



**TECHNOLOGY &  
CYBERSECURITY  
LAW GROUP**

October 27, 2017

*Submitted online*

**U.S. Federal Trade Commission**

Office of the Secretary  
Constitution Center,  
400 7th Street, S.W., 5th Floor  
Suite 5610 (Annex A)  
Washington, D.C. 20024

**RE: Informational Injury Workshop and P175413  
Comments on behalf of Client Lars Leifsson  
Comments of Technology & Cybersecurity Law Group, PLLC**

Honorable Commissioners and Staff of the Federal Trade Commission:

Thank you for the opportunity to comment upon privacy and data security issues to be covered by the U.S. Federal Trade Commission's ("FTC's" or "Commission's") Informational Injury Workshop, which is upcoming on December 12, 2017 ("Workshop"), and by the FTC's subsequent related activities, including regarding PrivacyCon 2018. The notice of the Workshop and the invitation for public comments is posted at the FTC's Web site at: <https://www.ftc.gov/news-events/events-calendar/2017/12/informational-injury-workshop>.

**About Technology & Cybersecurity Law Group and Its Privacy Work**

Since its inception in 2003, Technology & Cybersecurity Law Group ("TCLG") has served innovators in the technology sector and individuals and businesses impacted by technology. Among the most compelling matters as to which TCLG and its attorneys have represented are matters in which individuals are placed at risk and otherwise harmed due to privacy breaches and privacy erosions. Individuals are increasingly unable to maintain their personal information as securely private, within their sole control, and, to varying degrees, outside the marketplace that has commoditized their personal information and thus infringed upon the inviolable domains of their own personhood.

Among TCLG's privacy clients have been persons whose families have been held captive and prevented from leaving foreign countries to return to their homes in the United States; individuals who have been stalked, abused, or assaulted by their domestic partners; parents whose children have been at significant risk of international abduction; and others whose circumstances are similarly compelling. In these representations, TCLG and its attorneys have worked with other private counsel, elected officials, law enforcement agencies, victims' rights advocates, legal services

organizations, the Federal Bureau of Investigation, the U.S. Department of State, and other federal agencies.

### **Overview of Mr. Lars Leifsson and the Theft of His Identity and Harm**

Among TCLG's privacy clients for this FTC matter is Mr. Lars Leifsson, which is a pseudonym to protect his identity. Mr. Leifsson is a citizen of the United States and of Washington State. Mr. Leifsson was and continues to be a victim of crime, the initial and perpetuating crime being among the most egregious examples of identity theft that we have encountered in our practice to date or of which we are aware. Mr. Leifsson's experience and harm highlight, not only the unthinkable initial acts constituting identity theft, but also the misunderstanding and misuse of data in governmental agencies' database and systems within commercial data markets and contexts where there are few, if any, established rights or opportunities to know and to contest the information that is collected, used, transferred, and otherwise transacted.

The initial theft of Mr. Leifsson's personal information occurred in the early 1990s when a cousin, one Cody Safadago, allegedly stole Mr. Leifsson's birth certificate and illegally obtained and misappropriated Mr. Leifsson's Social Security number and information from Mr. Leifsson's driver's license. On information and belief, Mr. Safadago did so with the intent to commit identity theft. This intent, indeed, was born out and the identity theft that transpired and continues to this day has caused grave and multivariant harm to Mr. Leifsson and others in his family.

Since committing these crimes against Mr. Leifsson, Mr. Safadago has persisted unremittingly in his criminal career, which has ranged from California, Hawai'i, the Pacific Northwest, and even to other countries. Mr. Safadago's illegal activities began, records indicate, with domestic violence in 1992 at the age of twenty-two (22)<sup>1</sup> and continued with repeated drugs and weapons charges, abuse, felony theft, and other offenses; human trafficking in 2012; fleeing from parole and his resultant expulsion from Belize for return back to the United States<sup>2</sup>; and his 2015 arrest in Mexico for drug possession in quantities indicating his intent to distribute.<sup>3</sup> Mr. Safadago's nefarious career has culminated most recently at his April 2017 arrest for his vehicular killing of a teenage girl in Hawai'i while he was driving stolen vehicle and under the influence of alcohol and for other related crimes.<sup>4</sup>

---

<sup>1</sup> See *Hixon v. Safadago*, Case No. 92-2-14705-0 (King County Superior Court, filed Sept. 24, 1992).

<sup>2</sup> See Roland A. Parks, *U.S. Wanted Man Is Deemed Prohibited Immigrant to Belize*, AMANDALA (Mar. 4, 2014), <http://amandala.com.bz/news/u-s-wanted-man-deemed-prohibited-immigrant-belize/>.

<sup>3</sup> See, e.g., *Cae Norteamericano en Posesión de Droga* (North American Stopped for Drug Possession), EL VIGÍO (Mar. 12, 2015), <http://www.elvigia.net/066/2015/3/12/norteamericano-posesion-droga-190494.html>.

<sup>4</sup> See *Hawai'i v. Safadago*, Case No. 5CPC-17-0000172 (5th Cir. Crim. Ct., Lihu'e Div., filed May 10, 2017); *Man Arrested in Deadly Head-on Crash in Kauai Involving Stolen Truck*, KHON2 NEWS (updated May 1, 2017), <http://khon2.com/2017/04/28/man-arrested-in-deadly-head-on-crash-on-kauai-involving-stolen-truck/>.

Throughout his criminal activities, Mr. Safadago fraudulently has used Mr. Leifsson's personal information to establish and propagate an entire rank of false identities and aliases.<sup>5</sup> In addition to varying intermingling parts of his name with that of Mr. Leifsson, Mr. Safadago also used name and spelling variations to further confound law enforcement officials and others as to his identity, all of this at Mr. Leifsson's great expense. As he continued his criminal career and his interactions with law enforcement and the courts, Mr. Safadago's identity crimes against Mr. Leifsson thoroughly contaminated Mr. Leifsson's identity, as it was and is represented in data within numerous databases and systems.

We believe that Mr. Safadago has done committed the foregoing acts in his repeated attempts to evade law enforcement authorities and to otherwise evade detection, prosecution, or more adverse sentencing in view of his rich criminal record. As a result, Mr. Safadago's record is permeated with Mr. Leifsson's name, Social Security number, date of birth, and other indicia of Mr. Leifsson's identity.

Although Mr. Safadago's theft of Mr. Leifsson's personal information triggered the initial harm, we believe that it is the deceptive and unfair nature of data-related trade practices, including of law enforcement agencies that, as the remainder of this commentary illustrates, have so devastated Mr. Leifsson, his career, his employment, his health, his finances, and his professional, friendship, and familial relationships.

Some data trade practices, including of law enforcement agencies, may have an appropriately transparent, legally sufficiently disclosed, and legitimate basis for the collection, retention, propagation, transfer, aggregation, and analysis of and widely disseminated access to individuals' personal information. When identity theft occurs, however, irrespective of whether by data breach, cyber hack, online fraud, or an act such as by which Mr. Leifsson has been victimized, the harm propagates and amplifies through databases and systems that are devoid of appropriate checks and balances that one would expect for such sensitive and life-impacting information and that individuals require to enable their truly informed consents and to otherwise afford them essential consumer protections.

Further, the thus propagated and amplified harm persists with enduring and devastating effect. This is so because consumers may have little to no power or resources to obtain injunctive or other meaningful relief as to data practices and because practicable remedies are unknown, non-existent, extraordinarily difficult and expensive to effectuate, or any combination of the foregoing.

Where one wishes employment or even a consultative engagement, for example, one must submit to the background checks and other requirements of the subject employer and its agents, including, for example, outsourced recruitment and hiring firms, background check and similar investigative companies, and database providers. The FTC's unfairness doctrine would apply in such instances, as in Mr. Leifsson's case, where consumers cannot reasonably avoid submitting to background and other investigative checks as part of the required processes for seeking employment and where consumers have no established and known mechanism, except perhaps litigation, by which one can preempt or qualify negative background check findings due to data contaminated by identity theft

---

<sup>5</sup> See Identification & Criminal History Section, Washington State Patrol, *Conviction Criminal History Report 1* (Aug. 1, 2017) [hereinafter "Washington Rap Sheet"].

and other crimes. *See* FTC Act, Pub. L. No. 63-201, ch. 311, § 5, 38 Stat. 717 (1914)(codified as amended at 15 U.S.C. §§ 41-58 (2012)) (“FTC Act”); *id.* at § 5(n) (codified as amended at 15 U.S.C. § 45(n)).

For these reasons, Mr. Leifsson and surely others have experienced and continue to experience harm caused by data trade practices that are deceptive or unfair or both where those data practices work upon data which have been greatly compromised by identity theft; where consumers do not have any or adequate notice about the sources of data about them as are used in the background checking, immigration, law enforcement, and other processes; and where consumers lack the means and opportunity<sup>6</sup> to challenge those data and to remove, remediate, or even flag those data that are corrupted or otherwise compromised and therefore, not valid sources of data for the intended purposes as the demonstrable result, directly or indirectly, of identity theft.

### **More About Mr. Leifsson’s Experiences as an Identity Theft Victim**

Mr. Leifsson has suffered and continues to suffer significant harm as fall-out from the identity theft and, what is more damaging, the propagation, interchange, and retention of contaminated identity data in law enforcement, immigration, employment, background check and other investigative databases and systems.

#### **Mr. Leifsson’s Experience as to Law Enforcement**

To start, Mr. Leifsson wishes to state that he has many friends who serve within several different areas of law enforcement. He has and values greatly those deep and long-rooted friendships, and he deeply respects those law enforcement professionals.

The law enforcement and immigration or border control agencies with which Mr. Leifsson has dealt and as to which experienced harm as the result of the subject identity theft and the compounding and problematic data trade practices of same include, but are not limited to, the:

1. U.S. Federal Bureau of Investigation (“FBI”);
2. Washington State Patrol;
3. King County Sheriff’s Department;
4. Bellevue Police;
5. Seattle Police; and
6. Canada Border Services Agency, on information and belief, and others.

For example, Mr. Leifsson was stopped by police on two occasions for driving slightly over the posted speed limit. In one instance and despite his presentation of identity documentation, including a card issued to him by the relevant law enforcement authorities to demonstrate that his identity should not be confused with that of his physically distinct and criminal cousin, Mr. Leifsson and his vehicle were quickly surrounded by multiple police units. The police drew weapons upon Mr. Leifsson and pulled him out of the vehicle and onto the ground. They placed their boots upon his back and continued to hold drawn weapons upon him. He then was handcuffed and taken to jail. Mr. Leifsson’s clothing was taken, he was dressed in an orange jumpsuit, and he was

---

<sup>6</sup> Except as available under the Fair Credit Reporting Act. *See* 15 U.S.C. § 1681 *et seq.*

imprisoned in a holding cell with other alleged criminals, many of them aggressive and under the apparent influence of drugs. Mr. Leifsson was wrongly held in jail for some twelve (12) hours before the police freed him, having finally determined that he was not, in fact, Mr. Safadago. In the second instance, Mr. Leifsson was held in handcuffs in the back of the police car while officers sorted the matter, despite his having presented perhaps a dozen documents proving his identity.

#### Mr. Leifsson's Experience as to Border Control

Mr. Leifsson's experience in attempting an innocent family vacation by car to visit nearby Vancouver, British Columbia is likewise disheartening. At the Canadian border, Mr. Leifsson presented his identification documents to the Canadian immigration or border control officials. After checking those documents against their database(s) and system(s), the Canadian officials handcuffed and took Mr. Leifsson away from his family and detained him. The children were traumatized, as was Mr. Leifsson. The Canadian officials held Mr. Leifsson for several hours before permitting him and his party to enter the country with the strict, and atypical for an American tourist, instruction that if he did not return to the United States within twenty-four (24) hours, he would be arrested.

Those Canadian officials showed Mr. Leifsson an approximately seventy (70) page FBI dossier on him. Despite this, however, Mr. Leifsson has been unable to get any information, including as to existence of that dossier, by his Freedom of Information Act requests to the FBI or the U.S. Department of Justice.

The passage of surveillance and anti-terrorism laws post-9/11 is another driving force for information-sharing across law enforcement agencies and database or database access consolidations across state, local, federal, foreign, and international agencies. We do not dispute the public interest and national security needs for appropriate information-sharing nor do we express anything other than respect and appreciation for law enforcement professionals.

The harm to Mr. Leifsson and other victims of identity theft, however, is exponentially increased where there are insufficient controls and consumer protections on the commoditization and commercialization of and access to personal data from those law enforcement and immigration domains. The fact that cybercriminals, including state-sponsored actors, are constantly accumulating, interrelating, and transacting illegal business using individuals' personal information and highly granularized information about those individuals' social media and other activities means that personal data is now weaponizable and, as we have seen in the recent national election, weaponized. Even if those personal data were merely correct, imagine what harm does and may accrue to America consumers. Now imagine how much more harm consumers may experience, as has Mr. Leifsson, where those data are contaminated. Mr. Leifsson's experience in this regard in the employment domain provides an impactful example.

#### Mr. Leifsson's Experience as to Employment

Mr. Leifsson is a skilled management consultant and was formerly engaged in active productive work, as employee or a consultant, within the information technology sector. He has earned excellent references, including from multiple vice presidents within that sector, for his work, skills, and professionalism. Despite his experience, education, and excellent recommendations, however,

Mr. Leifsson has repeatedly been unable to secure employment in any position within that technology sector.

Even more overwhelming is the fact that Mr. Leifsson repeatedly has been unable to secure even unskilled employment, including at a local gas station or grocery store, due to background checks using contaminated data. These repeated denials of work opportunities have been only one of the great harms that Mr. Safadago's identity theft has precipitated, but in which insufficient consumer protections in the commercial data markets have greatly exacerbated.

Note that, examined without the contaminating effect for Mr. Safadago's identity theft crimes in commercial databases, Mr. Leifsson's own record is unsullied with only one minor traffic offense that occurred more than fourteen (14) years ago in 2003.<sup>7</sup>

In contrast to earlier times, successful background screening is now the norm for any job candidate for employment and consulting opportunities, and this is absolutely the case within the technology sector. The commercialization of and burgeoning market for individuals' personal information, the rapid rise in data mining, data analytics, data transfers, and artificial intelligence, and the outsourcing of recruitment- and hiring-related functions are seemingly irreversible trends in the American economy. These market forces and the trade practices that derive from those forces have greatly amplified and compounded Mr. Leifsson's victimization by his cousin's repeated acts of identity theft.

Among the companies with which Mr. Leifsson has dealt and as to positions with which he has experienced harm as the result of the subject identity theft and the problematic trade practices of same are the following, several of which were his former employers and for all of which he had favorable referrals and recommendations from high-ranking employees of the subject company:

<b>Sample Companies to Which Mr. Leifsson Has Applied</b>	<b>Previous Employer, Y/N?</b>	<b>High-Level Employee Referrals, Y/N?</b>
Company 1, one of the largest airlines in the United States	No	Yes
Company 2, a large online retailer	No	Yes
Company 3, one of the world's largest aerospace companies	No	Yes
Company 4, one of the world's largest information technology companies	Yes	Yes
Company 5, one of the world's largest online travel companies	No	Yes
Company 6, one of the world's largest software companies	Yes	Yes
Company 7, one of the largest retailers in the United States	Yes	Yes

---

<sup>7</sup> See Washington Rap Sheet, *supra* note 5, at 2.

Sample Companies to Which Mr. Leifsson Has Applied	Previous Employer, Y/N?	High-Level Employee Referrals, Y/N?
Company 8, one of the world's largest information technology companies	No	Yes
Company 9, one of the world's most well-known brands	No	Yes
Company 10, one of the world's largest telecommunications companies	No	Yes

Note that the companies referenced in the table, *supra*, are merely exemplars. Mr. Leifsson has applied for employment positions with dozens of other companies, many of them equally large and globally well-known. During the last ten (10) years and prevalently so since 2015, Mr. Leifsson has submitted numerous employment applications to these companies, those being for from three to six (3-6) positions per company. In all instances since 2015, Mr. Leifsson accompanied his applications with very positive recommendations from employees highly placed within all the companies with which he has applied.

In addition to his diligent efforts, Mr. Leifsson is a highly informed and skilled applicant. For example, he has invested in trainings to, among other optimizers, inform his high-level usage of key words in his resume with sufficient density of usage to maximize the possibility that automated systems will differentiate and select his resume for inclusion in the next steps of the recruitment and interviewing process. Mr. Leifsson has crafted a professional online presence, including with a top ranked LinkedIn profile. He also has suspended his use of Facebook or other “casual” or personal social media outlets during the times in which he was applying for jobs. He likewise has avoided triggering rejections by “over-applying.” Rather, he has limited his applications within a target company to no more than one or two very targeted positions at any given time. Further, Mr. Leifsson always has presented an accurate resume and limited his applications to positions for which he was qualified or well-qualified. In addition, he always has obtained and confirmed with each of his professional references their permissions for their names and contact information to be included in his application materials. He also has communicated with each of his references when applying so that each is aware of that submission and thus prepared to lend their strong support to his candidacy upon further inquiry by the human resources department or hiring manager.

Despite these valiant efforts, however, Mr. Leifsson began to observe that there were two (2) scenarios by which he was consistently being denied opportunities to interview for well- or even ideally-suited positions.

**Scenario 1: Online Submission of Resume**

1. Mr. Leifsson prepared and submitted his application for a position through the subject online job portal.
2. He received the automated confirmation that his application has been received.
3. Where Mr. Leifsson received any further response at all, he received an automated and consistent message (a) *within moments after* his receipt of the automated acknowledgement noted in Step 2, above, or (b) several months later, stating, in effect,

“Thank you, but no thank you. We are looking at other candidates who are a better match for the position.”

4. Otherwise, Mr. Leifsson received no response at all.

### **Scenario 2: Manually Submitted Resume**

1. Mr. Leifsson or the subject company’s employee who was recommending Mr. Leifsson for hire personally delivered Mr. Leifsson’s hard-copy application for the subject position to the human resources staff and the subject hiring manager, along with that employee’s letter of recommendation.
  - a. Typically, these recommending employees were director- or vice president-level employees who were hand delivering Mr. Leifsson’s application materials and providing their recommendations of his work and candidacy for the subject position.
2. Mr. Leifsson received an email or phone call from the Human Resources department regarding his interest in the position.
3. All the subject job positions then went into a “black hole,” as Mr. Leifsson describes it. Mr. Leifsson was advised that those positions were put on hold; or he never received any response from the company, despite his conscientious efforts in making multiple follow-up inquiries.
4. Further, the employees who had so glowingly recommended Mr. Leifsson suddenly did not return his phone calls or respond to his emails.

In some instances, Mr. Leifsson was informed that his background checks returned negative findings reflecting his cousin’s crimes and Mr. Leifsson’s thereby-contaminated personal data. In others, Mr. Leifsson was not informed of the results of those checks.

In addition, there is a pattern within the responses that Mr. Leifsson has received. The responses use the same language consistently during certain time periods and across companies suggesting that the legal and communications departments within these companies have been deeply involved with crafting these responses. In this way, the responses are akin to political talking points that one hears while watching a series of Sunday morning shows and then political coverages throughout the following week. There, the same talking points are repetitively used by each party and then others cycle through in subsequent. This pattern of responses suggests coordinated activity across the companies in rejecting Mr. Leifsson’s applications.

Something significantly untoward and possibly illegal seems to be occurring with respect to the hiring and employment screening processes within the technology sector, within the community of large employers in Mr. Leifsson’s local area, or both.

A further proof point suggests that this is even more definitively the case when comparing the results of Mr. Leifsson’s employment and application attempts within that sector and community with a trial background check undertaken for instant purposes in an entirely different sector and community, namely, in casino gambling.

At Mr. Leifsson’s request and expense, a friend who holds a senior position within a casino procured a background check on Mr. Leifsson as if Mr. Leifsson were applying for work at said casino. The casino gambling business is legally required to or follow hiring practices to include very stringent background checks to avoid, for example, hiring persons with a criminal background.

In this exemplar case, the casino used the service provider, HireRight, to carry out the most rigorous background check available on Mr. Leifsson. HireRight is known to carry out one of the more detailed background check processes, including its use of highly specialized and proprietary algorithm(s). See HireRight, Inc., <https://www.hireright.com/>.

The HireRight background check revealed absolutely nothing of concern in Mr. Leifsson's background, as seen in the HireRight results, below, which identify that no "discrepancy" was found. The results of the HireRight background check on Mr. Leifsson are, as follows.

- *Applicant's Personal Information*
- *Name: xxxxx xxxxxxx xxxxxxxxxx*
- *DOB: \*\*/ \*\*/ \*\*\*\**
- *Social Security Number: \*\*\*-\*\*-xxxx*
- *Results Summary*
- *Verification Status Discrepancy*
  - *SSN Validation Complete No*
  - *Court Records Complete No*
  - *Address History Complete No*
  - *National Sex Offender Registry Complete No*
  - *National Crim Search Complete No*

The results of the HireRight and, indeed any, background check is that those results are only as reliable and relevant to the intended purpose as the logic and requests that constitute the algorithm(s) used to execute and analyze the subject query(ies); the data elements involved in these searches and analyses; the sources of those data; and the relationships between and among the foregoing. The origin, providence, interchange, filtering and other processing, and custody of each data set and the consumption and context for each vary. Without clarity around each of those characteristics and, importantly, disclosure of and the informed consent of the consumers whose data these are and whom they regard, uneducated use, inadvertent misuse, and weaponized use of these data may result in scenarios, such as experienced by Mr. Leifsson, that harm consumers greatly and in a varied and intransigently persistent manner.

The pristine non-findings from the HireRight background check contrast starkly with results of Mr. Leifsson's other background check failures and with his repeatedly and otherwise inexplicably unsuccessful employment search efforts.

Therefore, we have reason to believe that there may exist a "black list" or a "Do Not Hire" list among technology or technology-enabled companies or among large companies in Mr. Leifsson's local market. Further, we believe that any such black list or Do Not Hire list may be derived, in whole or part, from Mr. Leifsson's personal data as contaminated by the identity theft.

Technology & Cybersecurity Law Group are currently investigating and gathering additional evidence by which Mr. Leifsson may see relief in Washington, including, but not limited to, under that state's black listing statute, Wash. Rev. Code § 49.44.010, under which he has a private right of action. See *Banks v. Yoke's Foods, Inc.*, No. 2:14-CV-0319-TOR, 2014 WL 7177856, at \*8 (E.D. Wash. Dec. 16, 2014).

In devastating effect, therefore, we suggest that Mr. Leifsson is a victim of weaponized and contaminated personal data. Although the initially triggering event was the theft of Mr. Leifsson's identity and personal information, the weaponization of the theft-contaminated data has occurred and continues unabated by its unremitting and almost viral propagation across databases and systems for a significant period of time.

In this way, Mr. Leifsson's experience is a cautionary tale of the most profound nature. Others have had their personal information stolen by state-sponsored actors, independent hackers, and other criminals and by data exposures and breaches, including those occurring due to failures to follow reasonable security measures. We predict that all victims of identity theft, data privacy failures, and deceptive and unfair data trade practices are at risk of similar informational injuries, harms, and fates.

Deceptive and unfair trade practices worsen and escalate the initial injuries by obfuscating which of consumers' data are collected, transferred, sold, retained, and leveraged across the law enforcement and other government databases and systems and then the commercial data market ecosystem. In this wild west of commoditized and inadequately protective data market, acts of cyberwar, ransomware attacks, and other malicious acts have weaponized and will continue to weaponize those victimized consumers' data with devastating and sustained harm to them.

### **Types of Harm Experienced by Mr. Leifsson Due to His Informational Injuries**

Following are short summaries of the types of harm that Mr. Leifsson has suffered. He stands ready and willing to provide more detailed information about these harms and to speak and testify before the Commission and others in full on these matters.

#### 1. Constitutional harm.

For fear of again being handcuffed and detained or worse at border crossings or even traveling across state boundaries, Mr. Leifsson has been injured by the resultant infringement of his constitutional right to freedom of movement under the U.S. Constitution's Privileges and Immunities clause. His rights to be protected against unlawful search and seizure under the Fourth Amendment rights also have been infringed.

#### 2. Employment harm.

Mr. Leifsson's employment and employment opportunities have been severely damaged. He is in a terrible quandary. He is rejected from employment if he proactively discloses to potential employers that his background checks may be flagged due to the crime-contaminated data within the subject databases and systems. He is likewise rejected if he does not provide that advance disclosure and negative background checks or black lists come into play. For Mr. Leifsson, the current state of affairs means that he may never win the opportunity to demonstrate his great value as an employee and a creative, hard-working, and high-performing contributor, a fact of which we speak from direct experience.

#### 3. Career harm.

Mr. Leifsson's career is in shambles as the result of his repeated and continuing informational injuries. With each employment defeat, his career growth and trajectory are further diminished.

4. Financial harm.

Mr. Leifsson estimates that the net present value of his damages from information injuries, including his lost wages, property, investments, and the like, is about \$10 million to date. Where his family members, primarily his mother, have invested in him and attempted to help him out of the financial chaos, the net present value of that harm is approximately \$1 million to date.

The identify theft, as exacerbated by the data contamination and commoditization issues referenced above, forced Mr. Leifsson to sell his real properties and cash out his retirement savings to survive, imposed capital gains taxes and penalties upon him, created a large tax amount due to the Internal Revenue Service, and imposed upon his mother, who supported him with paying majority of these liabilities.

5. Housing harm.

Prior to the escalating effects of his informational injury, Mr. Leifsson had worked hard, saved frugally, and invested wisely. He owned two real properties before the age of thirty (30).

He was also on track to purchase a retirement home in a modestly affordable location. That important long-term goal toward which he was working so diligently has vanished. That goal, however, is now a complete impossibility because, due to his financial harms, including foreclosure, he can no longer obtain financing with which to purchase a home or any other property.

In his current state of being unable to secure employment, Mr. Leifsson lives tenuously with the support of his family and is in constant danger of losing his residence.

6. Emotional harm.

Mr. Leifsson is a very strong individual, yet still very fragile in that he cares deeply about making others happy and doing his best. The fact that many family members, especially his mother, did not understand or believe him, as some in his family still do not, has crushed him emotionally. For many years, Mr. Leifsson felt that, because his family members did not believe him or understand the gravity of his informational injuries, there was little joy left in life and that he was merely getting through and surviving by investing in his further education and other topics for growth in the hope that, someday, at least some of his family members who eventually understand that, in fact, the identity theft had occurred and precipitated vast harm upon him.

7. Physical harm.

As discussed above, Mr. Leifsson has been physically restrained, handled, threatened, and imprisoned by law enforcement officials. He has been physically restrained and detained by border control officers. In addition, he has experienced physical manifestations associated with the severe stress and emotional distress caused by his informational injuries.

8. Psychological harm.

Mr. Leifsson believed that there would be no end to his psychological suffering until his cousin was apprehended and imprisoned. That psychic pain continues because, despite his cousin's current incarceration in Hawai'i, Mr. Leifsson learned that law enforcement databases would retain his contaminated personal information for ninety-nine (99) years, even if Mr. Safadago is imprisoned for

life or dies. Feeling that, despite his victimization, he had disappointed his beloved mother, further harmed Mr. Leifsson. Honor and personal integrity are important to Mr. Leifsson, and the feeling that he will never be able to clear his good name is also particularly painful.

Mr. Leifsson has a sense of living in the shadows. He feels exposed to the persistent threat to his well-being, freedom, and safety when he must venture forth in his car for fear he will again be wrongfully arrested and threatened with guns and other physical harm. He feels the constant stress associated with his fight to retain his residence due to his limited ability to secure work for which he is ably qualified or otherwise.

#### 9. Reputational harm

Mr. Leifsson's professional reputation is undeservedly in tatters. Despite repeated successes in his past employment and numerous well-deserved recommendations, he now experiences utter silence and non-responsiveness from those recommenders and others.

#### 10. Harm to familial relationships and friendships.

Among the most unfortunate personal tragedies arising from the foregoing, many of Mr. Leifsson's family members and friends did not believe him when he tried to share his experiences and harms precipitated by Mr. Safadago's criminal conduct and Mr. Leifsson's resultant informational injuries. The alienation and loss of consortia that Mr. Leifsson has experienced has been deeply corrosive and devastating.

As illustrated here, the informational injuries suffered by identity theft victims and exacerbated by deceptive and unfair data trade practices are multitudinously varying in type and intensely damaging,

### **Possible Legislative Models and Solutions for Identity Theft Victims**

Within the confines of their financial and time resources, victims of identity theft, including by proliferation of theft-contaminated data, can pursue private litigation in the attempt to seek relief for the great harm that they have endured and continue to endure. For most, such litigation is not an option. Further, litigation may not produce a remedy to purge or correct contaminated data and disassociate such data from other databases and systems.

The express right of private action is essential to victims of identity theft, however. The Commission and, similarly, state attorneys general have limited resources and, therefore, must prioritize their litigation activities to focus often on the largest scale or more systematically egregious perpetrators and fraudulent schemes. Consequently, without the right of private action, individual victims may be powerless to obtain any meaningful relief. To each victim of identity theft, the harms are pervasive and all-consuming. Therefore, it is critically important that all individual victims of identity theft have the clearly-established right of private action against those who perpetuate their victimization and, actually and in effect, weaponize contaminated data against them.

In addition to legislative action to establish a clear right of private action, new data protection legislation may further help victims of identity theft, such as Mr. Leifsson, to seek have recourse to seek remediation of corrupted personal data held in corporate and law enforcement databases. The Fair Credit Reporting Act provides a useful and analogous model. *See* 15 U.S.C. § 1681 *et seq.* Similarly-structured legislation dealing with individuals' personal data and data about those persons

(collectively, in this discussion, “their data” or “personal data”) would provide a means for individuals to, among other things:

1. Know the database names and other identifiers and locations where their data are stored and the companies under the control of which their data lie and have lain;
2. Examine all those data and the providence of same;
3. Examine all the collection, retention, association, sale, license, interchange, and other transactions (collectively, in this discussion, “data activities”) that are occurring and have occurred involving any of their data;
4. Examine all the instruments by which the subject individual purported consented to each data activity involving any of their data;
5. Examine a complete historical record and current statement as to all parties and third parties involved in each data activity involving their data;
6. Withdraw their consent as to any or all the data activities as to their data;
7. With some objective means of validation, notify the custodians of those data of errors or other data contamination; and
8. Establish a means within a thirty (30) day or similarly short time period for the custodian to remediate or remove erroneous or contaminated data or data associations.

Other protections from which the credit industry could also protect useful legislative models. For example, when consumers seek to make car or other purchases using credit, they are asked to authorize the merchant to obtain a credit report. The consumers are also entitled to receive a letter notifying them of any denials of credit based upon that information and then to request further information as to specific reasons underlying the denials.

As to the transparency by which individual can know the ways in which their data are used and to withdraw their consent to specific or all uses, the Health Insurance Portability and Accountability Act, or HIPAA, and related laws provide a collectively useful model. *See generally* Pub. L. 104-191, 110 Stat. 1936.

The Digital Millennium Copyright Act also provides a useful model for enable consumers to manage their data. Particularly, the DMCA requires notices to be place on Web sites and, importantly, the permanent identification there of a single point of contact by which individuals can communicate regarding possible copyright infringements. In the instant context, similar helpful legislation could establish requirement for easily accessible notices and for the permanent identification of a single point of contact by which victims of identity theft and other consumers could communicate as to possible data errors and contamination in the subject database or system. *See* 17 USCS § 1201 *et seq.*

In conclusion, the Federal Trade Commission has powerful legal authority to protect consumers against deceptive and unfair data trade practices under Section 5 of the FTC Act. We further assert, however, that further legislative action is needed to contemplate and reflect the cross-domain commercialization and commoditization of consumers’ personal data and other indicia of their identities. Such legislation must provide for meaningful and accessible systems by which consumers may know in all aspects their data and appropriately control same; be enabled to provide truly

**Technology & Cybersecurity Law Group**

Public Comment to the FTC: Informational Injury Workshop and P175413

October 27, 2017

Page 14 of 14

---

informed consent, where they wish to do so; efficiently and effectively achieve corrections to erroneous or otherwise contaminated data; and have a private right of action to supplement governmental efforts to protect them.

Thank you for your careful consideration of these public comments of Mr. Lars Leifsson and of Technology & Cybersecurity Law Group, PLLC and for the Commission's continued work to protect American consumers.

Respectfully submitted,

/s/

Emile Loza de Siles

Counsel to Mr. Lars Leifsson

Founder & Chief Technology Counsel

Technology & Cybersecurity Law Group, PLLC