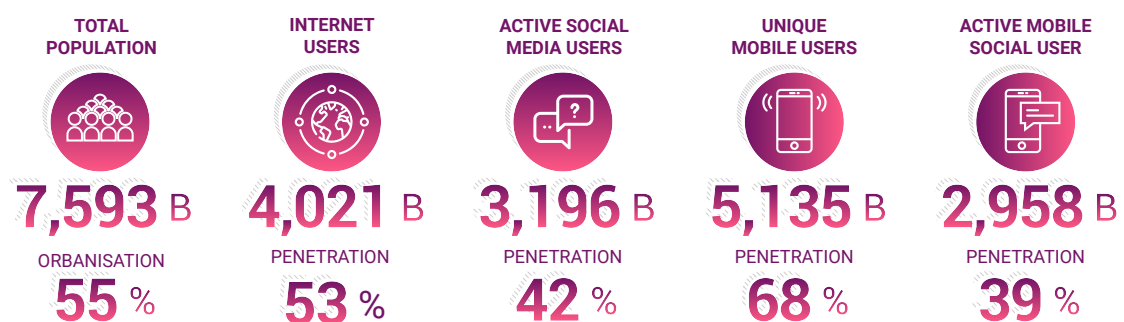
Origin	Technology	Infrastructure providers seeking to help financial institutions digitize and modernize their technology stacks Examples: FNZ, Marqetta, Onfido	Large technology ecosystems using financial services to strengthen relationships with users Examples: Apple, Ant Financial, Tencent
	Financial services	New entrants, startups, and attackers seeking to enter financial services using new technologies. Examples: SoFi, TransferWise, LendingClub	Incumbent financial institutions making significant investments in technology to lift their game Examples: Wells Fargo, Ping An
		Low	High
		Scale	

McKinsey & Company | Source: McKinsey analysis

Aside for the aforementioned catalyst that was the 2008 credit crisis, a number of market forces are creating the ideal ecosystem for fintechs to flourish, whether they are challenger banks or online loan providers.

1.1 ACCELERATION OF THE MOBILE ECONOMY

DIGITAL AROUND THE WORLD IN 2018



The world's ongoing appetite for smartphone use is without a doubt driving the transition from a cash-driven society to one that favours digitized financial services. According to the GMSA 2019 report of the state of the mobile economy, the number of mobile internet users is expected to reach 5 Billion by 2025, growing at a CAGR of 4.8%.

And the list of digitized financial services continues to grow. While nobody would have imagined using a QR code to say, pay for an electricity bill a decade ago, it is just one of the numerous processes facilitated by mobile adoption, along with loan application, mobile banking and insurance purchases, amongst others.

1.2 INCREASE IN PAYMENT CHANNELS

These days, even your local corner coffee shop needs to offer in-store as well as desktop and mobile ordering options. This means accepting physical payment in cash, credit, debit, gift cards, as well as digital payments from mobile wallets on phones and wearables, money transfers from apps, and sometimes even in a variety of cryptocurrencies.

Here is, for instance, a list of the payment methods accepted at Starbucks, according to their website:

- Gift cards
- Starbucks Mobile App
- Chase Pay
- Apple Pay
- PayPal
- Visa Checkout
- Credit Cards
- Cash.

All of these forms of payment need to occur instantaneously, while ensuring security, reliability, and integration across the business's other systems. For many firms, offering such a complex web of payments options requires working with third-party fintechs that offer point-of sale hardware, cloud-based software solutions, or payments infrastructure to facilitate these transactions.

1.3 MEETING CUSTOMER STANDARDS

Friction increasingly becomes the battleground where customers are won or lost. And fintechs were quick to realize that a seamless user experience is now a must for organizations. Challenger banks such as TransferWise, Revolut or Mondo, who benefited from reforms such as the Financial Services Act of 2012 in the UK, are now renowned for their ease of use, flexibility, and online-only operations.

This fantastic user experience is now setting the bar for other organizations. **Customers want to access financial products and services fast, at all times, on-the-go, and seamlessly.** Whether it's to apply for a loan or request an insurance quote, waiting in line at a brick and mortar location that only opens during working hours is increasingly unacceptable.

BRICK AND MORTAR VS ONLINE BANKING

Customer advantages: <ul style="list-style-type: none"> • No waiting, quick processes • Less printing and paperwork • On-the-go, no travel needed, can even use foreign companies • Cheaper, because less human resource is used • No human error in the process 	Business advantages: <ul style="list-style-type: none"> • Automated processes, less workforce is needed • Smaller office is enough, no space needed to work with clients • Ability to go international easily, scaling
Customer Disadvantage: <ul style="list-style-type: none"> • Complex issues are more difficult to solve • Intangible, feeling of insecurity • Unknown threats, more difficult to be up-to-date and prepare • No personal connection • You need to be digitally literate, older people might find it more cumbersome • Secure internet connection is needed 	Business Disadvantages: <ul style="list-style-type: none"> • Solving complex issues over phone or e-mail might be a problem • Server issue, or internet problem can lead to complete crash, backup is incredibly difficult when customers do not have the option to come in to a store • Complex security issues

1.4 TAPPING INTO TRANSACTIONAL DATA

As a well known [article from the Economist claimed in 2017](#),

„data is now the new oil.“

While smartphones and digital tools continue to provide abundant sources of data, fintechs are in the perfect place to tap into the transactional information that every customer inevitably creates - giving them a clear advantage over slower, less agile traditional institutions.

As we'll see in our future trends section, big data is a key tool for fintechs to provide better and more efficient service to customers. **Whether it's for customer segmentation, personalised services, risk management or fraud detection, transactional data has tremendous business-boosting value for fintechs**, and that source isn't set to dry out any time soon as the world's digital footprint continues to increase.

1.5 REACHING GLOBAL AND EMERGING MARKETS

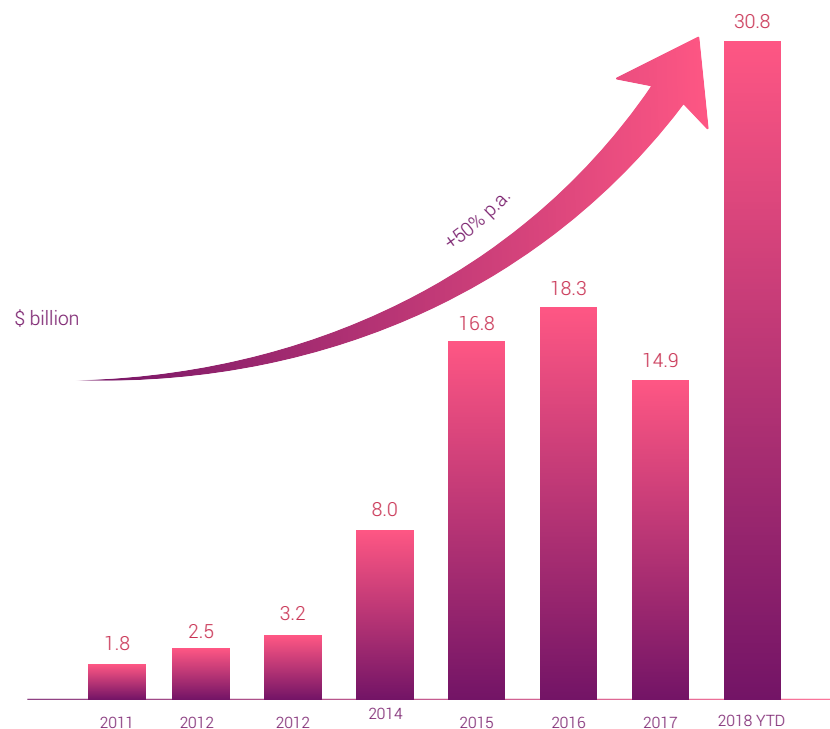
Fintechs with digital-only strategies enjoy highly scalable platforms because the majority of their costs are in the initial software development and infrastructure buildout. Additional customers require little incremental cost.

For instance, let's look at the example of tax preparation software. The cost of adding a new client is essentially zero: the software is already built no matter how many clients there are. There might be server and storage expenses, but in the digital age these costs are negligible, especially when contrasted with a traditional tax prep firm where every additional customer requires setting up a new, fully staffed branch to set up accounts.

This flexibility of scale is also what makes fintechs so suited to emerging markets. Previously, many users there were ignored by insurance companies, tax firms or banks, because they would be too expensive to access. These days, fintech firms are the best-positioned to [capitalize on this \\$380B opportunity](#).

1.6 INVESTOR INTEREST

GLOBAL VENTURE CAPITAL INVESTMENT IN FINTECHS



McKinsey & Company | Source: CB Insights; McKinsey analysis

According to McKinsey, funding for startups in the banking, insurance, lending and payment sphere increased at a compound annual growth rate (CAGR) of 50% between 2011-18. This represented over US\$30.8 billion in cumulative investment.

VCs, in short, love fintechs. In fact, the market now includes 30 VC-backed unicorns, worth a combined \$147.37 billion. As the money pours in, it attracts more competitors, fueling innovation and growth for the organizations that manage to stay ahead of the customer-traction game.

Key Trends

for the Future of Fintech

50 %

percentage of global payments predicted to flow through fintech channels by 2022 ([McKinsey](#))

\$ 200 M

investments poured into regtech companies since 2017 ([FinTech Global](#))

80 %

percentage of large banks set to support fintechs application development through open banking ([FData](#))

50 B

number of devices to be connected to the Internet (IoT) by 2020 ([Cisco](#))

To better understand where fintechs are headed, we aggregated and analyzed the insights of industry leaders in a variety of verticals such as digital banking, payment gateways, and added our own data as fraud prevention experts. Below are the points most touched upon, in order of importance:

2.1 A SHIFT FROM DISRUPTOR TO PARTNER

By far the most repeated prediction involves the changing nature of the relationship between fintechs and traditional financial institutions. **Fintech companies will shift from disruptors to partners in the financial services world**, bringing a synergy of strengths to the industry.

According to payments experts, by 2022, at least one in two transactions is likely to flow through channels not owned by banks but by a multitude of digital ecosystems, FinTechs, and other third-party interfaces, thanks to Open Banking and the rapid rise of digital channels.

Fintech partnerships should also allow companies to grow. One point [emphasized by The Financial Brand](#), for instance, is that **fintechs currently lack the ability to scale due to a lack of brand recognition. This is all set to be a thing of the past once they partner with banking leaders.**

However, we should note that banks and credit unions are still cautious around partnerships, [and sceptics abound](#). Their real goal is to find the right mix of fintech solutions and traditional banking and to play to the tried and true strengths of each type of organization while also opening up to new opportunities to access tools that will empower consumers and reinvigorate marketing opportunities.

This collaboration will involve the rise of regtechs, or regulated technology startups. As more and more technologies will be deployed to help companies comply with regulations that govern the fintech sector, we can also expect the boundaries between banking and the rest of the digital economy to continue to blur.

2.2 BANKS WILL CONTINUE TO OPEN UP

New regulations, such as **Europe's PSD2, will continue to fragment traditional retail asset and liability gathering in most markets.** Open Banking, which refers to the unbundling of traditional banking packages, is set to continue creating new business opportunities and to transforming banking's competitive landscape, primarily through the power of open APIs.

While for decades banks have sought to become more "vertical," offering services from top to bottom, many new entrants want to be "horizontal," dominating a lucrative specialty. They're going after things like account aggregation or back-office enablement, which historically all made a small part of a banking giant's series of financial services.

In the UK alone, there are currently 62 registered third-party providers who plan to take advantage of a fragmenting value chain. Stripe, now a leader as a 7-year-old specialist payments, commands [a valuation which isn't too far from that of Deutsche Bank](#) – a sign that horizontal can be very attractive. The upcoming years will see more fragmentation – and possibly efforts to re-bundle those components.

2.3 TAILORED SERVICES BECOME THE NORM

According to industry leaders, **fintechs will increasingly leverage data to create tailored services based on individual profiles rather than demographic-based clusters.** This segmentation means financial services will be recommended not based on generation such as young people, millennial or older users. It will be based on lifestyles, values, aspirations, mindsets and underserved needs.

Many banking and insurance organizations, for instance, will develop individualized communication and experiences for the segment of one. This is the ultimate level of innovative personalization allowed through data, advanced analytics and digital technologies.

Finally, it's worth pointing that serving a segment of one is not limited to individual consumers. Banks and credit unions will also focus their efforts on the small and medium enterprise (SME) segment and the needs of individual businesses.

As it stands, a number of financial services organizations are already taking the same approach as tech giants like Facebook or Google, leveraging insights and data derived from services and individual organizations to boost their core business.

2.4 A RACE TO REDUCE CUSTOMER FRICTION

One key consequence of the customer-focused approach is that the services will increasingly be designed with ease of access in mind. As opposed to technology taking a secondary position, supporting only the processing of transactions, future technologies will be more customer-centric and efficient, providing more targeted, secure and intelligent solutions through a frictionless experience.

„Friction, in fact, will become the new battleground where users are won or lost”

Friction, in fact, will become the new battleground where users are won or lost as financial service providers increasingly find a clear correlation between their quality of customer experience and business performance metrics. Like with the retailing industry, consumer expectations and the cost of alternative forms of delivery will redefine the way the banking industry is structured. Whether it's through faster credit scoring or AI-driven assistance, users will want to access services fast, on-the-go, and at all times.

Artificial Intelligence will therefore continue to be deployed in a variety of verticals and a variety of scenarios, from assisting with customer service, fraud management, to improving the precision of marketing targeting. Fintechs will not just craft journeys that begin when a customer comes looking for a loan to finance that asset - the journeys will begin as early as when they express an interest in purchasing that asset.

2.5 NEW REGULATIONS TRANSFORM THE PLAYING FIELD

One consensus from experts and industry insiders is that **regulatory complexity within countries and across regions is set to increase**, changing the current “winner takes all” approach that local fintechs have historically benefited from.

For example, with money transfers, regulatory approval in a single EU country was used across other EU countries. This encouraged many cross-border payments start-ups, such as WorldRemit and TransferWise in the UK, to expand into neighboring European countries before moving across the Atlantic, which requires additional regulatory investment.

But individual US states require licenses for money transfer, which makes US expansion more cumbersome for European operators. It is a pattern we see repeated across a number of regional markets as they mature. To successfully enter new markets, fintechs will need to adapt to growing sets of market dynamics and government regulations. **They will need to carefully select new markets based on a clear understanding of regional variations to avoid bans and heavy fines at the local level, which could damage a global expansion.**

2.6 ADVANCED TECHNOLOGIES BECOME INTEGRATED

As quickly as past technologies have become the norm, a new wave will combine digital technologies and the power of data to set new standards. In fact, many of the new technologies that are currently threatening the banking industry will be turned into significant opportunities.

Organizations big and small will therefore boost their efforts to leverage:

- **Blockchain technology:** While blockchain technology has not yet brought an end to the lack of transparency in the industry, we will begin to see the first tokenized commercial financial projects. Mastercard, for instance, already has several patents for the fractional reserve management of blockchain

assets, which is designed to build trust, loyalty and increase security for its customers.

- **IoT (Internet of Things):** PwC predicts that by 2020, [more than 50 billion devices will be connected](#) to the Internet. It forecasts that the IoT revenue will exceed \$3 trillion in 2020. By integrating IoT into FinTech, banks and other financial institutions can enhance data protection and customer service, while wearables can become a powerful branding tool. Certain wearable devices such as smartwatches will also facilitate digital payments.
- **Voice banking:** Ally Bank, Mercantile Bank of Michigan, and [Capital One](#) already offer voice banking features. While the tasks you can currently perform with voice banking are limited it isn't too far fetched to believe many banking tasks will be done by voice in the near future, such as transferring money and applying for mortgages.
- **RPA software:** Robotic Process Automation (RPA) software will be widely used in 75% of financial services institutions by 2020, automating repetitive human processes by utilizing the exact same application interface a human would, and eliminating built-in human inefficiencies.

However, the deployment of these new technologies will not be without challenges, especially in the context of security and cybercrime - which we will explore in detail below.

Fintech's Increasing Range of Digital Threats

CyberSecurity Attacks



Direct attacks



Phishing attacks against employees



Intentional harm by employees



Accidental data loss

Online Fraud



Lost fintech services and products



Chargeback costs



Defaulting clients



Wasted marketing costs



Regulatory fines

Cyber threats will continue to damage fintechs past 2019, as criminals increase the sophistication, frequency, and strength of their attacks. We therefore expect fintechs to up their investment in security tools significantly, with large institutions acquiring cybersecurity solutions themselves to counter both deterministic and probabilistic hacking methods.

The 2A Deloitte survey [predicts cyber monitoring and operations to account for the largest investments](#), followed by endpoint and network security. Apart from security technology, banks will need to invest in talent to combat the serious security skills shortage that have prevailed up to now, both to prevent cyberattacks, and the ongoing threat of online fraud.

3.1 MORE CYBERSECURITY ATTACK OPTIONS

Data breaches continue to cost organizations trillions of dollars annually, with the latest [estimate for 2019 set at \\$2.1 Trillion](#). Company data is still a goldmine for cybercriminals, and the **explosion of social-media platforms, connected IoT devices, e-commerce, mobile devices and cryptocurrency have all created dynamic new attack surfaces which complicates things for security experts.**

These days, business attack surfaces includes everything an organization owns on the web, whether they know about it or not. This means corporate websites, marketing websites, cloud-services accounts, mobile apps and web servers – and they're all discoverable by hackers on the internet in a number of ways:

- **Direct attacks:** hacking via brute force, server overloads to block systems (DDoS attacks), ransomware, and generally attempting to extract value from security weak spots.
- **Phishing attacks against employees:** through online tools (email, fake mobile apps) or social engineering, hackers can find holes in a company's defense and find their way into the rest of the data.
- **Intentional harm by employees:** stolen, leaked, or sold data can find itself in the hands of hackers thanks to disgruntled employees.
- **Accidental data loss:** displaced or lost devices will make things harder to control in the age of IoT and mass smartphone adoption.

As we continue to see a rise in data breaches, technologies such as biometric technology will no longer merely be an option but rather a necessity. Access management, whitelist and 2FA (2 Factor Authentication) will be increasingly implemented – and defeated by criminals. The never-ending game of cat and mouse will also continue with hackers as they attempt to bypass tried and tested solutions such as antivirus, firewall and encryption.

Finally, new areas of focus will include malicious exploitation of blockchain network's hashing power, and the challenge of managing shared data for customer-centric innovation. Banks and vendors of all kinds will be under increasing pressure to protect customer interest while respecting data protection ethics - stepping up for the new role of facilitating secure exchange of customer data with third party ecosystems.

One interesting point to mention is that, according to our proprietary research, **companies have spent up to 90% of their security budget on protecting the business perimeters (cybersecurity). We expect this percentage to shift in favour of fraud protection**, as reusing customer data lost to fraudsters becomes increasingly damaging for fintechs, both in terms of reputation and actual monetary value.

3.2 ONLINE FRAUD BECOMES COSTLIER

There was a [45% increase in account takeover attacks \(ATO\) between 2017-18](#), a trend that shows no signs of slowing down. Customer data is increasingly valuable for criminals, and just as costly for organizations, particularly in the fintech industry.

But don't just rely on the statistics that claim [\\$57.8 Billion was lost to fraud in 2018](#), because it's only part of the whole picture. In fact, it is estimated that every dollar lost to fraud ends up costing organization up to three dollars in indirect damages. The direct costs include:

- **Lost fintech services and products**
- **Chargeback costs:** depending on the card scheme, acquirer and processor, it can reach \$50 per chargeback for retailers.
- **Defaulting clients:** money that lenders will never see back after it's been borrowed.
- **Wasted marketing costs:** the price associated with attempting to attract new clients, who end up damaging your business rather than growing it.
- **Regulatory fines:** adding insult to injury, many organizations have to pay the price of allowing fraudsters in through government fines – especially in the financial sector.

Indirect losses might not be as easy to measure, but they are just as costly:

- **Hacks and security issues put a strain on your IT team**
- **Support is overwhelmed by customer requests who need to reclaim their accounts**
- **The finance department must fight chargebacks**
- **Loss of reputation and brand trust**

Fraud also impacts reporting accuracy. **The problem of false declines is particularly likely to go unchecked, because it's invisible.** It is an issue of lost potential, rather than negative cash flows.

Another noteworthy example of fraud skewing reporting is returns abuse, or when customers serially overbuy, knowing they will return most of the goods later. In the worst cases, these abusers effectively use retail stores as rentals. Because this isn't hard fraud, most merchants are hesitant to block serial returners. However, the practice may have a real impact on operational costs, skewing sales and inventory reports. Finally, all of the above may lead to a lower employee morale, which may affect the sales teams, executives, IT and even HR department in the long term. Which begs the question:

***„How can fintechs reduce the costs,
headaches and resources lost due to fraud?“***

And more specifically: how can they deploy effective prevention systems when mistakes and errors from other companies increase vulnerability? Stolen identities and compromised data-points result in hard-to-spot activities, so any information leak or data breach from other organizations may still affect your business. Which is why it is so important to keep your eyes on the bigger picture when designing and planning a risk management process.

Fraud Fighting for Fintechs



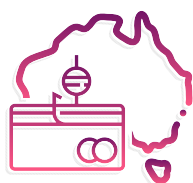
\$ 57,8 B

estimated cost of fraud
to businesses in 2018
([PYMNTS](#))



45 %

increase in fraud attacks
due to account takeovers
between 2017-18 ([Javelin](#))



76 %

increase in credit card fraud
Australia between 2017 and 2018
([Australian Payment Network](#))



\$ 3

estimated total cost of
fraud for every dollar lost
directly ([Lexis Nexis](#))

At SEON, our mission is to reduce the losses due to fraud. What this means, in practice, is that we have to understand how fraudsters think to fight them.

To better illustrate the challenges faced by online businesses - and fintechs in particular - we've therefore gone the extra mile and applied for an online loan with stolen IDs. Because lending is a 100% financial service, there are fewer barriers between fraudsters and their access to money, which makes them a particularly valuable target.

4.1 A TYPICAL FRAUDULENT JOURNEY

Like with many other illegal online activities, it starts with the dark web. This is the collection websites on the internet that are encrypted, non-indexed by search engines, and require specific tools and software to access.

One thing to note is that the dark web is fueled by cryptocurrencies. Being anonymous (or at least very hard to track to a physical address), bitcoins, litecoins and other cryptos are the preferred method of payment for fraudsters and cybercriminals.

- 1. Acquiring stolen data:** the first step was to acquire cryptocurrencies and purchase something called a Fullz - a package consisting of an address, date of birth, and social security number.
- 2. Faking credit scores:** of course, loan companies try to protect themselves from scams by deploying credit scoring systems. Unfortunately, fraudsters have a way around it. We simply purchased background and credit information with pre-existing high credit scores. Fraudsters often pay with a stolen credit card to avoid unnecessary expenses.
- 3. Bypassing IP checks:** another common way to flag fraudsters is to block suspicious IP addresses. Once again, this is easily fooled simply by purchasing a validated IP address, for instance from a residential UK address.
- 4. The bank drop:** loan companies will pay directly into a bank account. Fraudsters can simply purchase one from an illegal marketplace. It will sometimes provide a credit or debit card along with the required IBAN number.
- 5. Phone verification:** most online companies will implement 2FA authentication these days, which requires a phone number. Fraudsters can easily download apps from the App or Play store to generate numbers on a “burner” phone – one that is designed not to leave a trace.
- 6. The loan application:** at that stage, fraudsters have already found everything they need. But loan companies sometimes require extra document verification proof showing at least basic information. Since it’s unlikely fraudsters already have the exact paperwork they need, they can simply use an online service that photoshops the right paperwork for them.
- 7. Cashing out:** finally, fraudsters will need to wire the loan to the bank drop. Cashing the money out from the bank drop is really easily nowadays. This usually means sending it to a cryptocurrency exchange, where they can buy bitcoins or other currencies, which can be used to continue purchasing goods or more fraud tools.

4.2 THE THREE KEY TOUCHPOINTS

The example above should make it abundantly clear that losing customer data leads to more fraudulent attacks. Essentially, there are three points where screening information will go a long way in crippling fraudsters:

4.2.1 NEW REGISTRATIONS

The first step for most online businesses is to sign up new users. Flagging fraudulent users at this stage is the cheapest and safest solution. In our example above, fraudsters used a Fullz and bought IP address to create a new defaulting account whose details will look plausible to a loan company.

There are other reasons to create multiple accounts. It can be to abuse welcome bonuses, coupons or discounts from banks. To launder money through new accounts, apply for credit cards, or even resell the access on a marketplace. Payment providers are hit by fraudsters who create fraudulent merchant accounts, finance illicit activities and launder money, which can cost a lot in regulatory fines.

→ **Challenges of fraud prevention:** creating identity checks that create friction can turn users away. False positives end up losing organizations a lot of potential business.

4.2.2 LOGIN AUTHENTICATION

After registration, users need to login. They must do so from a variety of devices, browsers, locations and IP addresses. **A fraudster who can access the login information will have no problem taking over the account (ATO) and emptying a digital wallet, changing the password to lock the legitimate user out, or purchase items without the user's consent.**

Unfortunately, users are often careless with their login information, as 83% of them reuse the same password for multiple sites. Moreover, some information, which can be acquired from data breaches, cannot change depending on the platform. For instance, Tax, card or social security info are risky ID numbers to use at login because they are static, and fraudsters who acquire it on one platform can reuse it on others.

→ **Challenges of fraud prevention:** blocking legitimate users from accessing their accounts due to false positives leads to frustrations and loss of brand trust. A platform known for poor ATO prevention will also gain a poor reputation amongst users.

4.2.3 USER ACTION

This can be a number of actions depending on the platform. For loan companies, it can be the loan application or withdrawal. For banks it can be a money transfer or purchase. **It is the last chance you have to stop a fraudster before they damage your organization**, and therefore one where your decision will matter the most.

→ **Challenges of fraud prevention:** because user activity is complex and covers a wide range of options, it is difficult to have one system that tracks and monitors all potential actions.

4.3 DEPLOYING THE RIGHT FRAUD FIGHTING TOOLS

„Fraud prevention is all about discovering who you are dealing with.“

What kind of users should be allowed into your system, and which ones will try to scam you in the long term. This is why at its core, effective fraud prevention should perform three main tasks.

- **Gather the data:** at any of the three touchpoints above (registration, login, user action), your system needs to be able to read the data points.
- **Enrich the data:** a single data point can reveal a lot if it is enriched by cross referencing it. For instance, an email address can be compared to a known list of addresses lost in data breaches. If it is found in an old breach, it could mean higher authenticity, because it was previously used by someone. If an email wasn't found in a breach could spell trouble; it increases the likelihood of being used by fraudsters. Similarly, linking an email address to known social media profiles (Facebook, Twitter, LinkedIn) can reveal a lot about the user's online presence.
- **Sift through the data:** all this information is designed to create rules so you can automate your prevention or manually review ambiguous cases. Ideally, you should be able to let an intelligent system (AI-based) flag clear fraudulent cases and let in clear legitimate users. Only questionable cases should be sent for manual review.

Below are examples of the kinds of features a good fraud prevention solution should enable, and why.

4.3.1 EMAIL PROFILING

An email address is a lot like a digital passport. Since 51% of internet users have kept theirs for more than 10 years, it's easy enough to quickly confirm their identity. But like real passports, it's also easy to fake them. Email profiling therefore enriches the data of a single email address, and lets you know if it is suspicious or not by answering the following questions:

- **Is the email address real?** This is done via SMTP check: a simple, yet technical process that will ping the email server and returns a basic answer: does it exist or not?

Unfortunately, **it's extremely easy to create disposable email addresses hosted on real servers.** A quick Google search will bring up hundreds of temporary or throwaway email address services. You simply log on and use it like a regular email platform, but the address is only valid for a limited period of time. This is why you also need to check the following:

The screenshot displays the SEON platform interface for email profiling. On the left, a sidebar lists several email addresses with their associated scores and timestamps. The main panel is divided into three sections:

- Identity:** Contains fields for User ID (f2654eaba265), Full Name (Jim Sand), Username (jimsand99), Email (jim@hotmail.com), Password hash (8bca315445dbc330b36cdbeef57aca4), Total Amount (1 200 EUR), Total Transaction Count (1), First seen (7 months ago), and Username string analysis.
- Email Information:** Shows the email address (jim@hotmail.com) with a 'Flag as suspicious' button and a 'Search on Google' link. It also displays a Score (1.8) and various checks: Exist (SMTP check) Yes, Disposable No, Free Yes, Domain registered Yes, Domain Created (1996.03.27), Domain Updated (2014.10.16), No. of breaches (116), and First breach (2008.04.04).
- Addresses:** Displays three addresses with corresponding Google Maps images: Registered location (Pannonia u. 32, Budapest, 1136, HU), Billing address (Pannonia u. 32, Budapest, 1136, HU), and Shipping address (Hviezdna 1405/4, Nitra, 949 01, SK).

At the bottom, there is a map showing the location of the shipping address. The right sidebar lists various social media and service accounts (Facebook, Google, Yahoo, Microsoft, LinkedIn, Gravatar, Instagram, eBay, Twitter, Apple, Tumblr, Spotify, Weibo, VKontakte) with their status (Registered).

Screenshot from SEON platform showing email profiling features

- **Is the address disposable?** By ensuring the domain is not one offered by temporary email services, we can lower the users' risk score.
- **Is the domain suspicious?** Is it a free domain? When was it created? Does it require SMS or any other verification to open it? How about recent updates? Just a number of data points that can give great insights into an email address validity.

Now if you think about your own email address, it's probably used to sign into a number of services, especially social media platforms. These are great places to investigate in order to validate the emails address usage.

- **Social Media Profiling:** this process will essentially check if the email address has been used to sign on platforms such as LinkedIn, Instagram, Facebook etc...

Then there are databases, both internal and external, useful for fraud prevention. It's important to check if the email address is associated with:

- **Data breaches:** Are the credentials openly available? Some services track all stolen account info, which makes it easy to see if an email address has potentially been released in the open before.
- **Blacklists:** Is this user a repeat offender? Have they been caught before? By sharing and cross referencing other blacklists, it should be easy to see if the user is legitimate or fraudulent.

Last but not least, some subtle data points that can reveal a lot about an email address. They all have to do with the string of letters, numbers and characters used in the actual email address name.

- **Email string analysis:** Does the name on the email address resemble the user name? Does it use a number of suspicious characters or nonsensical words? Too many vowels vs consonant ratio? In short, this part of the system is trying to answer the question: does this email address look suspicious or not?

4.3.2 DEVICE FINGERPRINTING

The screenshot displays the SEON platform interface, showing a list of users on the left and detailed device fingerprinting parameters for a selected user, 'scottgrant'.

User List (Left Panel):

- scottgrant (2019.01.10, 13:22:13) - 69.77
- jimsand99 (2019.12.17, 16:46:44) - 84.8
- jimsand99 (2019.12.02, 18:18:07) - 84.8
- scottgrant (2019.10.11, 15:08:56) - 10
- scottgrant (2019.10.11, 15:07:31) - 10
- scottgrant (2019.10.11, 15:08:56) - 10
- scottgrant (2019.10.11, 15:04:40) - 10
- scottgrant (2019.10.11, 15:00:30) - 10
- jimsand99 (2019.09.26, 14:42:41) - 84.8
- jimsand99 (2019.09.26, 14:32:42) - 84.8

Device & OS Details (Main Panel):

- Devices & OS:** User desktop 1
- Device type:** desktop
- Operating system:** MacOS, Version 10.13.2
- User agent:** Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.167 Safari/537.36
- Device ID:** 984872732
- Cookie hash:** 61d786b165b74e15d8c55b1e96a8cdb3
- Browser hash:** c97a9e3e27dc8be9286f9c9ad575
- Flagged as suspicious:** By a not specified industry, 2019.05.03, 10:31:56
- Device hash:** c71d685a5df1a1c45f249b3bf3c39d0c
- Timezone offset:** UTC+01:00
- Cookie enabled:** Yes
- Private mode:** No
- DNS IP:** 89.134.46.85
- DNS IP country:** HU
- DNS ISP name:** UPC Magyarország Kft.
- Window size:** 1571x921

Detected Online profiles:

- YouTube, Facebook, Gmail, Flickr, Airbnb, GitHub

Font and Plugin Information:

- Font count: 28
- Font hash: -551360058
- Plugin count: 4
- Plugin list: Chrome PDF Plugin, Chrome PDF Viewer, Native Client, Widevine Content Decryption Module
- Plugin hash: -1978200868
- WebRTC activated: Yes
- WebRTC count: 1
- WebRTC IP list: 192.168.1.136
- Flash enabled: No
- Java enabled: No

Device Information:

- Device IP address: 80.99.56.91
- Device IP country: HU
- Device IP ISP: UPC Magyarország Kft.

Order details (Right Panel):

- ISP: Fiber Grid Inc
- Open Ports: 80
- Tor: No
- Web Proxy: No
- HTTP Proxy: No
- SPAM blacklists: 0
- Data center: Yes
- Transaction type: purchase
- User order memo: OrderMemo
- Discount code: 54321
- Gift: false
- Gift message: false
- Details url: https://www.apple.com
- Merchant ID: shop123
- Merchant created at: 2015.11.01. (1446370717)
- Merchant country: US
- Payment mode: card

Addresses (Right Panel):

- Registered location:** 366 Broadway, New York, 10013, US
- Billing address:** 366 Broadway, New York, 10013, US
- Shipping address:** Via delle Fosse di Castello, 3, Roma, 00193, IT

Map (Right Panel):

- Map showing locations in New York and Rome, Italy.
- Distance: 6395 km

Notes (Right Panel):

- Type your notes here...

Screenshot from SEON platform showing device fingerprinting parameters

When users access your platform, they do it with two tools: a device with a web browser or mobile application, and an Internet connection which retrieves an IP address. This creates two data sources. They are present at signup, login, checkout, or even when browsing a page. With the right solutions, we can extract useful information from these data points.

Combining information about a browser and device is what we call fingerprinting.

It gives a clear picture of how the user is connecting to your service. It lets us understand user behavior, and more importantly, flag potential fraudsters.

At SEON, our device fingerprinting tool checks and reveals more than 500 parameters, including:

- **Screen information**
- **Device build**
- **Operating system version**
- **Installed plugins**
- **Browser time zone**
- **Device number**
- **Battery information**
- **And much, much more....**

One of the most important features of our device fingerprinting tool, however, is the generation of specific hashes. You can think of them as unique IDs, created based on specific parameters:

- **Cookie Hash:** Creates an ID for each browser session. Clearing the browser cookies and cache will generate a new hash. But if multiple users share the same hash, it means they are clearly using the same browser and device.
- **Browser Hash:** Generates an ID by combining data from the browser, operating system, device and network. This hash remains unchanged, even if the user clears their browser cookies and cache, or browses privately. However, a device with multiple browsers installed, or even browser versions, will generate different hashes.
- **Device Hash:** Offers an ID based on the device hardware (e.g HTML5 canvas, audio fingerprinting, GPU, screen data and so on). While many users can share the same device hash (for instance two iPhone 7 Safari users), this allows us to detect Remote Desktop Connections, virtual machines or emulators. For instance, fraudster favorites such as AntiDetect, FraudFox, or Multilogin all generate the same device hash. Moreover, fraudsters using browser extensions that spoof HTML5 canvas will have very unique IDs – and should therefore be flagged as high risk.

As you can see, they each have their pros and cons. Still, **all these hashes becomes a near flawless screening tool when they are leveraged together.** Fraud analysts can easily create customer profiles that are precise, reliable, or even implement

rules that isolate suspicious hashes automatically.

The screenshot displays the SEON data enrichment interface. On the left, a sidebar lists several user entries with names like 'scottgrant' and 'jimsand99', each accompanied by a score and a red flag icon. The main panel shows the details for the user 'scottgrant' (User ID: 9384298). The interface is divided into several sections:

- Identity:** Includes fields for User ID, Full Name (Scott Grant), Username (scottgrant), Email (scott@gmail.com), Password hash, Registration Date, Affiliate name, Affiliate ID, Total Amount, Total Transaction Count, First seen, and Username string analysis.
- Customer status:** Shows 'BLACKLISTED' with an 'Email 1' button and 'WHITELISTED' with a note 'No data has been whitelisted'.
- IP Information:** Displays IP Address (165.231.234.219) with a 'Flag as suspicious' button, Proxy Score, Location (Helsinki (Uusimaa)), Country (Finland), IP type (DCH), ISP (Fiber Grid Inc), Open Ports, Tor, Web Proxy, HTTP Proxy, SPAM blacklists, and Data center.
- Phone number:** Shows Phone number (+3655549262), Valid, Possible, Country (HU), Type (FIXED_LINE), Billing Phone, and Shipping phone.
- Credit Card:** Displays Credit Card (5218 90... 4180), Card hash, AVS result, CVV result, Bank (BELFIUS BANK N.V. / BELFIUS BANQUE S.A.), Brand (MASTERCARD), Type (CREDIT), Level (PLATINUM), Country (BELGIUM (BE)), and Valid status.
- Email Information:** Shows Email (scott@gmail.com) with a 'Flagged as suspicious' button, a note 'By a not specified industry', a date '2019.06.18. 13:13:05', a 'Confirm as suspicious' button, and a 'Search on Google' button.
- Devices & OS:** Shows 'User desktop 1' as the device type and 'MacOS' as the operating system.
- Social Media:** Lists various social media accounts (Facebook, Yahoo, Microsoft, LinkedIn, Gravatar, Instagram, eBay, Google, Twitter, Apple, Tumblr, Spotify, Weibo, VKontakte) and their registration status.

Screenshot of SEON data enrichment feature

4.3.3 OTHER DATA ENRICHMENT FOR ID PROFILING

„At its core, data enrichment is refining and enhancing information.“

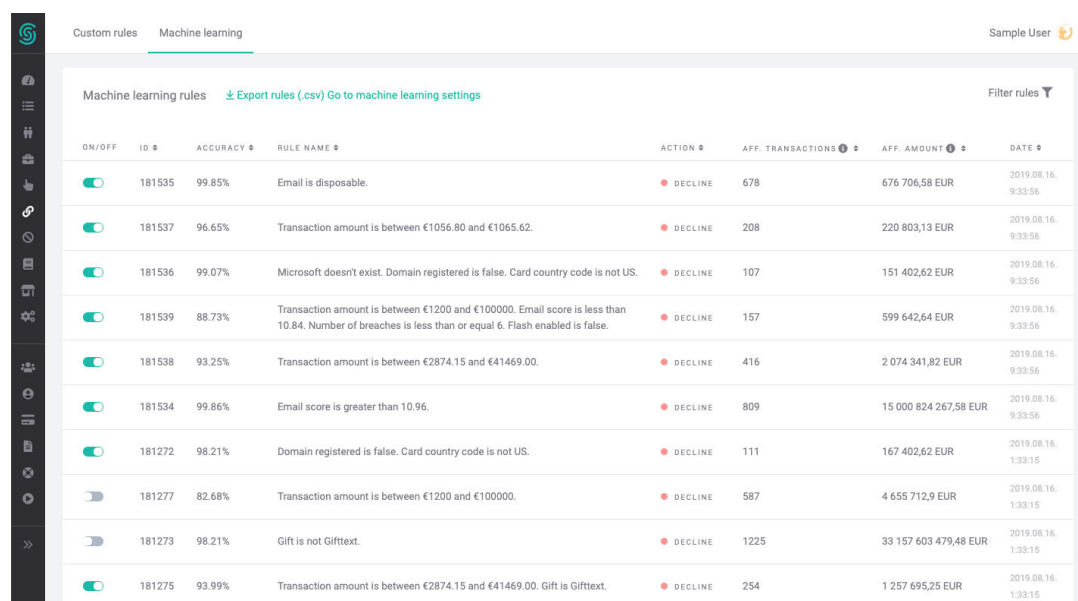
Organizations acquire raw data, but that data isn't always useful. It can contain mistakes. It can be too isolated to be useful (data silos). It can be too vague to be meaningful. But enriching seemingly unrelated data points can create a full digital profile, which can even be leveraged for improved credit scoring and KYC processes.

Similar your users' email addresses and devices, the IP address can reveal a lot about who they truly are.

- Where is the user based?
- Are they connecting through open ports – communicating with other servers?
- Are they using proxies, VPNs or TOR?
- Is the IP on any spam blacklists?
- Datacenter IP or residential connection (belonging to a homeowner)?

BIN (Bank Identification Numbers), also known as IIN (Issuer Identification Numbers) can tell us a lot about a card, and therefore its owner:

- What bank issued the card?
- What kind of card is it?
- What is the bank's phone number?
- What is the card' level (ATM only, Gold, Platinum, World Elite or Infinite depending on the provider)



The screenshot displays the 'Machine learning' tab in the SEON interface. It shows a table of machine learning rules used for fraud detection. Each rule includes a toggle for 'ON/OFF', an ID, an accuracy percentage, a detailed rule name, an action (DECLINE), the number of affected transactions, the affected amount in EUR, and the date. A sidebar on the left contains various navigation icons, and a 'Sample User' button is in the top right.

ON/OFF	ID	ACCURACY	RULE NAME	ACTION	AFF. TRANSACTIONS	AFF. AMOUNT	DATE
ON	181535	99.85%	Email is disposable.	DECLINE	678	676 706,58 EUR	2019.08.16, 9:33:56
ON	181537	96.65%	Transaction amount is between €1056.80 and €1065.62.	DECLINE	208	220 803,13 EUR	2019.08.16, 9:33:56
ON	181536	99.07%	Microsoft doesn't exist. Domain registered is false. Card country code is not US.	DECLINE	107	151 402,62 EUR	2019.08.16, 9:33:56
ON	181539	88.73%	Transaction amount is between €1200 and €100000. Email score is less than 10.84. Number of breaches is less than or equal 6. Flash enabled is false.	DECLINE	157	599 642,64 EUR	2019.08.16, 9:33:56
ON	181538	93.25%	Transaction amount is between €2874.15 and €41469.00.	DECLINE	416	2 074 341,82 EUR	2019.08.16, 9:33:56
ON	181534	99.86%	Email score is greater than 10.96.	DECLINE	809	15 000 824 267,58 EUR	2019.08.16, 9:33:56
ON	181272	98.21%	Domain registered is false. Card country code is not US.	DECLINE	111	167 402,62 EUR	2019.08.16, 1:33:15
OFF	181277	82.68%	Transaction amount is between €1200 and €100000.	DECLINE	587	4 655 712,9 EUR	2019.08.16, 1:33:15
OFF	181273	98.21%	Gift is not Gifttext.	DECLINE	1225	33 157 603 479,48 EUR	2019.08.16, 1:33:15
ON	181275	93.99%	Transaction amount is between €2874.15 and €41469.00. Gift is Gifttext.	DECLINE	254	1 257 695,25 EUR	2019.08.16, 1:33:15

Screenshot of SEON Decision Tree

4.3.4 MACHINE LEARNING: CONNECTING THE DATA DOTS

Finally, **all the data enrichment solutions above are only as powerful as the person who analyzes it.** And if you and your team need to manually check everything, you still end up doing a lot of hard work.

Which is why a good fraud prevention solution should also generate insightful scores designed to let you mitigate fraud risk yourself. At SEON, we believe machine-learning engine is the right solution, as long as it offers the following features:

- **Powerful algorithms:** machine learning is designed to improve with the data you feed it.
- **Confusion matrix analysis,** the system should work with any data, from currency to age groups. For instance, a ML system can take into account browser resolutions to flag suspicious values (as affiliate link fraudsters load content from sites with invisible iframes). It would have been a stroke of genius for a fraud manager, but is extremely easy for a machine.
- **Whitebox solution:** The machine learning model that delivers readable rules through a Decision Tree algorithm. Each applied rule creates a new branch where the nodes are clear parameters. However, we do not believe statistical analysis should be fully automated. Fraud managers still need to reign in machine learning, even if it is to improve the algorithms by training it.

This is why we also believe fraud prevention systems should include:

- **Custom rules:** this isn't something machine learning can do, but the right system should absolutely let them tailor rules to their own needs.
- **Whitelisting / Blacklisting:** similar to the above point, not something a machine learning system can implement for them.

Customer status

BLACKLIST NORMAL WHITELIST

User ID: 9384298
Count affected transactions: 10

IP (for 6 months): 51.179.96.103
Count affected transactions: 10

165.231.234.219
Count affected transactions: 10

1.33.70.177
Count affected transactions: 10

80.99.56.91
Count affected transactions: 10

Email: scott@gmail.com
Count affected transactions: 10

User address: us_newyork_10013_366broadway...
Count affected transactions: 10

us_newyork_10013_355broadway...
Count affected transactions: 10

Shipping address: it_roma_00193_viadellefossecastello3...
Count affected transactions: 10

Billing address: us_newyork_10013_366broadway...
Count affected transactions: 10

add comment and expiration

Cancel Submit

Screenshot of SEON Blacklist feature

Add new Blacklist Whitelist Flagged as suspicious

Manual input

INPUT FIELD: User ID STATE: blacklist VALUE: COMMENT: EXPIRATION: never

Load

Data preview

STATE	VALUE	DATA FIELD	COMMENT	EXPIRATION
blacklist	sample_123	user_id		never
blacklist	sample_456	user_id		30 days

Add to list

Screenshot of SEON Blacklist feature 2

- **Flagging suspicious users who have not yet committed any fraud:** based on their experience, the best fraud managers should be able to anticipate potential attacks from otherwise unsuspecting users.
- **Complete system control:** one of the most important points for fraud managers is the ability to leverage automation without rescinding control over the system. A good hybrid solution should allow one without sacrificing the other. This is particularly true in the context of fintechs, where user friction needs to be reduced to a minimum. So your machine learning system should only trigger stronger authentication methods such as 2FA or SMS verification when the risk is high.

Key Takeaways

While the fintech ecosystem is booming, it is also under constant pressure to adapt and evolve. A growing competitive landscape along with increasing regulations and attack vectors are set to make things more complicated for startups providing financial services.

In short, CEOs, CFOs and even investors need to ensure their fintech isn't just innovative, but also future proof. And our research shows that implementing a strong fraud prevention solution in place early can have numerous advantages and benefits for fintechs:

- Reducing lost costs due to fraud
- Increasing profits and therefore competitiveness
- Delivering better KYC processes
- Ensuring compliance in the face of growing regulation

To see how SEON can help your company prepare for the future,
please visit www.seon.io

or

schedule a personalised product showcase call



SEON Technologies Ltd.
seon.io

info@seon.io
0044-20-351-44790