DemystData

Demyst Use-Case Attestation (DUCA)

[CLIENT NAME]

February 2020

Introduction

This document provides an executive summary of the key third-party data requirements for Consumer Application Fraud at [Client], as of February 2020.

Demyst Overview

Founded in 2010, Demyst is a leading External Data as a Service provider that accelerates and improves the entire data access lifecycle, from frictionless testing, to single point of ingestion and access, while improving data compliance. Demyst has integrated and delivered data from arguably the largest set of external data partners across consumer, business, and place data, from large incumbents alongside niche providers. To date, we deliver over 500 third party data products through to end clients under Demyst contracts, through a range of access methods including a sandbox, portal. realtime API, and data lake ingestion processes.

Demyst services Tier 1 banks, leading online lenders, small business lenders, and insurers and has offices in New York, Hong Kong, Melbourne, and Singapore. The Demyst technology platform has been certified over and over by our customers for a broad range of test and production use cases. YearlyDemyst technology processes and architecture are audited through a SOC2 and an independent comprehensive security evaluation is completed by an external party.

[Client] Overview

[Client] is looking to be a market leader in data driven decisioning and service provision. The bank's AI/ML capabilities continue to leverage the breadth of external data available and wants Demyst to help improve the derived value from external data in the most compliant and effective way.

While these steps make the customer journey more frictionless, there is a broader ethical question on whether data, just because it is available, should be leveraged. The bank and partners such as Demyst must continually examine:

- Is the use of external data for application fraud detection fair treatment of customers?
- Is the way in which data is being used, transparent to both collectors and end users?
- Are contractual guardrails in place to protect each stakeholder as well as the end customer?

[Client] and Demyst Relationship

Disclaimer

This document is fluid and currently a work-in-progress. Until signed in final form the content of the document is subject to change. The information provided in this document does not, and is not intended to, constitute legal advice; instead all information, commentary, content and materials are for general information purposes only. Recipients of this document should contact their attorney to obtain advice with respect to any particular legal matter. No recipient of this document should act, or refrain from acting, on the basis of information in this document without first seeking legal advice from counsel in the relevant jurisdiction. The views expressed and commentary within this document is the opinion of DemystData based on its experience in the industry. All liability with respect to actions taken or not taken based on the contents of this document are expressly disclaimed.

Use-case: Consumer Application Fraud

[Client]'s detection and intelligence team is interested in rapidly evaluating a set of third-party data sources to identify attributes that are predictive for fraud at the time of a customer's application. The end-goal of this use-case is to develop a real-time API using the most predictive of these attributes to:

- Maximise fraud detection
- Minimise manual review time

Data Subscription

Requested Third-party Vendor Products:

➔ **Neutrino Geocode Address:** Provides the geocode of an address, partial address, or the name of a location
➔ **Neutrino IP Probe:** Analyzes and extracts provider information for an IP address
➔ **Seon Email:** Provides an in-depth analysis and provides a fraud score for a given email address.
➔ **Telesign Live Phone:** Provides the subscriber status and whether the phone is active or disconnected, for a given phone number.

Demyst conducts detailed diligence assessments of all vendors around key aspects of their compliance, security and operational capabilities. Not all of these are detailed in this document and are subject to existing agreements between The Client and Demyst.

However there are key elements of our diligence process that are particularly relevant to [Client]' specific queries on business continuity, privacy, provenance and ethics. The following summarises an excerpt of the diligence that Demyst conducted for the purposes of informing a client's decisioning on whether and how to harness these sources.

DemystData

Demyst Diligence Report

Category	Field	Demyst Response
Business and Financial Condition	Please describe the nature of your business.	Demyst is an External Data as a Service provider that accelerates and improves the entire data access lifecycle, from frictionless testing, to single point of ingestion and access, while improving data compliance.
	How many employees work for your company?	50-55
	Where are these employees located?	USA, Australia, Singapore, Hong Kong
Service Hosting	Is your service run from your own Data Centre Location(s) (relative to services provided)	No, our service is run from our AWS server locations.
	Which cloud providers do you rely on?	Amazon AWS is the cloud provider we rely on here at Demyst.
	Have you researched your cloud providers best security practices?	Yes we have and best practices are always utilized.
	Which data centers/countries/geographies are you deployed in?	us-east-1, ap-east-1, ap-southeast-1, ap-southeast-2, and eu-west-1 are the locations.
	On-premise solution only	N/A
Vendor Supporting Documentation	Most recent Application Code Review or Penetration Testing Reports (carried out by independent third party)	The most recent test can be found Here.
	Does the penetration test follow an industry approved methodology:	Yes it does follow an industry approved methodology
	Information Security Policies and Procedures	Information security policy can be found here.
	Data Flow Diagram	Data flow diagram is here.
	Any other Documents supporting your responses in this questionnaire (Please provide a description for each document).	N/A.
	PCI, SOC2 type II or ISO27001 certification reports	Yes. a SOC2 type II is available.

	Other Independent Audit report (please provide details)	N/A.
Encryption	Do you encrypt customer data? If so, please upload relevant documentation and describe how you encrypt customer data.	Yes. AES-256 bit is the encryption mechanism we utilize here at Demyst.
Data Provenance and Information Security	Describe where data contained in your data products is sourced from.	The data contained within the Demyst data products is sourced from third-party vendors who are fully vetted through Demyst's due diligence process.
	Describe how data contained in your data products is collected (e.g., data collection through customer input on website, scraping, etc.)	Data collection depends on each third-party vendor and may vary accordingly. Information on each relevant data vendor can be seen in the long form data vendor questionnaire.
	Is consent obtained from each data subject whose information will be provided to Demyst?	Data collection depends on each third-party vendor and may vary accordingly. Information on each relevant data vendor can be seen in the long form data vendor questionnaire.
	How is data quality, veracity, and integrity ensured?	Demyst validates the quality and integrity of data provided by onboarded products by running regular match rate, error rate and attribute fill rate tests against the connectors
	Where are the physical location(s) of your data? I.e., where are your servers and data centers located?	USA, Australia, Singapore
	How will you ensure that data sent to you by Demyst will be deleted after a job is completed?	N/A
Data Provenance and Information Security	Describe how your organization decides who does and does not have access to sensitive data	Data access is limited to those who strictly need to know to provide services.
	Do you have capabilities to encrypt data?	Yes.
	How is data anonymization implemented?	N/A
	How is the anonymized data used within your organization?	N/A
	Please describe your general rules management in relation to role provisioning, deprovisioning, and recertification.	Least privileged is applied when implementing role provisioning in our environment, and when also when deprovisioning to ensure users only have need-to-know access. While we currently do not recertify accounts, annual recertification will be implemented soon as a part of our annual security initiatives in 2020.

	Which groups of staff (individual contractors and full-time) have access to personal and sensitive data handed to you?	Only Demyst employees and contractors who have an absolute need to know have access to personal and sensitive data.
	Do you keep sensitive data (as defined by your data classification matrix) in hard copy (e.g. paper copies)? If so, please describe.	No.
	Do you have a procedure for securely destroying hard copy sensitive data?	Yes
	Do you support secure deletion (e.g. degaussing/cryptographic wiping) of archived or backed-up data?	Yes, see Amazon Web Services policies on hard disk removal.
	Describe the circumstances in which customer data is allowed to leave your production systems?	Customer data might leave Demyst production systems if a customer has approved our use of an external API integration. Only a select number of data attributes are sent over TLS and these attributes are not persisted by partners.
Authentication	Do you have an internal password policy?	Yes we do have a password policy that is enforced through our info sec policy.
	Do you have complexity or length requirements for passwords?	Yes we do have a password complexity and length requirement. Passwords must be at least 8 characters, containing an uppercase and lowercase letter, a number, and a symbol ● Passwords must expire after 90 days. ● Users should not be able to reuse the last twelve passwords
	Do you hash passwords? If so, please describe how passwords are hashed.	Yes, passwords are hashed using the bcrypt algorithm https://en.wikipedia.org/wiki/Bcrypt which is the default password hashing algorithm for OpenBSD and the SUSE Linux distribution.
	Do employees/contractors have the ability to remotely connect to your production systems? (i.e. VPN)	Yes, employees through SecureVPN and MFA to access network/AWS environment,
	Is MFA required for employees/contractors to log in to production systems?	Yes MFA is required for employees to log in production systems.
	Do internal applications leverage SSO for authentication?	No
Third Party Data	Do these processors (vendors) contractually comply with your security standards for data processing?	Yes processors are contractually required to comply with our security standards for data processing that we have set.

Processing	Do you regularly audit your critical vendors?	Yes we do regularly audit our critical vendors through our Vendor Due diligence program. Capabilities are expanding in which every single data provider will be audited and assessed.
GDPR/CCPA	Does the CCPA apply to your organization? If so, please describe your policies, procedures, and processes that ensure compliance with CCPA?	Demyst not located in California however, we may on occasion obtain data from California residents. This data comes from third-party vendors who are thoroughly vetted through Demyst due diligence process which addresses CCPA.
	Does the GDPR apply to your organization? If so, please describe your policies, procedures, and processes that ensure compliance with GDPR?	No GDPR does not apply to our organization.
EU Data/Privacy Shield	(Only applicable if your company/data centers are based in the US) For the provision of services, do you process EU citizens' personal data?	N/A
	Are you currently Privacy Shield certified? If so, please link to your certification.	No
	Have you appointed a Data Protection Officer (DPO)?	N/A
	Do you plan on being Privacy Shield certified within the next 12 months?	N/A
Management Program	Do you have a formal Information Security Program (InfoSec SP) in place?	Yes we do have a formal Information Security Program (InfoSec SP) in place
	Do you review your Information Security Policies at least once a year?	Yes we review info security policies on a yearly basis
	Do you have an Information security risk management program (InfoSec RMP)?	Yes we do have an InfoSec RMP within our InfoSec team.
	Do you have management support or a security management forum to evaluate and take action on security risks?	Yes internally we have a core team that evaluates and takes action on security risks.
	Do you have a dedicated information security team? If so, what is the composition and reporting structure?	Yes. Info Sec analyst reports to the Information Security Manager, who reports to the head of legal. Team works alongside our security infrastructure team.

Policy Execution	Do your information security and privacy policies align with industry standards (ISO-27001, NIST Cyber Security Framework, ISO-22307, CoBIT, etc.)?	Yes, we align our policies around ISO 27001 and the NIST frameworks.
	Do you have a policy exception process?	No we do not.
	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	Yes formal sanctions are established for employees who violate security policies and procedures.
Background Checks	Are all employment candidates, contractors and involved third parties subject to background verification (as allowed by local laws, regulations, ethics and contractual constraints)?	Yes anyone employed by Demyst is required to go through a background verification/check.
Confidentiality	Are all personnel required to sign Confidentiality Agreements to protect customer information, as a condition of employment?	Yes all personnel are required to sign Confidentiality Agreements to protect customer information, as a condition of employment, prior to coming on board.
Acceptable Use	Are all personnel required to sign an Acceptable Use Policy? Please attach	Yes. It can be found here.
Job Changes and Termination	Are documented procedures followed to govern change in employment and/or termination including for timely revocation of access and return of assets?	Yes an onboarding and offboarding checklist is regularly utilized to ensure timely revocation of access and returning of assets.
Independent Third-Party Penetration Testing	How is your network security testing performed? Internal, third parties or both? If so, what is the cadence? Explain your methodology	Third party pen test. Bi-annually (April and October).
	How is your application security testing performed? Internal, third parties or both? If so, what is the cadence? Explain your methodology	Third party pen test. Bi-annually (April and October).
Vulnerability Management/Patching	Do you have network vulnerability management processes and procedures? If so, please summarise or attach your network vulnerability management processes and procedures.	Vulnerability management policy can be found here.
	Do you have a timeframe for patching critical vulnerabilities? If so, please describe your timeframe for patching critical vulnerabilities.	Required to be patched within 48 hours as per Vulnerability management policy.

	Do you use tools for vulnerability management? If so, please describe the tools you use for vulnerability management.	Tenable is the vulnerability management tool we utilize.
	Do you have application vulnerability management processes and procedures? If so, please summarise or attach your application vulnerability management processes and procedures.	Yes we do, Attached is our Vulnerability management process overview. Here.
	Do you use tools for application vulnerability management? If so, please detail the tools you use for application vulnerability management.	Tnable is the vulnerability management tool we utilize.
	Do you regularly evaluate patches and updates for your infrastructure?	Yes patches are regularly evaluated for our infrastructure.
	Do you have an established bug bounty program?	No we do not.
Endpoint Security - End User	Are all endpoint laptops that connect directly to production networks centrally managed?	Yes all endpoint laptops that connect directly to production networks centrally managed through JAMF.
	Describe standard employee issued device security configuration/features. (Login Password, antimalware, Full Disk Encryption, Administrative Privileges, Firewall, Auto-lock, etc.)	Login Password, antimalware, anti-virus, Full Disk Encryption, Administrative Privileges based on need to know, Firewall, and DLP tool.
	Does sensitive or private data ever reside on endpoint devices? How is this policy enforced?	No. Through strict policies, provisioned “data labs” and using DLP technologies.
Endpoint Security - Production Server	Do you limit data exfiltration from production endpoint devices? If so, please describe how you limit data exfiltration from production endpoint devices.	Through our Data loss prevention (DLP) tool that is pushed out to each endpoint devices.
	What systems do you have in place that mitigate classes of web application vulnerabilities? (e.g.: WAF, proxies, etc)	AlertLogic IDS
	Do you have breach detection systems and/or anomaly detection with alerting?	Yes, through our IDS system.
Infrastructur	Are the hosts where the service is running uniformly configured?	Yes, through CloudFormation templates.

e Security	Are changes to the production environment reviewed by at least two engineers/operations staff?	Yes
	Describe your secrets management strategy:(auth tokens, passwords, API credentials, certificates)	Demyst uses a mixture of Usernames and Passwords as well as JWT and API key tokens.
	Are all security events (authentication events, SSH session commands, privilege elevations) in production logged?	Yes all security events in production are logged.
	Is the production network segmented in to different zones based on security levels?	Yes the production network is segmented in to different zones
	Do you have a process for making changes to network configuration? If so, please describe this process for making changes to network configuration.	Yes, all network configurations are kept in CloudFormation and changes go through a code review process.
	Is all network traffic over public networks to the production infrastructure sent over cryptographically sound encrypted connections? (TLS, VPN, IPSEC, etc). If there are plaintext connections, what is sent unencrypted?	TLS 1.2 is utilized to ensure network traffic is sent through an encrypted connection.
Cryptograp hy	Do you use cryptographic frameworks to secure data in transit over public networks? If so, please describe the cryptographic frameworks you use.	TLS 1.2
	Do you use cryptographic frameworks to secure data at rest? If so, please describe the cryptographic frameworks you use.	AES 256
	Do you use cryptographic frameworks to store passwords? If so, please describe the cryptographic frameworks you use.	Devise + Bcrypt for Ruby on Rails
	Are any custom cryptographic frameworks/implementations used? If so, have any custom cryptographic frameworks been reviewed by an independent 3rd party?	No
	Are cryptographic keys (key management system, etc) managed	All encryption keys are managed in AWS KMS.

	within your system? If so, please describe how cryptographic keys(key management system, etc) are managed.	
Security Awareness	Do you have a security awareness program for personnel? If so, please describe the program.	Yes. Security training is pushed out to each new employee, and security training modules (as of january 2020) will be a requirement for each employee to complete yearly.
Threat Intelligence	Do you keep aware of potential security vulnerabilities and threats that may affect your service? If so, please describe how you keep aware of potential security vulnerabilities and threats that may affect your service.	Yes, we subscribe to notifications of security related updates in Slack
Monitoring	Do you log and alert on relevant security events? (this includes the network and application layer)? If so, please describe how you log and alert on relevant security events.	Yes, collection of relevant security events is picked up through our IDS and our SIEM tool. Weekly reports are reviewed and distributed to the overall security team.
Incident Response	Do you have a Security Incident Response Program? If so, please describe or attach your Security Incident Response Program.	Yes. Attached here.
	Do you test your Incident Response Plan? If so, please describe how it is tested and include cadence.	Yes our incident response plan is tested annually
	Do you have a formal service level agreement (SLA) for incident response?	Yes. 5 days. Within no more than 5 business days of eradication, the IRT must conduct a retrospective, or post-mortem,
Incident Communication	Do you have formally defined criteria for notifying a client during an incident that might impact the security of their data or systems? What are your SLAs for notification?	Yes. The Business Owner is responsible for ensuring contact information is kept up-to-date. Minor incidents may be communicated via email. Initial notification of major incidents should be through both phone and email, and updates should be sent via email, or as otherwise agreed to by the client and Demyst. Clients may have specific instructions when communicating with their organizations. Special instructions from clients should be added to their services agreement with Demyst.
Secure SDLC	Do you do static code analysis?	Yes, we do conduct Static code analysis
	Do you ensure code is being developed securely? If so, please describe how you ensure code is being developed securely.	Yes. To prevent vulnerabilities to software authored by the Demyst software development team, all code changes are peered reviewed before they are deployed. If any reviewer feels changes may be degrading the security of the

		platform, the review is immediately halted and escalated to managers for review. Changes to critical infrastructure - including VPC configuration, Security Group rules, Network ACLs, and Identity & Access Management - must be reviewed by a member of the Infrastructure Automation Team that did not author the changes. If the change is urgent and no member of the Automation team is available, the CTO or a Senior Platform Engineer may review it. However, a member of the Automation Team must review it retroactively.
	Is threat modelling incorporated in the design phase of development? If so, please describe how threat modelling is incorporated in the design phase of development.	No
	Do you train developers in SSDLC / Secure Coding Practices? If so, please describe how you train developers in SSDLC / Secure Coding Practices.	Yes developers are trained in secure coding best practices. Details of what is learned by our developers is referenced above.
Deployment Processes	What percentage of your production code is covered by automated tests?	Depends on the system. Average is greater than 50%
	Is a staging/pre-production system used to validate build artifacts before promotion to production?	Yes
Dependency Management	Do you maintain a bill of materials for third party libraries or code in your service?	Yes
	Do you monitor vulnerabilities in dependencies? If so, please describe how you monitor vulnerabilities in dependencies.	Yes, Github vulnerabilities
	Do you outsource development? (contracted with a 3rd party? open source project inclusion?)	Yes, Intive in Poland.
	What types of security reviews do you perform on custom-built software?	Demyst has a code review process for any change that will move into production. As part of our code review process we evaluate the change from a security standpoint.
Authentication	Please describe how you authenticate users: If passwords are used, describe complexity requirements, and how passwords are protected. If SSO is supported, please describe the available options	For password authentication we require at least one symbol, number, upper and lower case letter, and total length > 8 characters. Passwords are hashed using the bcrypt algorithm and only the hash is stored in

		the database. For SSO we support SAML integrations.
	Does application allow user MFA to be enforced by admins?	No
	Does application support IP whitelisting for user authentication?	No
Role Based Access Control	Does your application support standardized roles and permissions for users (ie admin, user)?	Yes standardized roles such as admin, users are enforced and supported.
	Does your application enable custom granular permissions and roles to be created?	Yes
Audit logging	Which audit trails and logs are kept for systems and applications with access to customer data?	Yes
	Does your application provide customer administrators with direct access to verbose audit logs (API, export, viewer etc)?	No, but it can be provided
Data Retention	Does your application allow for custom data retention policy for customer data?	Yes
Change management	Does your application provide a change log?	Yes our application does provide a change log.
	Does your application provide a sandbox environment to customers for testing?	Yes
API Management	Does your API implement rate limiting?	No
	Does your application store API keys? If so, please describe how your application stores API keys.	Yes, API keys are created and then encrypted.
	Does application support IP whitelisting for API access?	Yes
Internal Audits	Do you conduct internal audits (audits lead by your personnel) of the service? If so, please describe the scope, remediation process and frequency of audits.	While we do not have audits conducted on our service, we do have external audits conducted on our company, and pen-tests done on our network and application.

External Audits	Do you conduct external (third-party) audits of the service? If so, please describe the scope and frequency of audits.	
	Please provide a copy of the most recent report.	N/A
Certifications	Which IT operational, security, privacy related standards, certifications and/or regulations you do comply with?	SOC 2 type II.
	Please provide a copy of the most recent certifications.	SOC 2 type II.
Privacy	Are your confidential data access controls in line with your data classification matrix?	Yes. Only those Demyst employees and contractors with an absolute need to know are permitted to access data. This applies across the board and encompasses all types of data.
	Do you share customer data with, or enable direct access by, any third-party?	No.
	Do you seek a right to use or own customer derived data for your own purposes?	No.
	Is your Privacy Notice/ Privacy Policy externally available? Please provide us with the URL.	Yes - https://demyst.com/privacy-policy

DemystData

Vendor Use-case Metadata

Field	Neutrino Response	Seon Response	Telesign Response	Demyst Comment
Nature of Business	Neutrino's Web based APIs makes developer lives easier by providing a set of useful, easy and time saving API's to solve common and recurring problems across different platforms and programming languages.	Seon strives to help online businesses reduce the costs, time, and challenges faced due to fraud. Their AI-powered solutions allow for easy data enrichment and improved fraud decision making	Telesign is a communications platform that emphasizes security. Telesign Live Phone ID provides the subscriber status, whether the phone is active or disconnected, of the phone number.	*Acceptable*
Business Continuity and Disaster Recovery	Neutrino API operates a fully distributed system spanning multiple cloud providers. Within 24 hours for any event in which our servers or your account data has been potentially accessed by an outside party. They have a secondary data centre that with all of the same security processes and procedures in case the primary centre crashes	Seon uses CloudTrail (AWS) for event history on their AWS account to detect system compromise. They assume data breach incidents as a general incident according to the ISMS_PL_09_Information Security Incident Management Policy and have built their BCMS according to the best practices (ISO 22301). They have Business Continuity Policy, Framework and Plan which is tested annually along with a backup centre	Customer traffic is distributed via geo-load balancing among active data centers. All data centers are externally monitored by a third-party on a 24x7x365 basis. In the event of a disaster impacting one or more active data centers, TeleSign will shift traffic away from the impacted data centers within minutes as part of their Disaster Recovery (DR) process.	*Acceptable*
Conducted probity checks for any individuals with access to client data	Yes	Yes	Yes	*Acceptable*
Contains information on individuals?	Yes	Yes	Yes, Phone ID Contact is contracted to Demyst and can return first and last name, and an associated billing address. Contact Plus is also available, and in some geographies could also return email and a national ID.	*All providers must ensure compliance with any and all DPL. Telesign doesn't provide any sensitive information so no heightened scrutiny is triggered.*

Contains Personally Identifiable Information (PII)?	IP Address, Street Address, Latitude/Longitude	Yes - Email, Phone number, IP Address	Some products may return, or require, other data that is PII. In particular, the products requesting or returning other PII are PhoneID Contact, Contact Plus, and Contact Match.	*No heightened scrutiny is triggered based on these attributes*
GDPR and CCPA considerations	Neutrino API complies with the provisions of the Regulation (EU) 2016/679 of the European Parliament, known as the General Data Protection Regulation (GDPR) as well as the New Zealand Privacy Bill (https://www.neutrinoapi.com/privacy-policy/)	Seon's infrastructure including servers and databases are based in the EU (Dublin, Ireland) and US (Northern Virginia). Seon is registered as a data-processor at the Hungarian National Authority for Data Protection and Fraud prevention is a legal basis for processing data according to the GDPR. Per GDPR requirements, fraud prevention requires passive consent on the controller side.	TeleSign is fully GDPR and CCPA compliant. TeleSign employs a Privacy Office that is responsible for privacy policy and compliance of the organization and a documented privacy policy. - TeleSign's compliance with GDPR Privacy regulations – www.telesign.com/gdpr - TeleSign's compliance with CCPA Privacy regulations - www.telesign.com/ccpa - TeleSign's alignment with ISO Security standard – www.telesign.com/security Customers should sign a DPA with TeleSign.	*Neutrino is acceptable for GDPR, need more information to determine acceptability for CCPA* *Demyst would suggest gaining more information to ensure Seon's compliance with GDPR and CCPA requirements.* *Telesign is acceptable for GDPR and CCPA*
Data Quality and Reliability	Neutrino regularly reviews their data using both machine algorithms and human checks	The nature of their service is that they get it from third parties. They monitor the ratio of false positives and false negatives from the data received from their third-parties. If the DevOps team aren't confident in the quality/accuracy of the results they will return the results as "unknown".	TeleSign regularly assesses data providers and prioritizes those with the highest quality, reliability and data integrity when sourcing data.	*Acceptable*
Presence of explainable, proprietary attributes or scores	No	Seon provides a proprietary fraud score for each of their APIs and returns the rules that make up the score as part of the API response.	Where proprietary attributes/scores are returned, a limited explanation for the Score can be provided.	*Acceptable*

Upstream source of data, if any.	Various in-house tools and third-party providers of publicly available data sources. None of these sources have access to customer data provided to Neutrino.	Seon's primary upstream sources for their data are: - WhoIs - HaveIbeenpwned - Scraping of publicly available information from Social Media sites. - Open source APIs	TeleSign is sourcing directly our data from carriers/providers and other authoritative sources compliant with any applicable laws with regards to use of personal data. By other authoritative sources we are referring (but not limited to): - Local aggregators appointed by carriers to promote and re-sell identity services - Local aggregators appointed by local regulators to offer one or many services for telecom regulation purposes (e.g. porting management) - Technical integrator in charge of telco asset management - Carriers Consortium - Any other service provider supplying relevant and timely information as well as contextual data around phone numbers	*What sources do these providers constitute as "public" sources? If they are sources other than governmental sources, what is the lawful use basis for collection, use case and onward transfer? Do they audit third-party providers for lawful use basis?*
Are there agreements in place with upstream sources that enforce information security controls?	In cases where Neutrino API purchases data from third party suppliers, formal reseller contracts are in place and Neutrino API has been expressly given the legal rights to resell and/or reuse such data from the third party suppliers.	Certain databases, particularly domain-based ones are stored and maintained locally by Seon and others are dynamic leveraging upstream data sources. For those that have access to the data that Demyst provides to Seon, Seon only shares the minimal information required for matching. Seon maintains contracts with their third-parties to ensure no data is stored and that their data has been collected with sufficient customer consent.	TeleSign assesses all Third-Party Providers (e.g. external vendors, suppliers, consultants, service providers, and individuals) that provide goods and services before they are allowed access to Sensitive and Confidential data. The assessment of the Third-Party Provider information security (based on the ISO 27002:2013 security domains) and privacy controls is conducted by TeleSign's Global Security Operations (GSO) Team. Once the assessment is complete, the Third-Party Provider will enter into a contract with TeleSign, reviewed and approved by our Legal Department. The contract obligates the Third-Party Provider to adhere to TeleSign's information	*Do these contracts also state a lawful use basis is in place to allow these providers to obtain and sell the data?*

			security policies and standards.	
Physical location of your servers or data centres	USA, UK, Germany	SEON is based on AWS, utilising Ireland (primarily) and Northern Virginia data-centers. For EU clients, all of the data is stored in the EU servers. They are currently being audited for ISO2001 and are hoping to have the certification completed within the next 2-3 months.	Our current data centers are co-location facilities with Equinix in Los Angeles, Dallas, and Amsterdam.	Are steps taken by the se provider to comply with German DPL and onward transfers of information from EU and EEA?
Data Storage and Retention	They have a strict no data logging policy. Data is only kept in volatile memory for the duration of API request	For logging purposes Seon maintains data for 6 months before permanently purging however, upon request, they are happy to delete customer data within a specific timeframe.	All backups and retention are governed by standard TeleSign contracts, to have the data not retained for any longer than 90 days.	Acceptable
Data Refresh Frequency	Real-time	All Seon data is updated in real-time. If there are any service interruptions during this process, it will provide advance notice. All of Seon's upstream providers are waterfalled with multiple providers to maximise product stability	Data is not stored by TeleSign beyond 90 days.Each request for data is passed to downstream carriers/providers and other authoritative sources who are responsible for updating data. TeleSign regularly assesses data providers and prioritizes those with the highest quality, reliability and data integrity when sourcing data.	Acceptable
Contains sensitive personal information on individuals?	No	No	Yes. Phone number can be considered PII in some cases.The phone number is the basis of all TeleSign products and must be passed to TeleSign to use any service. Some products may return, or require, other data that is PII. In particular, the products requesting or returning other PII are PhoneID Contact, Contact Plus, and Contact Match.	Acceptable, and agreed that phone number can be PII, however, sensitive PII requires heightened scrutiny - how this is defined requires on the applicable law. Outside of this, no heightened security is triggered.
Contains information on minors (<18 years old)?	No	If the client sends an email address/IP address/phone number for an individual who is younger than 18 years old, then Seon will return their standard set of attributes for this individual.	No.	Acceptable for Neutrino and Telesign. For Seon, responsibility falls on the client to not send data pertaining to minors.

What are the typical use-cases for your data?	Risk / Fraud / KYC	Fraud, Credit Risk, KYC	Use case examples: - Add Two factor authentication - verify phone numbers - minimize fraud - send messages - enable secure account recovery - KYC - send alerts, notifications and reminder - reduce fake accounts - prevent account takeover - establish trusted identities - build 2-way communications	Acceptable
Are there any use-cases that this data should not be used for?	No	NA	All TeleSign data is provided as a recommendation or 'best effort' result, so should not be used as the basis for decisions where data accuracy must be guaranteed.	Acceptable
Has implied or express consent been given by the subjects of your data?	Neutrino only collects consumer email addresses if they choose to provide this information on sign up to their service. For verified accounts they also collect your phone number strictly for verification purposes. No other personal information is kept and they do not collect or store any information sent via the API	According to GDPR, passive consent is sufficient for fraud prevention. They advise clients to add a paragraph in their service to tell customers that they are using a third-party fraud prevention tool.	TeleSign has a defined customer onboarding process in which our team verifies compliance with contracts/consent and data management and protection requirements. TeleSign products are configured and made available manually via TeleSign's customer success team. Only after the required onboarding requirements have been met will a TeleSign product be made available to our customers. TeleSign also employs a Privacy Office that is responsible for privacy policy and compliance of the organization.	Demyst interprets Neutrinos response to include both implied and express consent Seon's response is acceptable for GDPR and fraud use cases, but more information required for CCPA and use cases outside of fraud. Telesign's response is acceptable

DemystData

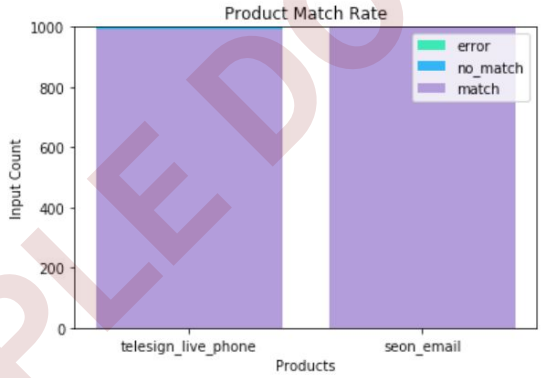
Summary Statistics

Product	Average Response Time	Error Rate	Uptime
neutrino_geocode_address	643 ms	0	100%
neutrino_ip_probe	1757 ms	0	100%
seon_email	1703 ms	0.061	100%
telesign_live_phone	1621 ms	0.29	100%

Data Quality Report

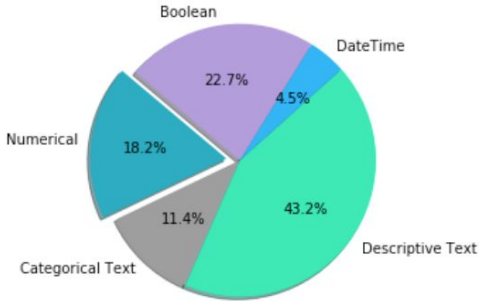
Product Stats

- telesign_live_phone
- seon_email



Data Types

- Numerical
- Categorical Text
- Descriptive Text
- DateTime
- Boolean



Demyst Recommendation

Banks have an prudential obligation to exercise reasonable care and skill when processing new applications and thus, thorough due diligence during the customer onboarding process becomes vital. ASIC Deputy Chair Peter Kell said “banks must also have robust systems in place that ensure their customers' funds are protected from the risk of fraud." As such, preventative controls, designed to deter or minimise fraud prior to onboarding, need to be implemented and the usage of third-party data plays a crucial role in that regard.

We believe that solving this broad problem benefits [Client]’s customers and achieves better financial outcomes and we believe that external data is an amazing, under-leveraged resource that [Client]’s has an opportunity to capitalise on.

We believe Neutrino, Seon and Telesign offer commercially useful data to solve this problem and in addition are compliant, secure and meet best-practices around consent and ethical usage of data.

We recommend that [Client]’s proceed with leveraging their data for application fraud detection.

Change Log

- 2020.01.15 – Version 1.0
- 2020.02.05 - Version 1.1

Approved By: _____

Signature: _____

Date: _____