

Practical ~ Experian Organizational and Subject OSINT

Analyzing the risk of a social engineering attack.

By: Domenic Lo Iacono

12/12/2023

Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. For the eyes and ears of individual recipients only, no further.

Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.

Table of Contents

Practical ~ Experian Organizational and Subject OSINT.....	1
Table of Contents.....	2
Executive Summary.....	3
Findings.....	4
Organizational.....	4
Technical and computing OSINT.....	8
Subject 1.....	10
Subject 2.....	11
Analysis.....	12
Note on analysis methodology.....	12
Organizational.....	12
Subjects.....	12
Recommendations.....	13
Appendices.....	14

Executive Summary

This document is an analysis of the potential increase in risk to Experian due to publicly available information that can be found using common OSINT techniques which can then be used to craft targeted social engineering attacks.

Experian is one of the big three credit reporting agencies and as such is at risk to social engineering attacks as they are involved in credit scoring and freezing as well as identity theft and fraud cases. Knowing this information, if additional information identified via OSINT is accessible a convincing social engineering attack can be made possible.

In the analysis of the report following the findings, it is shown that common OSINT techniques would likely enable a malicious actor to mount this type of attack at a medium risk level.

Furthermore, two specific subjects were identified and findings were collected. Those two subjects are Lynn Manzano and Cynthia Schirmer. Both listed as Directors they are in contact and in charge of critical business operations.

However, after analyzing the findings it was found that there was a low risk associated with the increase in likelihood of a successful attack due to OSINT collection regarding the two subjects.

Lastly, recommended actions that Experian should take include knowing their customer base, documenting how they show their messaging as legitimate, and attempting to remove organization data from common OSINT collection sites. Recommendations for the two subjects include practicing digital footprint reduction and understanding common phishing techniques.

Findings

Organizational

Profiles found with high confidence to be owned and operated by Experian:

Platform	Link
Facebook	https://www.facebook.com/experian/
Twitter (X)	https://twitter.com/Experian
Github	https://github.com/experiandataquality
Youtube	https://www.youtube.com/@ExperianExchange
Google Play store	https://play.google.com/store/apps/details?id=pe.com.experian.app
SoundCloud	https://soundcloud.com/experian_us/sets/look-ahead-podcast
TikTok	https://www.tiktok.com/@experian_us
LinkedIn	https://www.linkedin.com/company/experian
Indeed	https://www.indeed.com/q-Experian-I-Newport-Beach,-CA-jobs.html?vjk=5cdba51163ffddd4
Apple Store	https://apps.apple.com/us/developer/experian/id1087101089

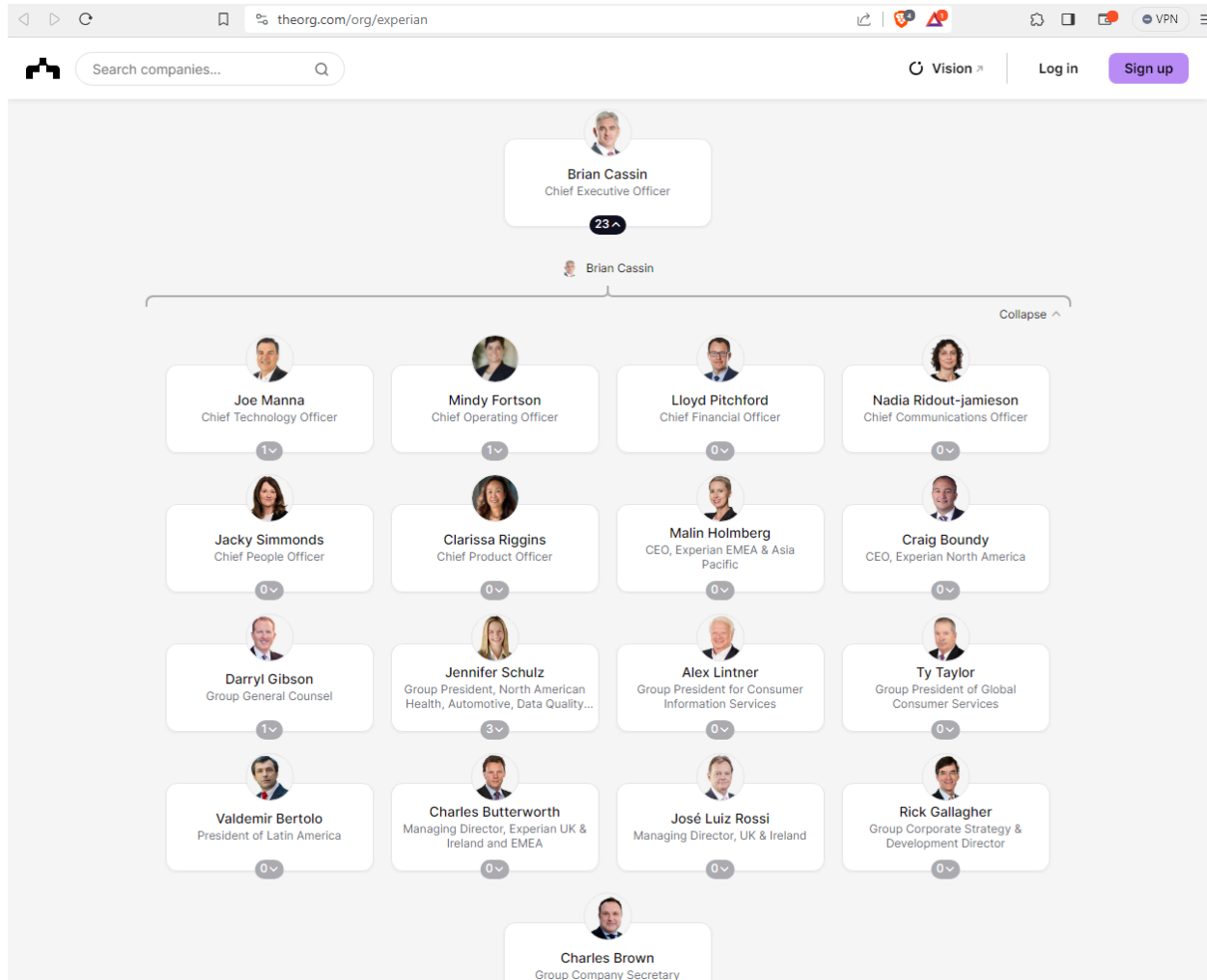
Table 1. Social Media Platforms found to be associated with Experian.

Logo which was used to reverse image search and find the profiles under Experian¹

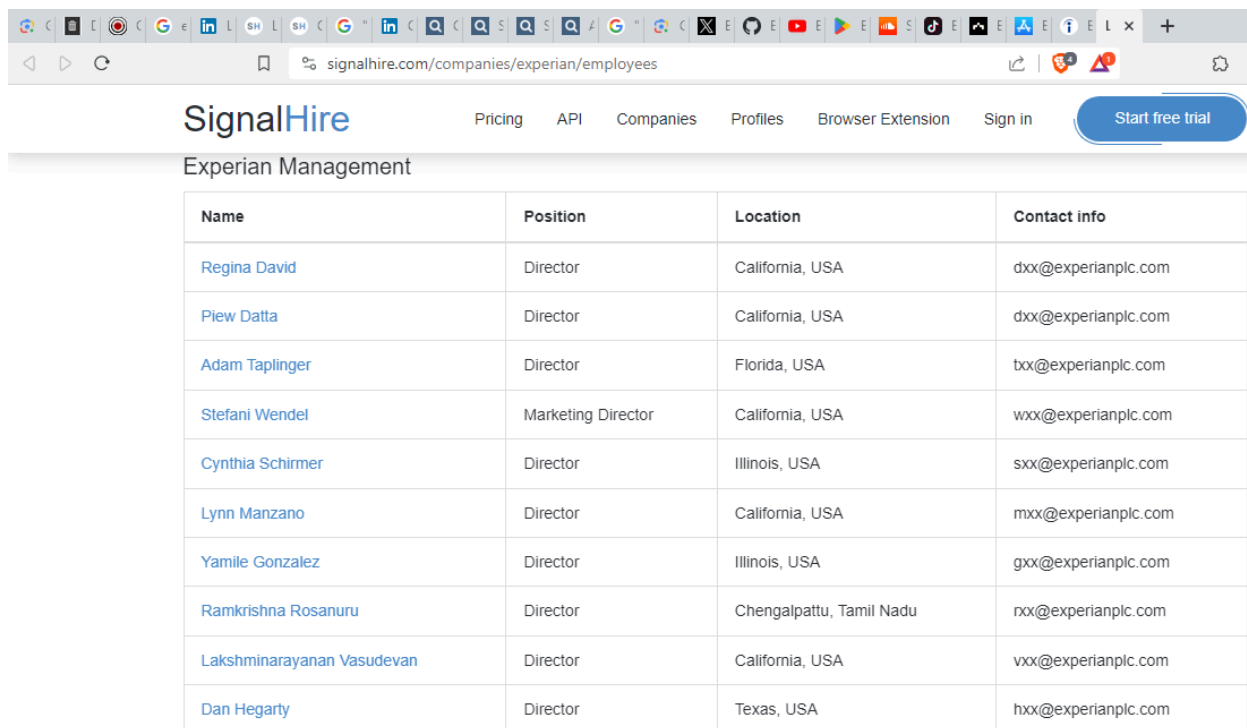


¹

Org data with high confidence²:



²<https://theorg.com/org/experian>



The screenshot shows a web browser window with the URL signalhire.com/companies/experian/employees. The page title is "SignalHire" and it includes navigation links for Pricing, API, Companies, Profiles, Browser Extension, and Sign in. A "Start free trial" button is also visible. Below the navigation bar, the section "Experian Management" is displayed, containing a table of employees.

Name	Position	Location	Contact info
Regina David	Director	California, USA	dxs@experianplc.com
Piew Datta	Director	California, USA	dxs@experianplc.com
Adam Taplinger	Director	Florida, USA	txx@experianplc.com
Stefani Wendel	Marketing Director	California, USA	wxx@experianplc.com
Cynthia Schirmer	Director	Illinois, USA	sxx@experianplc.com
Lynn Manzano	Director	California, USA	mxx@experianplc.com
Yamile Gonzalez	Director	Illinois, USA	gxx@experianplc.com
Ramkrishna Rosanuru	Director	Chengalpattu, Tamil Nadu	rxx@experianplc.com
Lakshminarayanan Vasudevan	Director	California, USA	vxx@experianplc.com
Dan Hegarty	Director	Texas, USA	hxx@experianplc.com

Note: The above screenshot captures the site³ that served as a pivot for the two identified subjects Lynn Manzano and Cynthia Schirmer.

³<https://www.signalhire.com/companies/experian/employees>

Technical and computing OSINT

Geolocation of the Experian server by pinging experian.com and pivoting the ip address as input into MaxMind⁴.

GeoIP2 Databases Demo

Show Sidebar >

IP Addresses

45.60.132.189

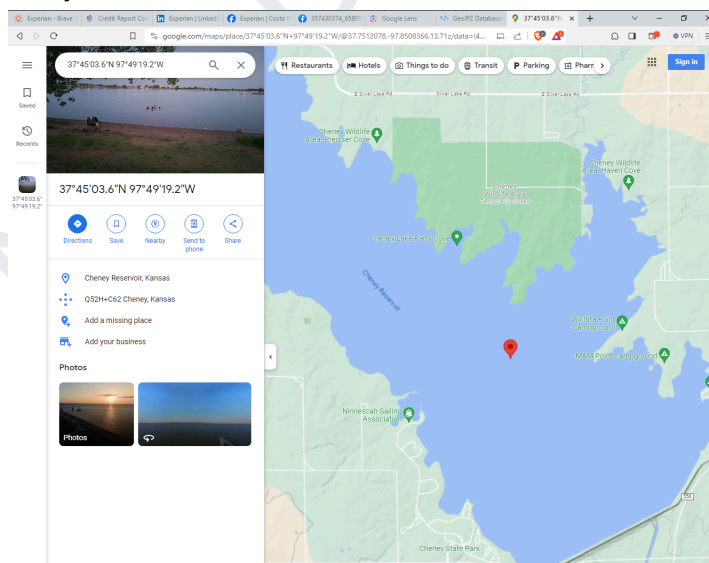
Enter up to 25 IP addresses separated by spaces or commas. You can also [test your own IP address](#).

Submit

GeoIP2 City Plus Database Results

IP Address	Country Code	Location	Network	Postal Code	Approximate Coordinates*	Accuracy Radius (km)	ISP	Organization	Domain	Metro Co
45.60.132.189	US	United States, North America	45.60.128.0/19		37.751, -97.822	1000	Incapsula	Incapsula		

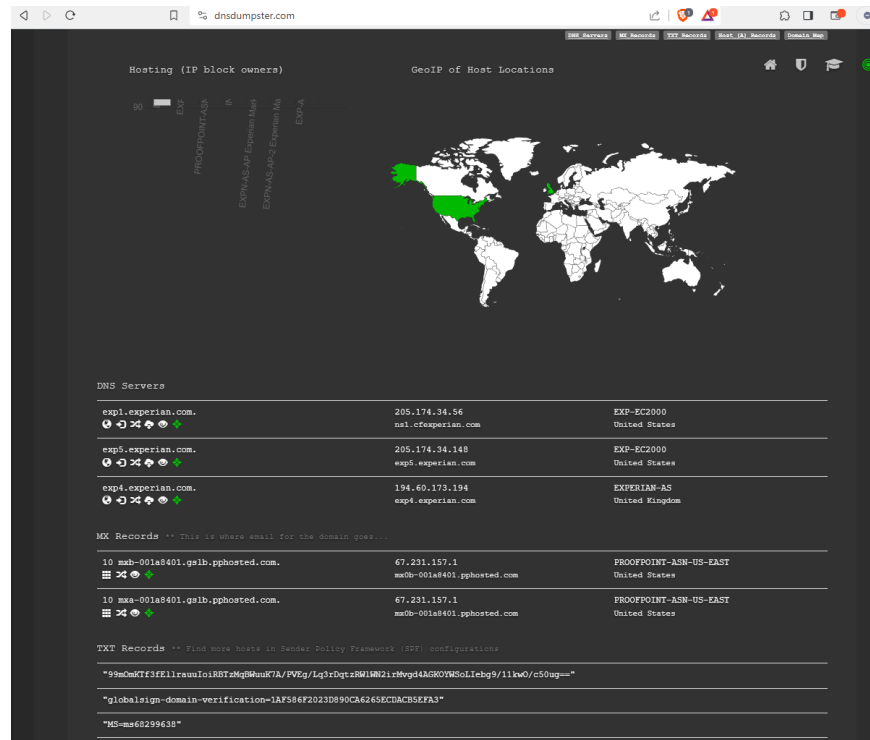
The coordinates shown above (37.751,-97.822) when viewed with Google Maps⁵ are unreliable and as such should be held with low confidence. Maxmind reinforces this confidence value when stating the accuracy radius is 1000 kilometers.



⁴<https://www.maxmind.com/en/geoipdemo>

⁵<https://www.google.com/maps/place/37%C2%B045'03.6%22N+97%C2%B049'19.2%22W/@37.7472412,-97.8269942,13.5z/data=!4m4!3m3!8m2!3d37.751!4d-97.822?entry=tuu>

DNS dumpster⁶, a tool hosted by hackertarget.com revealed information on the DNS servers and subdomains.



The screenshot above shows that Experian is hosting exclusively in the United States and Great Britain.

⁶<https://dnsdumpster.com/?q=experian.com>

Subject 1

Subject 1 is [REDACTED].

Profile identified at LinkedIn.com⁷.

Information listed in the profile includes her job title as director and physical location as [REDACTED].

Physical location is confirmed with high confidence after pivoting to Truepeoplesearch⁸.

Address: [REDACTED]

However it does display an email address for [REDACTED]@experian.cm.

Personal Connections:

- Daughter [REDACTED] Instagram account found as well as evidence of [REDACTED].
- Son [REDACTED] with an identified gmail address [REDACTED]
- Likely Husband/spouse [REDACTED]

⁷[https://www.linkedin.com/\[REDACTED\]](https://www.linkedin.com/[REDACTED])

⁸[https://www.truepeoplesearch.com/\[REDACTED\]](https://www.truepeoplesearch.com/[REDACTED])

⁹[https://www.\[REDACTED\]](https://www.[REDACTED])

Subject 2

Subject 2 is [REDACTED]

Profile identified at LinkedIn.com¹⁰

Information listed in the profile includes her job title as [REDACTED] and physical location as [REDACTED]

Physical location is confirmed after pivoting to Truepeoplesearch¹¹.

Address: [REDACTED]

Email addresses displayed include:

[REDACTED]
[REDACTED]
[REDACTED]

Personal connections displayed by Truepeoplesearch (Low confidence)

[REDACTED]
[REDACTED]
[REDACTED]

¹⁰[https://www.linkedin.com/in/\[REDACTED\]](https://www.linkedin.com/in/[REDACTED])

¹¹[https://www.truepeoplesearch.com/find/\[REDACTED\]](https://www.truepeoplesearch.com/find/[REDACTED])

Analysis

Note on analysis methodology

Social engineering is an attack that can be launched without much information on a target. However, having additional information about the target and being able to target the victims weaknesses can have a dramatic impact on the outcome of the attack. For the purposes of analysis the level that a social engineering can be likely improved past a base level using publicly available information collected via OSINT is what will determine the qualitative assessment. In other words, a target or one of the two subjects could very well become a victim of a 'base' level phishing or social engineering attack, which in my analysis would be placed at a low. There is a chance that a victim will fall for the simplest or least targeted social engineering attack. However, this also means that a very targeted and researched attack may not work. To reiterate the analysis is simply a qualitative assessment of how OSINT and collected data can increase the likelihood of a potential social engineering attack.

Organizational

After analyzing the data collected via OSINT that there is a medium risk associated with social engineering to the organization and its customers. This is due to the fact that Experian's services to common customers are publicly available and anyone can make an account. All basic information on C-Suite executives is also available via org charts. What really elevates Experian to a medium risk level though is the business that they are involved in. Experian handles credit reporting and credit freezes for millions of customers. Knowing this, an attacker could easily craft specific phishing emails claiming that a customer's credit score has dropped drastically and that there is a fraud alert on the account. In addition to the urgent scenario all branding and naming conventions for their emails are included in my findings which means an attacker could work to make the email look very convincing.

Subjects

██████████ and ██████████ are both listed as ██████████ in their LinkedIn profiles clearly and have publicly available information listed on multiple websites. However, the amount of information present doesn't significantly increase the targeting capability of an attacker. For this reason, there is a low risk of OSINT collection and other publicly available information making a significant difference in social engineering attacks against the subjects.

Some attacks that could still be launched include impersonating higher management, urgent calls/emergencies related to loved ones identified, and targeting secondary emails.

Recommendations

My overall recommendation to the organization is to understand the customer base. Many that use Experian's services for credit reporting and credit freezes could be susceptible to different scams or social engineering attacks related to those services. Make sure to have clear cut and easily identifiable information that points to why the alerts that are legitimately sent out are legitimate and be sure to alert customers to potential scams.

A secondary recommendation is to wipe or clear org chart data from the web when possible. This information makes it very easy for an attacker to plan a potential attack and seek high priority targets. Furthermore, implementing phishing training for corporate employees that are at the highest risk of compromise is a necessary strategy.

For the two subjects, practicing digital footprint reduction on themselves as well as family members or trusted individuals would likely mitigate the risk of social engineering attacks stemming from OSINT collection. Being aware of common scams as well as phishing techniques through training is also necessary at the individual level.

A specific example of practicing digital footprint management for subject 1 [REDACTED] would relate to [REDACTED]s (Identified as [REDACTED] Daughter) [REDACTED]. Understanding the risks associated with social media and being careful not to post any identifiable or sensitive information is an important step to mitigate the risk of a social engineering attack.

Appendices

Confidence Level	Description
High	The information or finding was collected from a highly reputable source as well as consistent with other sources.
Medium	The information of finding was collected from a fairly reputable source and consistent with some other sources.
Low	The information of finding was collected from either a fairly reputable source but lacking in consistency from other sources or is from a less reputable source. There is either little or no contradictory evidence to the finding.

Table 2. Confidence Levels and Descriptions

Risk Level	Description
High	A large amount of high confidence data was found on the target that includes any of the following: personally identifiable information, sensitive information, location data, critical business information/procedures, etc.
Medium	A fair amount of high or medium confidence data was found on the target that includes any of the following: personally identifiable information, sensitive information, location data, critical business information/procedures, etc.
Low	A small amount of medium or low confidence data was found on the target that includes any of the following: personally identifiable information, sensitive information, location data, critical business information/procedures, etc.

Table 3. Risk Levels and Descriptions