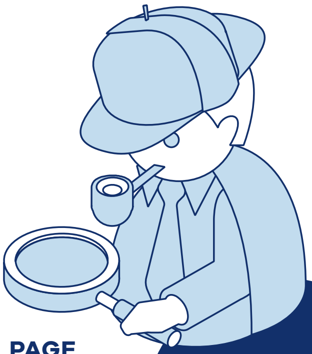
RISK IDENT

eSIM TECHNOLOGY POISED TO CHANGE FRAUD PREVENTION METHODS

CONTENTS



You can click on a number to go directly to the corresponding page!

1 THE RISE OF eSIMS

The year 2021 marks the 30th anniversary of the birth of SIM cards, and it may well mark their upcoming death, as well.

Having been invented in 1991, conventional SIM cards have enabled network connectivity to billions of mobile devices around the world. Over the course of the last three decades, they've decreased in size to allow for increased internal device space – which is necessary for the ever-smaller, more powerful, feature-packed smartphones, smartwatches and other mobile devices currently on the market.

However, consumers' appetite for fast and intelligent connected devices is insatiable, and as they continue to expect even faster, smarter, smaller and more frictionless devices and connectivity, traditional SIM cards are quickly becoming impractical and unscalable. An embedded SIM, or eSIM, has been introduced as the solution to speed, size and connectivity constraints.

1.1 Goodbye SIM Cards, Hello eSIMs...

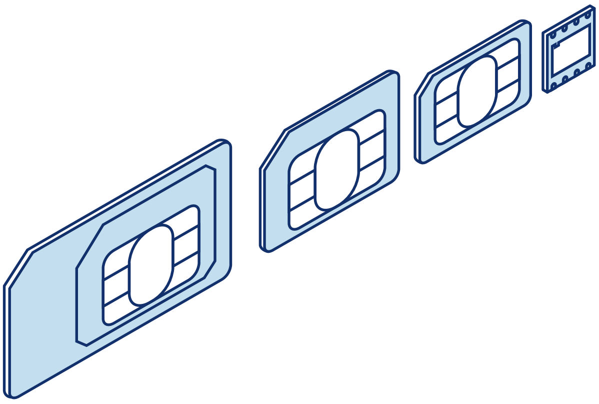
eSIMs are on track to have almost 90 % market penetration by 2025, with 80 % of manufacturers and 90 % of mobile network operators (MNOs) reporting that they will offer eSIM technology by that time.[1] Most new phones, tablets and wearables already offer eSIM and/or dual SIM capability, and many of the major telecommunications carriers already support eSIM activation, including Vodafone, AT&T, Verizon, T-Mobile, EE, O2, Three and Deutsche Telekom. Experts predict that within the next three years, 7 billion eSIMs will have been activated in consumer and IoT devices around the world[2], leading the eSIM market to reach an expected $6.53 billion by 2028.[3]

1.2 ...But Also, Hello Fraud?

Whenever new technology is introduced to the market, fraudsters immediately look for security gaps that they can use to their advantage. Because of this, fraud teams have learned that it is incredibly important to monitor any signs of possible fraud in the earliest days of new tech trends, particularly those that are poised for quick market saturation. The faster new types of fraud are detected, the faster the security gaps can be filled – which can ultimately save millions if not billions of dollars lost to fraud.

As such, in the early days of eSIM technology, experts at **RISK IDENT** – a leading fraud prevention company that works closely with Europe's largest MNOs – examined possible risk management issues connected to the proliferation of eSIMs.

One finding has been that due to the strictly digital onboarding process and the digital transmission of eSIM activation data, postal and delivery addresses are becoming obsolete as a data point for fraud prevention, while email verification and strong KYC (Know Your Customer) methods are becoming increasingly important. This valuable information translates to all industries that sell digital products and/or use digital identity verification, and this paper will illuminate these important fraud management findings through the story of eSIMs.



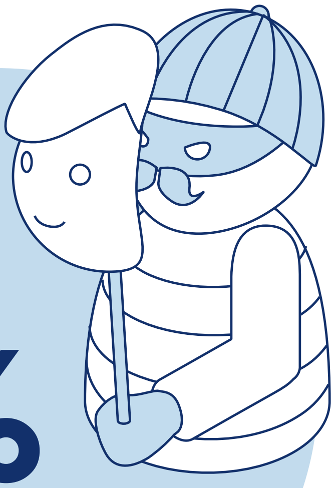
2 WHAT IS ESIM ACTIVATION FRAUD AND HOW DOES IT WORK?

The advent of mobile technology has allowed more and more people to stay connected at all hours of the day from virtually any place on Earth. However, mobile technology has also made it easier for criminals to connect with one another and carry out their crimes. Using devices with prepaid SIM cards has allowed criminals to stay anonymous and avoid detection while they carry out illegal activity such as financial fraud, terrorism, money laundering, and drug and human trafficking.

As a way to combat this, governments around the world have implemented mandatory SIM card registration policies, which require users to provide personal information and proof of identity documents in order to activate a prepaid SIM card and – more recently – eSIMs. As of January 2020, the governments of 155 countries mandate SIM and eSIM registration policies.[4]

While mandatory SIM card and eSIM registration is indeed helpful in ascertaining the true identity of SIM card holders and making sure users aren't on blacklists, the implementation of such policies has had an unintended consequence: criminals are relying more heavily on obtaining fake or stolen identities to register SIM cards.[5] In fact, in the years following mandatory SIM card registration, the identity fraud rate in the telecom industry increased by more than 50 %.[6] These cases contribute to the overall fraud picture around the globe, which as a whole has experienced a rise in identity fraud. For example, in 2020, 61 % of fraud cases in the U.K. were identity fraud cases.[7]

Fraudsters are increasingly becoming more sophisticated at stealing, forging and altering identity documents in order to evade detection. This has presented challenges in document verification and fraud prevention, particularly as identity authentication – and now delivery of SIM activation data – has shifted from being done in-person to being done completely online.



61 %

of fraud cases in the U.K. were identity fraud cases (2020).[7]

3 THE HIGH COST OF TELECOM FRAUD

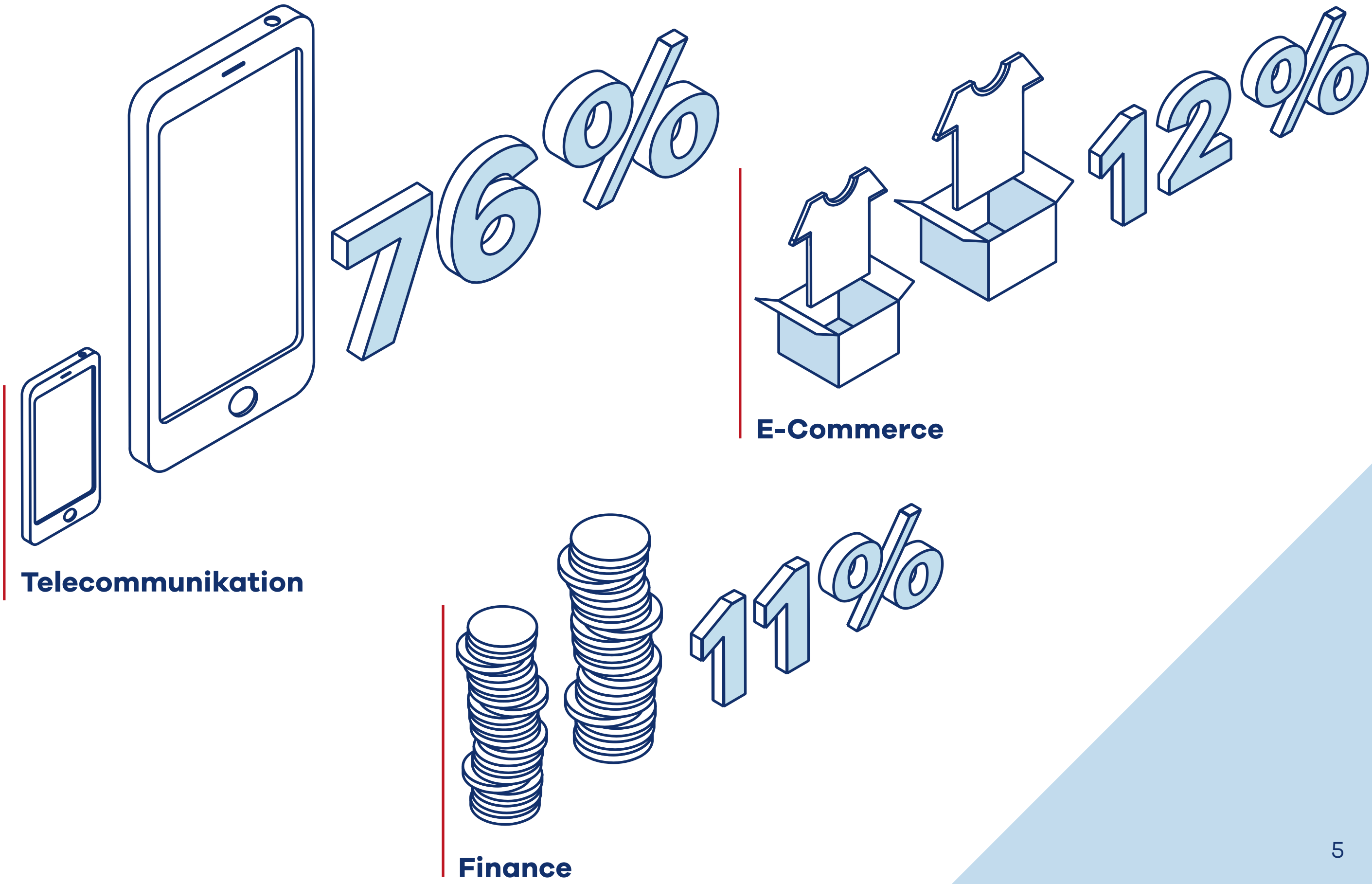
The telecommunications industry experienced an estimated $28.3 billion in fraud losses in 2019, with a significant portion of that being attributed to subscription fraud and payment fraud.[8] The losses for 2020 and 2021 are likely to be higher, as the telecommunications industry experienced a 76 % increase in suspected fraud during the first half of 2020, when the COVID-19 pandemic began.[9] (This is compared to a 12 % increase of suspected fraud in e-commerce and an 11 % increase of suspected fraud in the financial services industry during that same period.)[10]

Subscription fraud, which includes identity theft and account takeover (ATO), is one of the most problematic telecom fraud trends, representing up to 10 % of mobile network operators' gross revenues.[11] Fraudsters engage in this type of fraud in order to use data, mobile banking, virtual wallets and other high-value telecom services anonymously – at the cost of the duped telecom provider and original ID holder.

But it's not just the direct costs of fraud that are proving to be expensive for MNOs. Other steep financial costs that can be incurred due to fraudulent activity include:

- brand damage
- staff time
- compensation and incentive payments
- financial liability issues with banks
- updating security systems, fraud prevention software and other back-end systems
- ad campaigns to restore trust with consumers and investors

Suspected fraud during the first half of 2020, when the COVID-19 pandemic began – per Industry.[9]

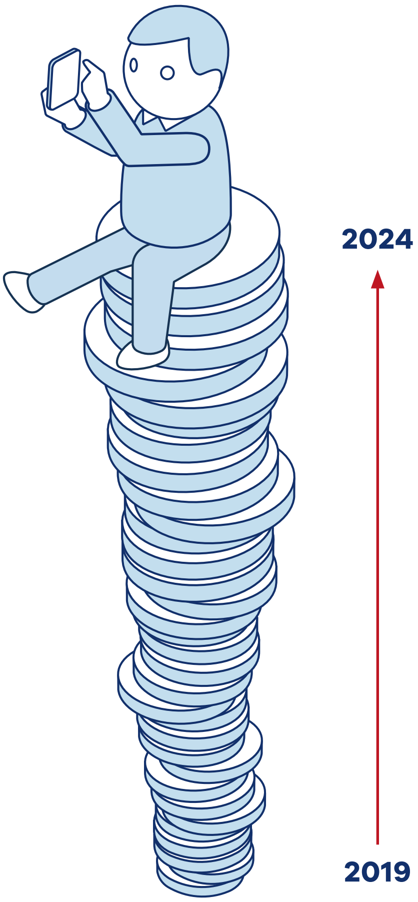


3.1 A Hidden Cost: MNOs Have Become The New ID Brokers

The telecommunications industry is increasingly being used by fraudsters to carry out criminal activity, but most mobile network operators continue to battle against fraud without much help from law enforcement. The leading reason telecommunications companies do not report fraud is “lack of perceived interest or understanding by law enforcement,” while 10 % of MNOs say they do not report fraud due to lack of success in previous cases.[12] Unfortunately, this leaves telecom companies singlehandedly battling fraud and identity theft related to telecommunications fraud.

Meanwhile, other industries that experience high levels of fraud – including banking and e-commerce – are increasingly turning to MNOs as their first defence against fraud, as well. Many banks and service providers rely on a customers’ mobile phone as a method of verification, and the argument is that MNOs have access to a vast amount of data on their customers, including real-time device data and network information. Using this knowledge – which includes device location data, roaming status, SIM lifecycle and billing status – has been shown to increase fraud detection by 45 % over other systems.[13]

The good news is that mobile digital identity, which ensures identity verification through SIMs and eSIMs, is expected to generate over $7 billion for MNOs in 2024. This is up from an expected $859 million in 2019 – a growth of over 800 %.[14] But the bad news is that the pressure will continue to mount for MNOs, who are increasingly responsible for ID verification that blocks fraudsters from signing up for new accounts using stolen identities, stops fraudulent payments and default payments, and detects cybercriminals who are taking over user accounts – both in the telecommunication industry as well as in banking and e-commerce.



800 %

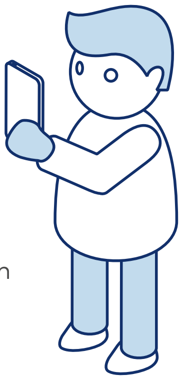
Estimated increase in revenue of identity verification through SIMs by 2024 (from 2019 levels)

4 HOW MNOS CAN PROTECT AGAINST ESIM ACTIVATION FRAUD

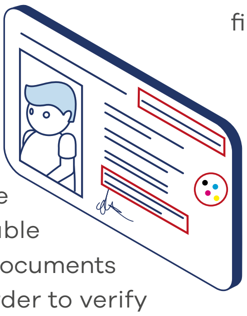
Because SIM and eSIM fraud are closely connected to terrorism, money laundering, and other criminal activitites that have high financial and societal costs, telecommunications companies already rely heavily on KYC (Know Your Customer) solutions to ascertain the identity of subscribers. But the proliferation of digital transactions, digital customer service and digital SIM and eSIM activation has spurred an increase of eKYC solutions, such as biometric authentication companies that provide digital onboarding and identity verification.

4.1 Biometric Authentication Solutions Help — But Have Limits

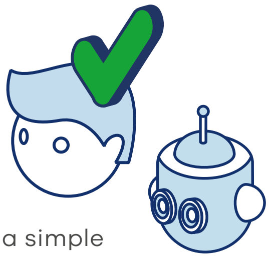
Biometric identity authentication solutions examine things like fingerprints and facial features to ascertain the identity of customers. Some of the features that biometric solutions provide include:



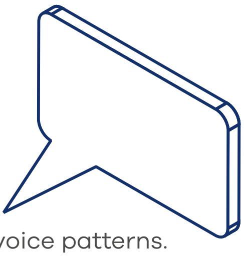
Facial Recognition: Users take a photo of their identity document and take a selfie within the program so the two images can be compared. This only works if the identity document presented hasn't been forged or altered, as the fraudster could place his or her image on the document so it matches the selfie.



ID Recognition: This technology extracts the Visual Inspection Zone (VIZ) data and the Machine-Readable Zone (MRZ) data from the identity documents that are uploaded by the user in order to verify and authenticate the information. It also works to detect forgeries and alterations by checking the color profile of the document, validating the expiration date of the ID and recognizing the over-stickered letters and pictures on the document.



Active Liveness Checks: This technology asks the user to do a simple task, such as follow a moving dot on their mobile phone screen, to ensure that there is a real live person on the other end of the digital onboarding process rather than just an image.



Voice Recognition: Voice biometrics technology helps validate identity by detecting over 100 physical and behavioural factors in an individual's voice patterns. These include things like accent, pronunciation, emphasis, and speed of speech. The human voice has several identifiers that make it just as unique as a fingerprint.[15]

Biometric solutions show such promise that experts predict that within the next five years, the total biometrics market size will surpass $50 billion – a significant leap from the $7 billion spent globally in 2014.[16] And, as of 2020, 8 % of countries globally require Mobile Network Operators (MNOs) to capture a photograph, fingerprints, and other biometric attributes of users in order to complete SIM and eSIM registration.[17]

Though biometric identity solutions are becoming more popular as a tool against fraud, this type of fraud prevention is facing serious problems around the globe. The use of biometrics has sparked privacy concerns in countries that regulate data protection, and the technology has yet to inspire consumer confidence. A 2021 report by a leading biometric identity company found that although 81 % of consumers recognize that biometrics are the next wave of protection in payments and financial services, 52 % understand that a fake ID could be used to set up accounts in their name, and 46 % are concerned that fake IDs will be used to steal their money or that of someone they know.[18]

Part of what is fueling the distrust of biometric solutions is the fast-rising phenomenon of deepfakes, in which videos, images (such as government ID) and audio recordings are manipulated or distorted to incorrectly represent an individual. Although deepfakes have primarily been used for social sharing and entertainment, they are increasingly being employed for fraudulent purposes and impersonation relating to digital identity.[19]

What's more, biometric identity authentication solutions are relatively new in comparison to traditional fraud prevention tactics, which means that their databases aren't as robust. Though these types of fraud solutions will be more and more common in the future, many current biometric solutions still face the challenge of scaling their databases in order to make them more efficient (an example of this is that some facial recognition services deliver below 20 % success rates).[20] Therefore, the use of traditional fraud prevention solutions continues to be and will remain a very valuable tool in the fight against eSIM fraud.

4.2 Drawbacks of Biometric Solutions

Email addresses are increasingly becoming more than just simply tools to send and receive digital messages. With email addresses being mandatory for registering and logging in to every online account – from bank accounts to social media accounts – they're almost like an online passport. This has made them just as important for identity authentication and verification as other data points like ID checks, credit info and biometrics.

However, fraudsters know how to game the system when it comes to creating email addresses. For example, they can easily create a free email account with a name that matches a stolen credit card, which helps them avoid suspicion. They can also create unlimited free email addresses, or – for very little cost – they can purchase real, mature email addresses from the dark web.

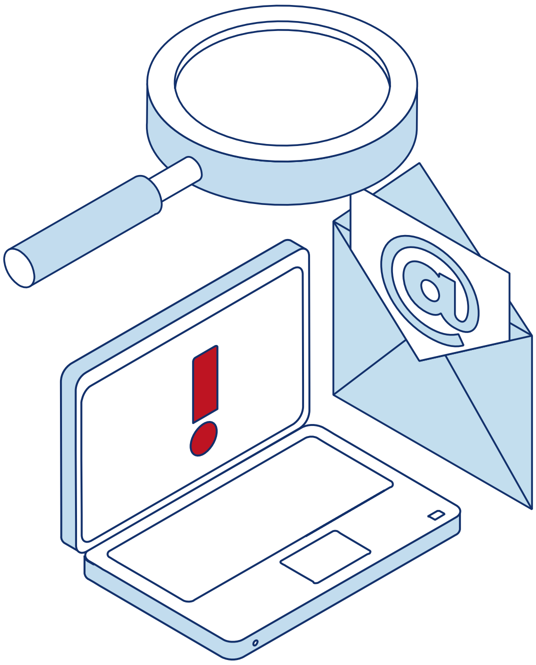
Fortunately, email risk assessment tools can help discern whether or not a given email address is legitimate and if it belongs to the person presenting it. Some of the data points that email verification tools can examine include:

When was the email address created?
Brand new email addresses tend to be riskier, while addresses that have been in operation for quite some time are more likely to indicate a legitimate customer.

Is the email address valid or deliverable?
Email assessment tools can perform SMTP checks to ping the domain server and ascertain if the given address is real.

Does the address use a free domain provider?
An email address that was created for free isn't suspicious in and of itself (widely used programs such as Gmail are free), but knowing more information about the free provider can be helpful in fraud decisions. For example, Gmail has implemented a phone verification step when a user sets up an email account, whereas many other domain providers do not require extra security steps.

Was the email involved in a data breach?
Contrary to what many might believe, an email address that has been involved in a data breach can actually indicate less risk. This is because if an email address has previously been leaked, it's more likely to be a mature one.



Is the email attached to any social media sites?
With social media being so ubiquitous, it's common for an email address to be associated with sites like Twitter, Instagram, and TikTok. If the email being examined has no connection to social media sites, it's more likely to be higher risk.

Is the address disposable?
If an email address was created with a service that offers disposable addresses, there's a pretty high chance that it is associated with fraud.

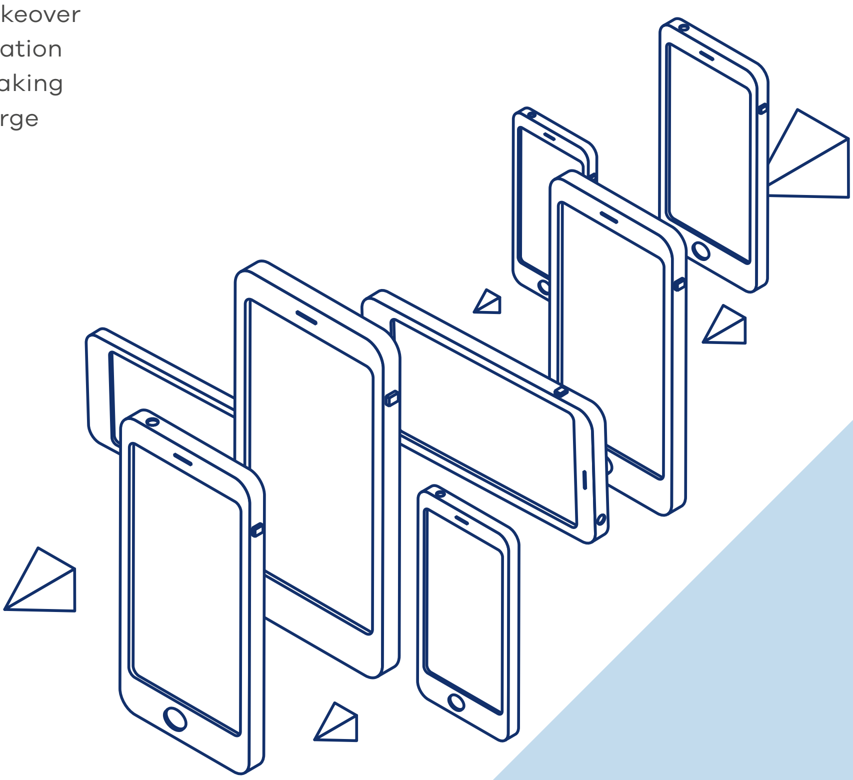
4.3 Traditional Fraud Teams Must Examine New Data Points To Catch eSIM Activation Fraud

When it comes to fraud prevention, the more data points you can examine, the more confident you can be about the trustworthiness of a transaction. In other words, examining every single customer data point at your discretion – from device fingerprints to identity verification – can help you make a more informed fraud management decision. However, the rise of eSIMs and the digital onboarding that comes along with eSIMs is changing the data points that traditional fraud management teams examine when searching for fraud.

One of the traditional data points that anti-fraud systems examine when it comes to the purchase of physical goods is the customer's delivery address. In the case of regular SIM cards, which are delivered through the mail, fraud software can examine different attributes of the given address to ascertain the trustworthiness of a transaction. For example, is the address on a regular street in a neighborhood (less risky) or is it the address a large warehouse near a shipping dock (more risky)? Also, has the address been associated with previous fraudulent orders?

Another example of using an address as a data point to determine fraud risk is in a B2B account takeover (ATO) scheme currently facing telecommunication companies. This crime works by a fraudster taking over an email account of an employee at a large company and contacting a salesperson within the company to make a large, fraudulent telecom order. For example, the fraudster, posing as the legitimate employee, could order 300 mobile phones and 100 laptops, using fake documents, IDs, and other means for procuration of the order. He or she then puts pressure on the real employee, saying that the order is urgent and needed for an important project. Because the order comes from an email address of a real person within the company, it's not obvious that the request is fraudulent. But one way to ascertain the legitimacy of the order is by examining the delivery address: a real order will be delivered to a company address or a company subsidiary address, while a fraudulent order will most likely be delivered elsewhere.

When it comes to eSIMs, the onboarding process is done digitally, without a physical delivery address being involved. This means that fraud prevention teams must analyse other data points in order to verify the identity and trustworthiness of a customer.



4.4 Rising Importance of Email Risk Assessment

Email addresses are increasingly becoming more than just simply tools to send and receive digital messages. With email addresses being mandatory for registering and logging in to every online account – from bank accounts to social media accounts – they're almost like an online passport. This has made them just as important for identity authentication and verification as other data points like ID checks, credit info and biometrics.

However, fraudsters know how to game the system when it comes to creating email addresses. For example, they can easily create a free email account with a name that matches a stolen credit card, which helps them avoid suspicion. They can also create unlimited free email addresses, or – for very little cost – they can purchase real, mature email addresses from the dark web.

Fortunately, email risk assessment tools can help discern whether or not a given email address is legitimate and if it belongs to the person presenting it. Some of the data points that email verification tools can examine include:

When was the email address created?
Brand new email addresses tend to be riskier, while addresses that have been in operation for quite some time are more likely to indicate a legitimate customer.

Is the email address valid or deliverable?
Email assessment tools can perform SMTP checks to ping the domain server and ascertain if the given address is real.

Does the address use a free domain provider?
An email address that was created for free isn't suspicious in and of itself (widely used programs such as Gmail are free), but knowing more information about the free provider can be helpful in fraud decisions. For example, Gmail has implemented a phone verification step when a user sets up an email account, whereas many other domain providers do not require extra security steps.

Was the email involved in a data breach?
Contrary to what many might believe, an email address that has been involved in a data breach can actually indicate less risk. This is because if an email address has previously been leaked, it's more likely to be a mature one.

Is the email attached to any social media sites?
With social media being so ubiquitous, it's common for an email address to be associated with sites like Twitter, Instagram, and TikTok. If the email being examined has no connection to social media sites, it's more likely to be higher risk.

Is the address disposable?
If an email address was created with a service that offers disposable addresses, there's a pretty high chance that it is associated with fraud.

4.5 Device Fingerprinting Remains Valuable

While email verification is becoming more and more important in the fight against fraud — and is particularly helpful in combating eSIM fraud and digital goods fraud — the use of device fingerprint technology remains a valuable tool for telecom fraud teams that are facing eSIM fraud.

Device fingerprinting is able to collect dozens of recognition features from the devices that carry out transactions on websites and ascertain whether or not the device is trustworthy, or if it has been connected to past fraud attempts. For example, when a customer initiates a transaction, device fingerprinting software can examine things such as:

- Which operating system the customer is using
- The type and version of web browser being used
- The web browser's language setting

These features help identify a unique device, much like a fingerprint left at a crime scene can identify the perpetrator.

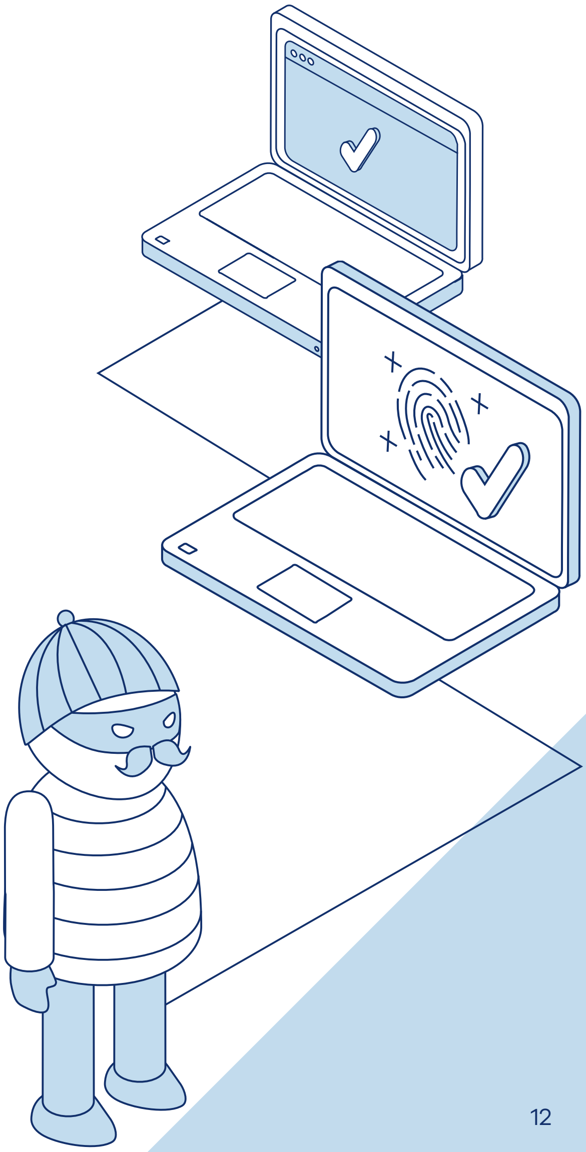
However, the problem with device fingerprinting when it comes to detecting eSIM fraud is that, in most cases, the devices that are being used to register an eSIM are brand new — which means that they have not been logged into device fingerprinting global databases yet. Therefore, their unique fingerprints cannot be compared to those that already exist within the database.

Fortunately, there are some features that device fingerprinting technology can examine to help detect eSIM fraud, even when the device being used to register the eSIM is brand new. When a customer goes through the digital registration process to activate a new eSIM, device fingerprinting software can examine:

The network being used: Has this network been connected to previous fraud attempts carried out by other devices?

If a VPN is being used: Is the user trying to hide his or her location and other details? While not a strong fraud indication in and of itself, it's one piece of useful information in an overall picture of risk.

Device identification alone cannot detect eSIM activation fraud, but it does deliver invaluable data points and should be the baseline of any fraud prevention strategy, including the detection of possible eSIM fraud.

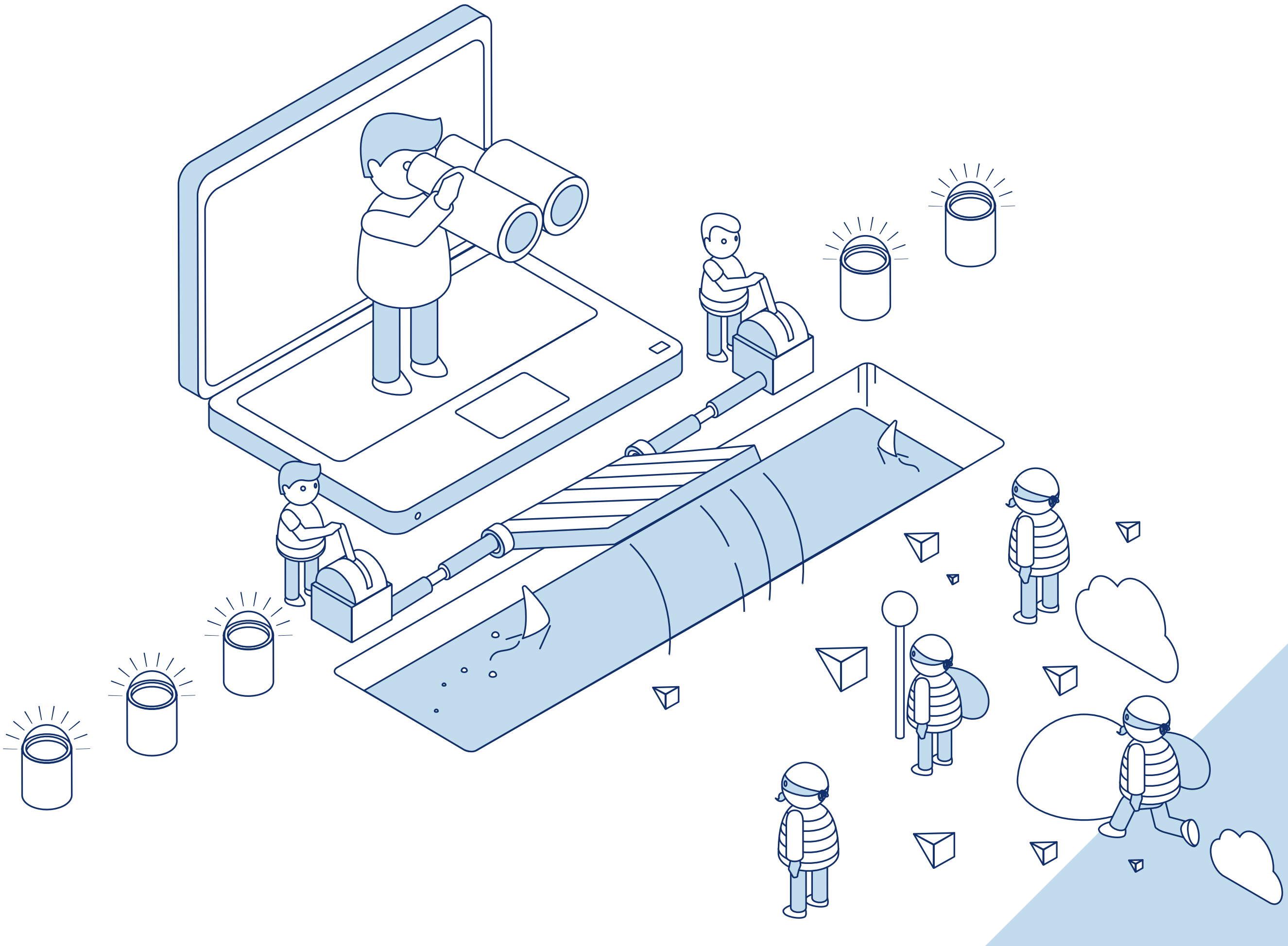


5 CONCLUSION

The change from traditional SIM cards to eSIM technology is expected to grow incredibly quickly around the globe in the next four years, leading to more and more dependence on digital onboarding and activation, eKYC solutions, and digital identity verification methods. The need for new fraud management methods has already been detected by **RISK IDENT**'s telecom industry fraud experts, who work with some of Europe's largest mobile network operators. The sooner MNOs are alerted to these new fraud management trends and the sooner they are armed with the knowledge and methods to combat eSIM activation fraud, the sooner the telecom industry as a whole can decrease eSIM fraud rates and decrease the financial and societal costs that come from this type of telecommunication fraud.

RISK IDENT recognizes the need for more sophisticated and scalable eKYC methods and identity verification methods to detect eSIM activation fraud in the telecommunications industry. **RISK IDENT** has also recognized that traditional fraud prevention solutions and teams remain valuable in the fight against telecommunication fraud and identity fraud within the industry, but they must evaluate and change the data points that they typically examine during fraud prevention to better detect eSIM activation fraud.

When mobile network operators and fraud prevention teams work together and share their knowledge, they can significantly decrease fraud rates in the telecommunications industry. That's why we at **RISK IDENT** would love to hear your thoughts and insights on detecting and stopping eSIM activation fraud and identity fraud in the telecommunications industry. Do you think that digital onboarding for eSIM activation provides new avenues for fraud?
Do you agree that email risk assessment and device fingerprinting are valuable tools to detect and decrease eSIM activation fraud? Let us know by Contacting one of our fraud experts today.



RISK IDENT

ABOUT RISK IDENT

RISK IDENT is a agile, fast-growing software company based in the heart of Hamburg. Founded in 2012 as a subsidiary of the Otto Group, we quickly became the market leader in the DACH region in the field of fraud prevention. Today we have a strong customer base of well-known companies, most of which come from the fields of e-commerce, telecommunications and financial services. Each year, we protect over €55 billion turnover against fraud for our customers. Our team currently consists of over 70 colleagues, each of whom are passionate about what we do.

HOW CAN WE HELP YOU?

Feel free to contact us anytime!

JÜRGEN +49 1604877257

Jürgen Brandt
VP of Business Development
juergen@riskident.com

RISK IDENT

Risk.Ident GmbH
Am Sandtorkai 50
20457 Hamburg
www.riskident.com

6 SOURCE OF INFORMATION

[1] "Mobile Operators Moving Too Slowly On eSIM Adoption, Say Device Manufacturers" Truphone. https://www.truphone.com/about/newsroom/mobile-operators-moving-too-slowly-on-esim-adoption-say-device-manufacturers/

[2] "Seven billion eSIMs to be active by 2024" Mobile World Live. https://www.mobileworldlive.com/latest-stories/esim-activations-set-to-reach-7-billion-in-era-of-open-mobile-connectivity

[3] "Global Embedded SIM (eSIM) Market Analysis 2016-2018 & Forecast to 2028 - Automotive Data Brokerage / 5G and Telematics 4.0 / Truck Platooning" Research and Markets. https://www.prnewswire.com/news-releases/global-embedded-sim-esim-market-analysis-2016-2018--forecast-to-2028---automotive-data-brokerage--5g-and-telematics-4-0--truck-platooning-300775506.html

[4] GSMA "Access to Mobile Service and Proof of Identity 2020: The Undisputed Linkages" https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/03/Access_to_mobile_services_2020_Singles.pdf

[5] "The Mandatory Registration of Prepaid SIM Cards" GSMA https://www.gsma.com/publicpolicy/wp-content/uploads/2016/09/GSMA2013_WhitePaper_MandatoryRegisatrationofPrepaidSIM-Users.pdf

[6] "New Report Reveals Record Level of Identity Fraud" CIFAS https://www.cifas.org.uk/newsroom/new-report-reveals-record-levels-identity-fraud-2017

[7] "This Is Fraudscape 2020" Cifas. https://www.fraudscape.co.uk/

[8] "Communications Fraud Control Association Announces Results of 2019 Global Telecom Fraud Survey" CFAA. https://cfca.org/sites/default/files/Fraud%20Loss%20Survey_2019_Press%20Release.pdf

[9] "Fraud Hits Millennials, Telecommunications Industry Hard During Pandemic" CNP https://news.cardnotpresent.com/news/fraud-hits-millennials-telecommunications-industry-hard-during-pandemic

[10] "Fraud Hits Millennials, Telecommunications Industry Hard During Pandemic" CNP https://news.cardnotpresent.com/news/fraud-hits-millennials-telecommunications-industry-hard-during-pandemic

[11] "Cyber-Telecom Crime Report 2019" Europol. https://www.europol.europa.eu/publications-documents/cyber-telecom-crime-report-2019

[12] "Communications Fraud Control Association Announces Results of 2019 Global Telecom Fraud Survey" CFAA. https://cfca.org/sites/default/files/Fraud%20Loss%20Survey_2019_Press%20Release.pdf

[13] "Customer Digital Onboarding" Experian. https://www.experian.co.uk/assets/business-services/brochures/digital-onboarding.pdf

[14] "Mobile Digital Identity To Be A $7 Billion Opportunity In 2024, As Operators Become ID Brokers" Juniper Research. https://www.juniperresearch.com/press/press-releases/mobile-digital-identity-7-bn-opportunity-2024

[15] "Biometrics and Fraud: You're One in 7 Billion" Payments Cards and Mobile. https://www.paymentscardsandmobile.com/biometrics-and-fraud-youre-one-in-7-billion/

[16] "Biometrics and Fraud: You're One in 7 Billion" Payments Cards and Mobile. https://www.paymentscardsandmobile.com/biometrics-and-fraud-youre-one-in-7-billion/

[17] GSMA "Access to Mobile Service and Proof of Identity 2020: The Undisputed Linkages" https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/03/Access_to_mobile_services_2020_Singles.pdf

[18] "Consumer Concerns On Cybercrime Rise As Faith In Anti-Fraud Disappears" Payments Cards and Mobile. https://www.paymentscardsandmobile.com/consumer-concerns-on-cybercrime-rise-as-faith-in-anti-fraud-disappears/

[19] "Consumer Concerns On Cybercrime Rise As Faith In Anti-Fraud Disappears" Payments Cards and Mobile. https://www.paymentscardsandmobile.com/consumer-concerns-on-cybercrime-rise-as-faith-in-anti-fraud-disappears/

[20] "Customer Digital Onboarding" Experian. https://www.experian.co.uk/assets/business-services/brochures/digital-onboarding.pdf