

Identity Verification is essential to the future of the online marketplace.

The exponential growth of the Digital Economy has created many challenges for businesses in validating and protecting their users' private information. These and other impediments such as establishing trust in the online marketplace and verifying users are costing business multiple billions annually and impacting consumer confidence.

The threat of personal information: name, address, password, credit card details, etc. being regularly stolen for fraudulent use and monetary theft is constant and causing significant issues for all stakeholders of the digital economy. Consumer's credit cards can be used without their permission leading to their identity being exploited to create new accounts with online merchants for criminal activity.

Verizon Enterprise reported 53k+ security incidents, in its 2018 Data Breach investigations Report. Non-compliance with EU GDPR carries penalties of up to €20m or 4% of global revenue and this takes no account of the costs to business of the breach itself. Sedicii's unique ZKP technology helps organisations to comply with strict AML and Data Protection legislation as no data is exposed during the authentication process.

Sedicii ZKP Verification

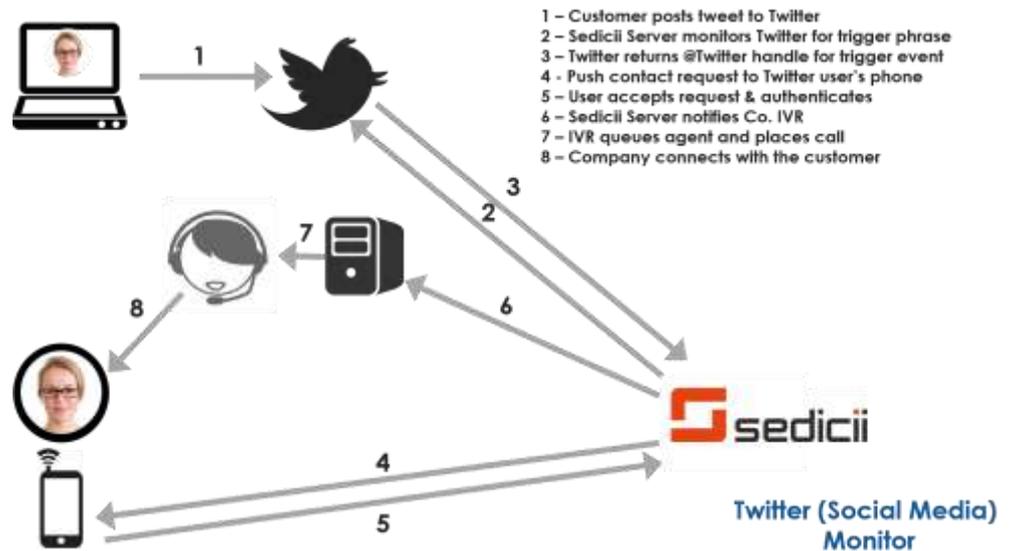
- ✓ Maximum Reliability
- ✓ Full Automation
- ✓ No Data exposure
- ✓ Fully GDPR/AML Compliant

The Problem:

Social media has become the channel of choice for many interactions between service providers and the public. These channels create huge problems for companies because of their public and real-time nature. If the post on the channel is negative, it requires a rapid response to the customer to address and solve it. Equally, this contact could be a sales opportunity if it is captured and actioned right at the time that it happens. It may or may not be appropriate to address the person via the same channel and hence the ability to communicate personally via phone could be extremely beneficial.

The Solution:

Sedicii has developed a social media monitoring service that will allow a trigger event to be monitored for. Once the event has been identified the Sedicii service immediately sends a request to the registered phone for the user of the associated Twitter or Facebook account. This allows an organisation to address a comment made in a very public channel, Twitter, in a private and personal way and do it immediately before it has possibly expanded into a much bigger issue. At the initiation of the push request the customer has a choice as to whether they want to interact or not. Should they choose to interact the customer is asked to authenticate and then they are connected to an agent to deal with the matter at hand.



Sedicii Real-time Social Media Authentication

See Sedicii in action...

A Sedicii demonstration can be arranged to experience the benefits of Sedicii Zero Knowledge Proof Verification in action.

To find about more or to set up a live demonstration, call or contact us using the details below.

Sedicii Headquarters, Ireland
ArcLabs Research & Innovation Centre,
W.I.T. West Campus,
Carriganore, Waterford
Ireland
X91 P20H
Phone: +353 (0)51 302191

Sedicii UK
20 Ropemaker St
London
EC2Y 9AR
Phone: +44 20 8144 8279

Sedicii USA
2F Plug and Play Techcenter
440 N. Wolfe Rd.
Sunnyvale CA94086
Phone: +1 408 786 5485

Sedicii Tenerife
C/Fotografo Jose Norberto
Rodriquez Diaz Zenon, 2
Piso 3 Oficina 3-5
Tenerife 38204

online at:

Web: www.sedicii.com
Email: contactus@sedicii.com
Twitter: [@GRRSedicii](https://twitter.com/GRRSedicii)

The purpose of the service is to allow organisations to engage with customers via a secondary, private channel (the phone) when the initial communication has been observed via a primary, public social media channel (Twitter). This allows for immediate action to be taken in the case of either a customer service event or a sales opportunity.

The Value:

The majority of today's digital consumers have embraced social media to communicate to others, irrespective of topic. This has meant an explosion of information that businesses need to monitor so they know what their customers are saying. The idea of keeping something private in today's hyper-connected world is almost non-existent.

Using the Sedicii Twitter monitor in combination with an active contact centre environment will:

- (a) Facilitate immediate action when a customer satisfaction related trigger event occurs on Twitter so that it can be addressed in a personal manner
- (b) Allow a sales opportunity to be addressed by an agent at the point where the greatest likelihood of a sale occurs
- (e) increase customer satisfaction ratings as customer complaints can be dealt with faster, more efficiently and through a personal interaction.
- (f) provide bi-directional, mutual authentication for contact centre and the customer so that the transaction can have a high degree of trust associated with it (where required).

Commercial Considerations:

The Sedicii Social Media Monitoring Service can be deployed in an 'on premise' configuration where the client enterprise will manage and maintain the service entirely independently. In the 'on premise' configuration, it is sold on a licensed basis depending on the number of users and applications.

Or, it can be provided in a cloud configuration where the same service may be shared by a number of organisations or services. In this configuration, the service is delivered on a transaction basis and managed entirely by Sedicii on behalf of the client enterprises.

Sedicii proves that a customer is not being impersonated, quickly, securely and reliably, **WITHOUT** any underlying sensitive personal information having to change hands. The user's identity attributes **NEVER** leave the device, browser or server. This reduces the burden of responsibility on the merchant whilst protecting the consumer. All sides win.