IRONSWEEP

DIGITAL RISK ASSESSMENTS & MONITORING

TRACE Assessment

Presented To:

Marta J. Williamson

Date:

May 3, 2025

help@ironsweep.com

www.ironsweep.com

About TRACE

Digital Footprint Assessment

A digital footprint refers to the trail of data you leave behind when you interact with digital services — whether actively, such as using an app or making an online purchase, or passively, when others publish information about you on platforms like social media or online forums.

Having a digital footprint is inevitable in today's connected world. However, because elements of your digital presence may be publicly accessible, it's important to understand what information is exposed and how to manage it proactively.

The **TRACE ASSESSMENT** outlines what can be discovered about you through basic online research — and offers practical steps to reduce your visibility to bad actors and protect your personal security.

We scan the surface of the internet to find what's publicly visible about you — including old accounts, directory listings, and anything that might come up when someone searches your name.

"I had no idea how much of my personal information was still online until TRACE uncovered it all — and helped me clean it up fast."

--C. Williams, Trace Assessment Client

How to Read This Report

This report was created to give you a clear view of what others — from bad actors to business partners — can discover about you online. It's organized to highlight the most critical risks first, followed by detailed findings and actionable recommendations. Items in red are critical and require urgent attention.

Even if some items seem minor, patterns of exposure can be exploited. Public-facing professionals are prime targets for social engineering — where attackers use publicly available details to manipulate, impersonate, or deceive. The more they can learn about you online, the easier it becomes to breach your trust, your network, or your reputation. Please read carefully, ask questions, and take steps where advised — your digital safety depends on it.

Executive Summary

This TRACE assessment uncovered **multiple critical exposures** tied to the client's name, email addresses, and online activity. Sensitive personal information, historical data leaks, and impersonation vectors were discovered across mainstream and obscure platforms. Immediate remediation is advised to reduce reputational and operational risk.

Scope & Methodology

Target identifiers include:

- Full legal name
- Known aliases
- Three active email addresses
- One phone number
- Publicly available photos

This assessment focused on unprotected and publicly accessible data sources only.

Findings Overview

Digital Identity & Exposure

- Full home address and spouse's name listed on:
  - Spokeo
  - Intellius
  - BeenVerified
- Amazon wish list (still public) containing children's names and a future travel itinerary
- Resume PDF cached from a former employer's site containing DOB and SSN last four digits

Social Media Presence

- Inactive Facebook account still indexable with outdated employer and personal email
- Found duplicate Instagram profile using client's photo and near-identical handle
- Twitter account had public "likes" tied to politically sensitive content from 2017

Data Breaches

- Exposed in 8 known breaches including Dropbox, MyFitnessPal, and LinkedIn
- Email-password combinations still searchable in at least 3 public breach aggregators
- One leaked password matched an active business account login

Impersonation Risk

- Spoof email domain registered 3 months ago (example: executive-name.net)
- LinkedIn clone profile found with altered employment history and used in recruitment scam
- Craigslist ads falsely listed under client's name and city, including one in "adult services"

Search Engine Visibility

- Cached forum post from 2009 discussing controversial political views tied to full name
- Publicly indexed PDF showing client's signature and scanned ID on an old nonprofit site
- Negative Glassdoor review implying unethical behavior (name not tagged, but inferred contextually)

Business & Legal Exposure

- Home LLC registration exposed full residential address on state business filings
- Personal cellphone listed on 3 brokered data sources and WHOIS domain history
- Digital event sign-up from 2022 publicly shows all registrants' names and titles

Your Criticality Assessment

CRITICAL

Findings:
- Public wish list revealing family patterns (location, school names)
- Active login credentials in breach reused on current email
- ID scan and signature publicly available

These findings pose high reputational, physical, and account compromise risk.

IRONSWEEP Criticality Assessment Scale

Level	Description	Example Risks
LOW	Minimal impact. Exposure is outdated, low-value, or unlikely to be exploited.	Old social profile with no identifying info, generic public listing
MODERATE	Exposure could be used in combination with other data or in low-level scams.	Leaked email address in old breach, full name on third-party directory
HIGH	Poses a direct risk to personal or professional safety or security.	Public home address, active account credentials, impersonation profile
CRITICAL	Immediate risk of exploitation with high business, legal, or reputational impact.	Reused password in breach, ID scan online, spoofed domain or email in use

My Recommendations:

Based on what we uncovered, Marti, and given our conversation about your concerns and your recent experiences following the convention you attended and your misplaced phone, I strongly recommend that you take immediate steps to lock down the most sensitive areas of your digital presence. Several findings in this report — including outdated but still visible personal data, duplicate accounts, and credential exposures — leave you vulnerable to impersonation, targeted scams, and even reputational damage.

This is the exact type of information used to craft convincing phishing attempts, fake profiles, and social engineering campaigns. You're in a high-visibility position, and that makes you a more appealing and profitable target. You already claimed to have recently been the target of a possible phishing attempt, which your assistant thankfully thwarted.

The good news is that most of these issues are fixable, but timing matters. The longer your exposure sits out there, the more likely it is to be exploited or compromised.

If you’re looking to dig deeper, I recommend following up with a **SHADOW assessment** to investigate any active impersonation attempts or suspicious profiles that may already be live. If the exposure we found could be used for manipulation or fraud, the **SIGNAL assessment** can help you understand how your data might be exploited by social engineers or malicious actors. These follow-ups are especially important for public-facing professionals whose digital presence is actively monitored or targeted. Let’s discuss the next step that makes the most sense for your risk level.

If you’re ready, we can help you clean up what’s already out there and establish protections to prevent future exposure. That’s what the WATCHTOWER protection plans are built for — consistent oversight, ongoing scans, and real-time response if something new shows up. Let me know how you’d like to proceed.

Remediation Recommendations:

- Remove/privatize Amazon wish list and secure all social media privacy settings
- Contact LinkedIn and hosting registrar to report impersonation and spoof domains
- Initiate password hygiene overhaul using unique passwords and MFA across all platforms
- Consider SIGNAL or WATCHTOWER protection plans for monitoring and prevention

Ongoing Monitoring Options

Due to high public visibility and risk exposure, we recommend enrollment in IRONSWEEP's WATCHTOWER plan. This ensures quarterly monitoring, breach alerts, impersonation tracking, and incident response support tailored to executive profiles.

Recommended Follow-Up Assessments:

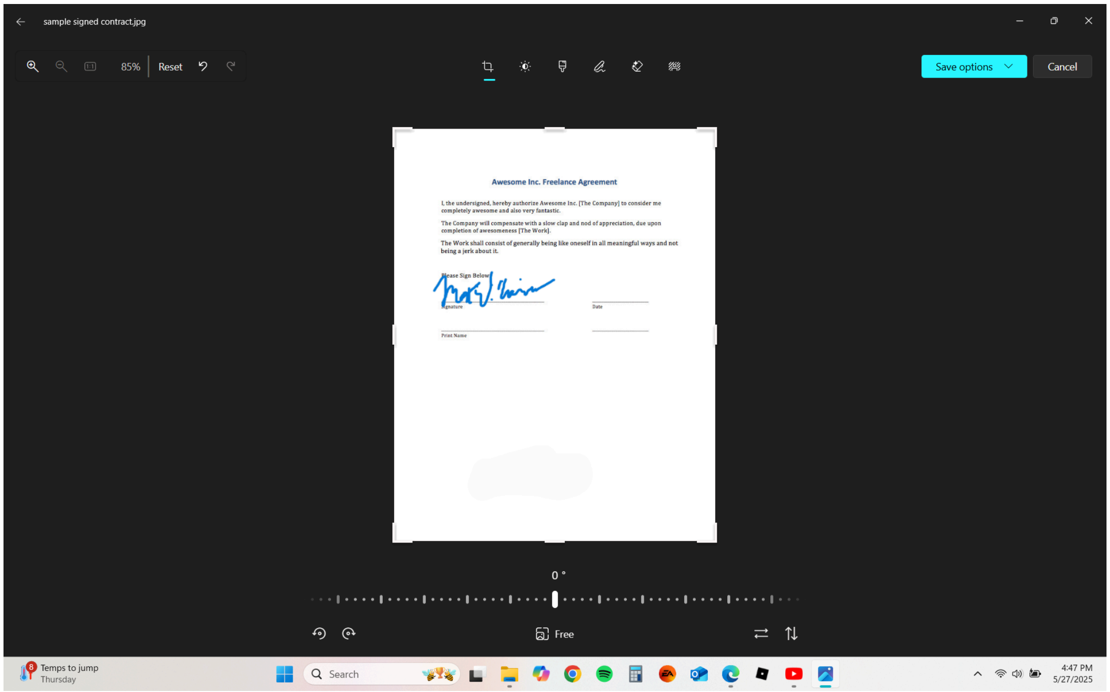
1. **SHADOW — Impersonation Risk Check**
   To investigate duplicate accounts, spoofed identities, or any unauthorized use of their likeness or name across platforms. Especially important if we find fake profiles, suspicious domain registrations, or misleading public content.

2. **SIGNAL — Human Attack Surface Assessment**
   To go deeper into how your online behavior, habits, and exposure patterns could be used in social engineering, fraud, or corporate espionage. This assessment connects the dots between scattered data and actual exploitability.

3. **COMMAND — Infrastructure & Domain Exposure**
   To delve into your business's digital presence, this assessment digs into email security, domain spoofing, exposed internal tools, admin panels, misconfigured subdomains, and public company records.

Appendices / Evidence Log

- Screenshot: Leaked PDF with ID and signature [Redacted]



Awesome Inc. Freelance Agreement

I, the undersigned, hereby authorize Awesome Inc. [The Company] to consider me completely awesome and also very fantastic.

The Company will compensate with a slow clap and nod of appreciation, due upon completion of awesomeness [The Work].

The Work shall consist of generally being like oneself in all meaningful ways and not being a jerk about it.

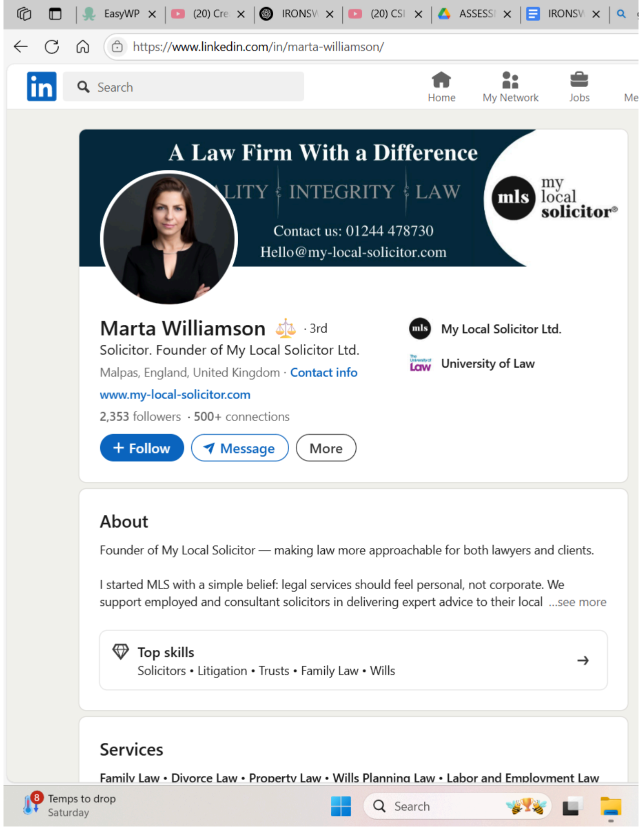
Please Sign Below

Signature

Date

Print Name

- Screenshot: Spoof LinkedIn profile



A Law Firm With a Difference

LITY | INTEGRITY | LAW

Contact us: 01244 478730
Hello@my-local-solicitor.com

mls my local solicitor®

Marta Williamson · 3rd
Solicitor. Founder of My Local Solicitor Ltd.
Malpas, England, United Kingdom · Contact info
www.my-local-solicitor.com
2,353 followers · 500+ connections

+ Follow | Message | More

My Local Solicitor Ltd.
University of Law

About

Founder of My Local Solicitor — making law more approachable for both lawyers and clients.

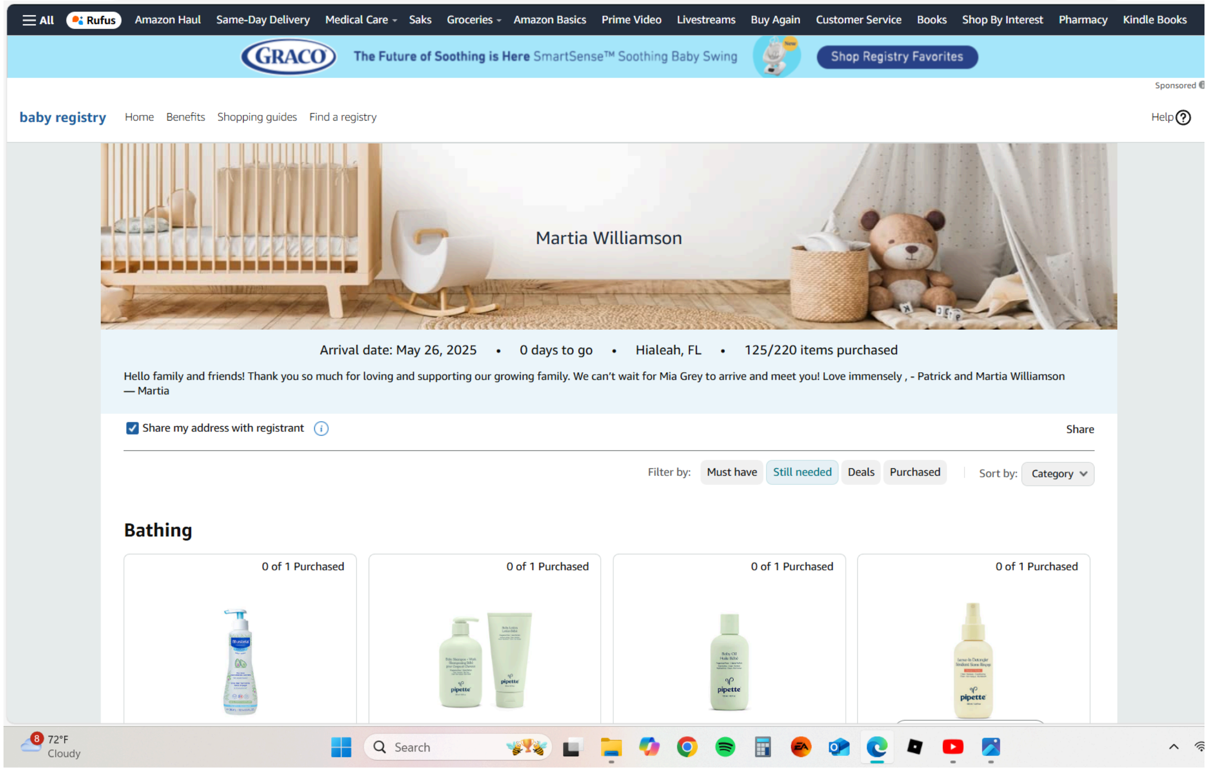
I started MLS with a simple belief: legal services should feel personal, not corporate. We support employed and consultant solicitors in delivering expert advice to their local ...see more

Top skills
Solicitors • Litigation • Trusts • Family Law • Wills

Services

Family Law • Divorce Law • Property Law • Wills Planning Law • Labor and Employment Law

- Screenshot: Amazon wishlist with identifiable items and recipient names



Martia Williamson

Arrival date: May 26, 2025 • 0 days to go • Hialeah, FL • 125/220 items purchased

Hello family and friends! Thank you so much for loving and supporting our growing family. We can't wait for Mia Grey to arrive and meet you! Love immensely , - Patrick and Martia Williamson
— Martia

☑ Share my address with registrant

Share

Filter by: Must have Still needed Deals Purchased

Sort by: Category

Bathing

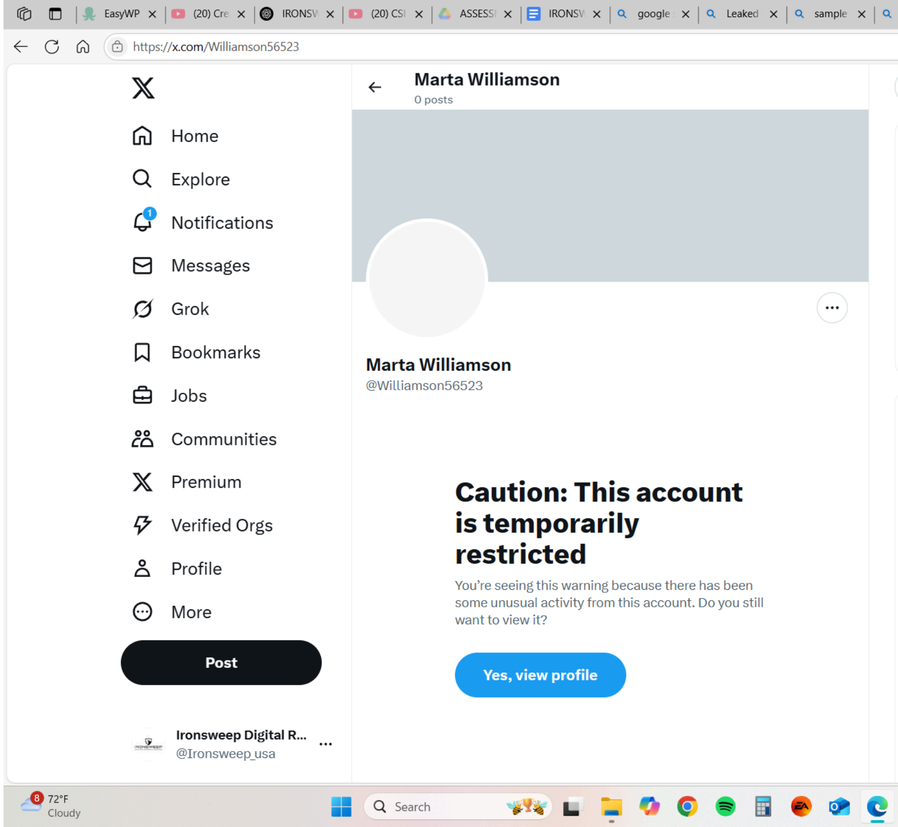
0 of 1 Purchased

0 of 1 Purchased

0 of 1 Purchased

0 of 1 Purchased

- Screenshot: Twitter like history [Archived Copy]



Marta Williamson
0 posts

Marta Williamson
@Williamson56523

Caution: This account is temporarily restricted

You're seeing this warning because there has been some unusual activity from this account. Do you still want to view it?

Kick it up a notch.

If this assessment left you with more questions than answers — or if you're concerned about what wasn't visible today but could surface tomorrow — your instincts are dead on. A one-time scan gives you a snapshot. But exposure evolves. Platforms change. New data breaches are discovered daily. That's why IRONSWEEP offers Watchtower Protection Plans — designed for individuals and teams who need more than a one-time look.

Our ongoing protection plans monitor your digital footprint on a rolling basis, flag emerging risks, and alert you to new breaches, impersonation attempts, or unwanted exposure before they escalate. You'll receive regular updates, expert guidance, and priority support if a threat emerges. If staying one step ahead matters to you — Watchtower is how you stay protected, not just informed.

☎

Phone Number

(client visibility only)

✉

Email Address

help@ironsweep.com

🌐

Website

www.ironsweep.com

IRONSWEEP
DIGITAL RISK INTELLIGENCE