(Rev. 7.30.2020)

ATTORNEY GRIEVANCE COMMITTEE
Supreme Court, Appellate Division
First Judicial Department
180 Maiden Lane, 17th Floor
New York, New York 10038
(212) 401-0800

JORGE DOPICO
Chief Attorney

Email Complaint and Attachments to: AD1-AGC-newcomplaints@nycourts.gov. In addition, please send **one copy** of your complaint and attachments **by regular mail** to the above address. (If you do not have a personal email account, please send two (2) complete sets of your complaint and all attachments. There may be a delay in processing your matter if it is not emailed. Please **do not** include any original documents because we are unable to return them.)

Background Information

Today's Date: November 22, 2026

Your Full Name: (Mr. Ms. Mrs.) Mr. Jason Thompson

Address: [redacted]

City: [redacted] State: [redacted] Zip Code: [redacted]

Cell Phone: [redacted] Business/Home Phone:

Email Address: [redacted]

Are you represented by a lawyer regarding this complaint? Yes ☐ No ☑ If Yes:

Lawyer's Name:

Address:

City: State: Zip Code:

Business Phone: Cell Phone:

Attorney Information

Full Name of Attorney Complained of: (Mr. Ms. Mrs.) Mr. Michael D. Margulies

Address: [redacted]

City: [redacted] State: [redacted] Zip Code: [redacted]

Business Phone: [redacted] Cell Phone:

Email Address: [redacted]

Date(s) of Representation/Incident: October 30 through November 19, 2026

Have you filed a civil or criminal complaint against this attorney? Yes ☐ No ☑ If Yes:

If yes, name of case (if applicable):

Name of Court:

Index Number of Case (if known):

Have you filed a complaint concerning this matter with another Grievance Committee, Bar Association, District Attorney's Office, or any other agency? Yes ☐ No ☑

If yes, name of agency:

Action taken by agency, if any:

Details of Complaint

Please describe the alleged misconduct in as much detail as possible including what happened, where and when, the names of any witnesses, what was said, and in what tone of voice, etc. Use additional sheets if necessary.

On October 30, 2026, Michael D. Margulies transmitted SecurityScorecard's demand for arbitration against me and Factor Cybersecurity, Inc. I allege he violated Rule 3.1 by pursuing arbitration when neither of us had agreed to arbitrate these claims. Section 21 of the May 2023 contractor agreement superseded my 2017 agreement. I never signed the later standard form. Factor never agreed to arbitrate. Yet SSC sought to stay our Delaware lawsuit, and its attorney Michael L. Yaeger submitted the unsigned 2023 form as Exhibit E, arguing that my offer letter incorporated it. I allege that forcing us to defend a second proceeding increased our costs and served to harass us.

On November 19, Margulies invoked that same proceeding in letters sent directly to [EMPLOYEE B], Factor's VP of Growth, and [ADVISOR A], its strategic advisor. Factor counsel Charles Brown represented [EMPLOYEE B] in this matter. Margulies copied Brown. To my knowledge he never consulted Brown or obtained consent. I allege improper direct contact under Rule 4.2.

Both letters repeated allegations of unauthorized use of SSC intellectual property, bad faith and breach of fiduciary duty. I consider their circulation defamatory. They directed recipients to notify personnel, coordinate with IT and acknowledge receipt by December 4. [ADVISOR A] had joined only days earlier, yet his letter reached back to January 1, 2017.

I allege Yampolskiy has stalked me since July 2025. Factor advisor [ADVISOR B] led the BitSight investigation that identified the Emma Mason account I allege Yampolskiy used to take BitSight intellectual property. Around July 12, 2026, [ADVISOR B] relayed Yampolskiy's warning that he planned to subpoena Factor advisors and that [ADVISOR B] should reconsider serving. Wilton Manors Police documented my July 13 report of client contacts. Delaware State Police documented my August 19 request for stalking charges. On November 5, I reported witness pressure to FBI Boston. On November 16, after speaking with the FBI about the BitSight matter, I sent updated evidence. Three days later Margulies sent the letters. I ask the Committee to investigate his participation in the alleged intimidation. See Exhibits A-K.

Complainant's Signature (Required):

Exhibit K | The allegedly baseless arbitration demand

Why the proceeding matters to the November 19 contacts

Margulies opened both letters by identifying SSC as counsel's client in a proceeding against me and Factor. That caption tracks SSC's October 30 arbitration demand, AAA No. 01-26-0006-3102. I contend the demand was unlawful because no enforceable arbitration agreement covers these claims against either me or Factor. I never signed the 2023 agreement, and Factor never agreed to arbitrate. I signed a 2017 agreement during an earlier period of employment. My position is that the later contractor agreement superseded it and provided for a court forum.

What SSC's counsel submitted in Delaware

SSC moved to stay the Delaware case pending arbitration. In the declaration supporting that motion, Michael L. Yaeger identified Exhibit B as my signed 2017 agreement, Exhibit C as the 2023 contractor agreement, Exhibit D as the June 2023 offer letter and Exhibit E as SSC's standard 2023 agreement. He asserted that the offer incorporated Exhibit E by reference. SSC thus submitted an unsigned form to support its claim that I assented to arbitration. The offer letter said I would be required to sign a separate form. I dispute that accepting employment established consent to its arbitration clause. Yaeger also submitted the arbitration demand as Exhibit L. Source: D. Del. No. 1:26-cv-01119, D.I. 13–15, Yaeger declaration ¶¶ 4–7, 14.

Defense costs and harassment of Factor personnel

I allege that pursuing me and Factor in a second forum increased our defense costs and that invoking that proceeding in letters sent to a represented executive and a newly appointed advisor extended the harassment to my staff and advisors. Counsel had a route through Brown. Instead, the letters put SSC's accusations and demands for action directly before the people whose cooperation Factor relies on. On November 5, before these letters arrived, I had already reported to FBI Boston my concern that mounting legal expense was being used to impede cooperation (Exhibit J).

Stalking and law-enforcement involvement since July 2025

I allege that Yampolskiy has stalked me since July 2025, beginning with the period when I reported his threat to shoot me and continuing through contacts with people associated with Factor. Wilton Manors Police recorded my July 13, 2026 report of contacts with clients. Delaware State Police recorded my August 19, 2026 request for stalking charges. In November, FBI Boston followed up on my report concerning the alleged BitSight access, and I reported pressure on witnesses to the same office. Exhibits F through J document the threats, police reports, civil allegations and FBI correspondence.

Exhibit K | Why the arbitration demand implicates Rule 3.1

The agreements counsel had when the demand was made

Section 21 of the May 17, 2023 contractor agreement supersedes all pre-existing written or oral agreements between its parties. Section 20 selects the state and federal courts in New York County for disputes arising from or relating to that contractor agreement. I contend section 21 displaced the 2017 arbitration agreement from my earlier employment. I did not sign the later standard form. Factor did not sign the 2017 agreement or the later form. The attached contract page sets out sections 20 and 21 together.

What Margulies knew and did

On October 30 Margulies transmitted SSC's demand against both me and Factor. SSC's own demand, printed pages 22–23, recites my supersession objection and disputes it. SSC argued that the June offer letter and later MAX bonus letter incorporated or reaffirmed the standard employment terms. My position is that the offer contemplated a future signature and that neither letter supplied the missing assent to arbitrate these claims. The federal declaration identified the 2023 exhibit as a standard form. My objection concerns counsel's asserted basis for enforcing it.

Why I allege professional misconduct

New York Rule 3.1(a) requires a nonfrivolous basis in law and fact to bring a proceeding or assert a position. Rule 3.1(b)(2) specifically reaches conduct serving merely to harass or maliciously injure. Delaware Lawyers' Rule 3.1 and ABA Model Rule 3.1 likewise require a nonfrivolous legal and factual basis. District of Delaware Local Rule 83.6(d) adopts the Model Rules for practice before that court.

Application to the demand and the November letters

I allege Margulies pursued arbitration without a good-faith basis for binding either respondent after supersession. He sought acceptance of service in a second forum, and SSC used the demand to seek a stay of our Delaware suit. Margulies then invoked that proceeding when he contacted my VP and advisor directly. Those steps increased our defense costs and put demands on Factor personnel. Their sequence, together with counsel's possession of the superseding agreement and unsigned form, is the basis of my allegation that the proceeding was used to harass us in violation of Rule 3.1.

WHETHER BASED IN CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHER THEORY OF LIABILITY, REGARDLESS OF WHETHER COMPANY WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND NOTWITHSTANDING THE FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY. IN NO EVENT SHALL COMPANY'S LIABILITY ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT EXCEED THE AMOUNTS PAID BY COMPANY TO CONTRACTOR UNDER THIS AGREEMENT FOR THE SERVICES, DELIVERABLES OR INVENTIONS GIVING RISE TO SUCH LIABILITY.

14) Reimbursement of Expenses. Contractor shall not be authorized to incur on behalf of the Company any expenses and will be responsible for all expenses incurred while performing the Services, except as specified in this Agreement or the applicable Statement of Work or otherwise agreed to by the Company, which consent shall be evidenced in writing. As a condition of reimbursement of any expenses, Contractor shall be required to submit to the Company reasonable evidence that the amount involved was both reasonable and necessary to the Services provided under this Agreement and any other documentation requested by the Company.

15) Independent Contractor. The parties acknowledge that this Agreement does not create an employment relationship nor partnership nor joint venture but only that of independent contractors. As a consequence, (i) Contractor shall have no authority to enter into contracts or agreements on behalf of the Company, (ii) all taxes that might be due and payable as a result of this Agreement by Contractor in whatever jurisdiction shall be the sole responsibility of Contractor, and (iii) Contractor will not be covered by the Company's workers compensation insurance or eligible for any Company benefits, including the Company's pension, health or other fringe benefit program, and, to the extent Contractor otherwise would be eligible for any Company employee benefits but for the express terms of this Agreement, Contractor (on behalf of itself and its employees) hereby expressly declines to participate in such Company employee benefits.

16) Insurance. During the term of this Agreement, you shall maintain in force adequate workers' compensation, commercial general liability, errors and omissions, and other forms of insurance, in each case with insurers reasonably acceptable to the Company, with policy limits sufficient to protect and indemnify the Company and its affiliates, and each of their officers, directors, agents, employees, subsidiaries, partners, members, controlling persons, and successors and assigns, from any losses resulting from your acts or omissions or the acts or omissions of your agents, contractors, servants, or employees. Consultant shall provide proof of coverage upon request.

17) Background Check: This contractor engagement is conditioned on successful completion of a background check. Please note that by signing this agreement and the attached FCRA Authorization Form, you grant approval to initiate this background check.

18) Notices. Any notice given in connection with this Agreement shall be given in writing and shall be delivered by either overnight mail, or regular mail, return receipt requested, to the parties as stated in the addresses below the signature block.

19) Successors and Assigns. Except as otherwise provided in this Agreement, this Agreement, and the rights and obligations of the parties hereunder, will be binding upon and inure to the benefit of their respective successors, assigns, heirs, executors, administrators and legal representatives. The Company may assign any of its rights and obligations under this Agreement. No other party to this Agreement may assign, whether voluntarily or by operation of law, any of its rights and obligations under this Agreement, except with the prior written consent of the Company.

20) Governing Law; Consent to Personal Jurisdiction. This Agreement will be governed by and construed in accordance with the laws of the State of New York without giving effect to the choice of law provisions thereof. Contractor hereby expressly consents to the personal jurisdiction and exclusive venue of the state and federal courts located in New York County for any dispute arising from or relating to this Agreement.

21) Entire Agreement. The parties acknowledge that this document represents the entire Agreement between the parties and supersedes any and all pre-existing agreement, written or oral, between the parties.

22) Severability. If any provision of this Agreement shall be held to be invalid under applicable law, the parties agree to renegotiate such provision in good faith. In the event that the parties cannot reach a mutually agreeable and enforceable replacement for such provision, then (i) such provision shall be excluded from this Agreement, (ii) the balance of the Agreement shall be

Statement of Jason Thompson

Conduct for investigation

I am proceeding pro se in this grievance. Charles Brown represented Factor and me in the underlying dispute. On November 19, Michael D. Margulies emailed two people on Factor's leadership team. He addressed each individually and copied Brown. I report that Brown was never consulted.

What Margulies asked each recipient to do

In Exhibit A he identified [EMPLOYEE B] as "Co-Founder and Vice President of Growth for Factor." In Exhibit B he identified [ADVISOR A] as "a Strategic Advisor to Factor." Each letter covered records from January 1, 2017 forward, including subsequently created records. Each asked the recipient to "notify any of your personnel reasonably likely to hold relevant records" and "coordinate with appropriate IT personnel or service providers." Each requested acknowledgment by December 4 and the identity of a contact. The letters expressly limited the request to preservation and disclaimed production or waiver. They invited discussion "through your counsel if appropriate." My complaint concerns the direct instructions and return communications sought from people identified by their roles at Factor.

The accusations circulated to the two recipients

Both letters described a dispute involving alleged breaches and identified "unauthorized use of SSC's intellectual property, bad faith, and breach of fiduciary duty." I deny the underlying misconduct. I consider the circulation of these accusations to people on whose professional trust Factor depends defamatory. The attached Delaware pleading sets out our denial, including our allegation that I lacked access to SSC source code.

Why the recipients matter under Rule 4.2

Factor counsel represented [EMPLOYEE B] in this matter. Margulies identified him as a Factor executive and asked him to direct personnel and coordinate with IT. As to [ADVISOR A], the letter establishes his advisory role. Rule 4.2 coverage turns on his representation or his responsibilities for Factor in this matter.

Applicable rules of professional conduct

New York

New York Rule 4.2(a) governs a lawyer communicating about a matter with a party known to be represented in it. It requires prior consent from the other lawyer or legal authorization. Comment [7] addresses organizational constituents. Rule 4.2(b) addresses client-to-party communications. Exhibits A and B are letters from counsel himself.

Delaware and the pending federal proceeding

Delaware Lawyers' Rule 4.2 and comment [7] address direct contact with a represented person and covered organizational constituents, subject to consent or authorization by law or court order. The underlying federal case is Factor Cybersecurity, Inc. et al. v. SecurityScorecard, Inc. et al., D. Del. No. 1:26-cv-01119. District of Delaware Local Rule 83.6(d) adopts the ABA Model Rules for lawyers admitted or authorized before that court, subject to federal modifications. ABA Model Rule 4.2 and comment [7] supply the federal counterpart.

Related questions of truthfulness and burden

I request review under New York and Delaware Rules 4.1 and 8.4(c) if evidence establishes a knowingly false representation or dishonesty by counsel. Delaware Rule 4.1(a) requires materiality. I allege that directing these demands to the recipients personally served no substantial purpose beyond intimidation and burdened them within the meaning of Rule 4.4(a). The preservation purpose stated in the letters bears directly on that inquiry. Earlier conduct by Yampolskiy explains why I experienced the letters as pressure. I attribute the November letters to the lawyer who signed them.

The July warning and the November letters

In July, [ADVISOR B] relayed Yampolskiy's warning that he would subpoena Factor's advisors and that [ADVISOR B] might want to leave (Exhibit E). On November 19, the two people Margulies contacted included a represented VP and an advisor who had joined only days earlier. I know of no basis for asking [ADVISOR A] to preserve records dating to 2017. Exhibit B identifies only his new advisory role. I allege these contacts were intended purely to intimidate.

Authorities

New York Rules of Professional Conduct, 22 NYCRR Part 1200, Rules 3.1, 4.1, 4.2, 4.4, 8.4, 8.5. Delaware Lawyers' Rules of Professional Conduct, same rule numbers. U.S. District Court for the District of Delaware, Local Rules of Civil Practice and Procedure, effective September 1, 2026, Rule 83.6(d). ABA Model Rules 3.1 and 4.2.

Prior contacts, threats and reports

[EMPLOYEE B] and [ADVISOR A] | Exhibits C and D

My witness statement dates Yampolskiy's LinkedIn comment on [EMPLOYEE B]'s page to approximately December 18, 2025. The comment urged partnering with "higher-quality companies (than Factor)." On Cobalt AI's June 18, 2026 announcement of [ADVISOR A] as CTO, Yampolskiy urged Cobalt to coach its CTO not to "send retarded messages to Executives on Linkedin." The full image shows both the appointment and his words. [ADVISOR A] publicly responded on Sunday evening, June 28, 2026 (Eastern time), placing the apparent comment date on or about June 28. The supported posting range is June 18–28.

[ADVISOR B] | Exhibit E

In October 2025, I alerted [ADVISOR B] to suspicious access through a furniture-company account. [ADVISOR B] led BitSight's incident response. His team identified the Emma Mason account, disabled it, and reported that the unauthorized access ceased. My witness account also identifies former SecurityScorecard CTO Christos Kalantzis as having confirmed to [ADVISOR B] that Yampolskiy had accessed BitSight and taken its data and intellectual property. On or about July 12, 2026, [ADVISOR B], by then a Factor advisor, relayed Yampolskiy's message: "I plan to subpoena all the advisors soon" and "So you probably don't want to be on it." The unredacted exchange includes the theft accusation and reference to my child-protection report. [ADVISOR B] said the message arrived the previous day around noon. My witness statement dates the message to approximately July 12.

Threats to me and to Josh Fazio | Exhibit F

I reported that on July 2, 2025, Yampolskiy threatened to take me outside and shoot me. My statement gives his words as "Take you out back and shoot you like a dog." I raised the threat in writing that evening. Josh Fazio served in Illinois law enforcement and later worked as a SecurityScorecard sales-engineering executive. He helped me investigate Yampolskiy by providing information about suspected unauthorized access to BitSight. The August 10 letter identifies him as a witness to that access. Fazio described a blocked, voice-masked call his wife witnessed: "If you help Jason Thompson, we will kill you." The meeting summary records his attribution to Yampolskiy and labels Fazio [redacted] my caption explains the error. It dates the call to Saturday, July 18, consistent with 2026. Counsel's August 10, 2026 letter instead gives July 2025 and requests phone records to identify the caller.

Florida and Delaware | Exhibits G, H and I

Wilton Manors Police report 43-2607-008675 records my July 13, 2026 report about LinkedIn contacts and allegations made to clients. The officer's narrative (packet p. 25) incorrectly identifies Yampolskiy as "owner of Factor Cyber Security." Yampolskiy was CEO of SecurityScorecard, my former employer. Factor Cybersecurity, Inc. is a separate Delaware C corporation. I am one of its shareholders. The report classified the incident as information and marked it inactive. Delaware State Police report 07-26-056846 records my August 19 request for stalking charges; the August 25 report records insufficient evidence to identify the caller or establish probable cause. The September 3 Delaware federal complaint describes alleged intimidation and interference, including the advisor warning and LinkedIn comment. A separately filed Florida stalking petition or order has not been verified for this submission.

CARLTON FIELDS

ATTORNEYS AT LAW

[redacted]

Atlanta
Hartford
Los Angeles
Miami
New York
New Jersey
Orlando
Tallahassee
Tampa
Washington, DC
West Palm Beach

Michael Margulies
Shareholder
[redacted]

November 19, 2026

By Email [redacted]
[EMPLOYEE B]
Factor Cybersecurity, Inc.

Re: *SecurityScorecard, Inc. v. Jason Thompson and Factor Cybersecurity, Inc.*

Dear Mr. [EMPLOYEE B]:

We are counsel for SecurityScorecard, Inc. ("SSC") in the above-referenced proceeding against Jason Thompson and Factor Cybersecurity, Inc. (together, "Factor"). This dispute concerns alleged breaches of Thompson's agreements and contractual and policy obligations to SSC, as well as disparagement of SSC, competitive harm to SSC, unauthorized use of SSC's intellectual property, bad faith, and breach of fiduciary duty.

We understand that you are Co-Founder and Vice President of Growth for Factor. You may therefore possess records relevant to this dispute. Please promptly take reasonable steps to preserve all documents, data, and electronically stored information. You are expected to promptly take reasonable steps to preserve such documents, data, and information within your possession, custody, or control, for the period January 1, 2017 to the present, and preserve any subsequently created or received records. Please do not destroy, delete, or materially alter such records and take reasonable steps to prevent their loss through routine deletion or other processes.

Please also preserve relevant paper records and electronic information, including email, text messages, messaging application communications, shared drive and cloud workspace records, and records on devices or accounts used for the relevant engagement. And please preserve native files and associated metadata, materially different versions, annotated copies, and unique attachments. Please avoid preservation methods that strip metadata or replace native records with printouts or screenshots alone.

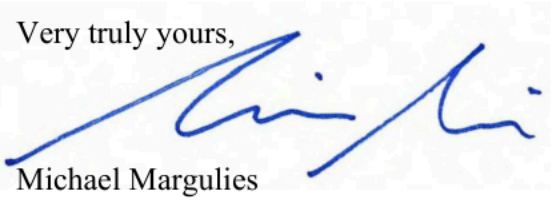
Also, to the extent applicable, please notify any of your personnel reasonably likely to hold relevant records and coordinate with appropriate IT personnel or service providers to suspend routine deletion, auto-delete, ephemeral-message settings, or other processes to the extent reasonably necessary to prevent loss of relevant information. If potentially relevant information exists only in a backup or other source that presents a material preservation burden, please contact us promptly to discuss an appropriate approach before it is lost.

Relevant materials may be sought through appropriate formal process. This letter requests preservation only; it does not request production of documents or disclosure of privileged or protected information, or ask you to waive any privilege, protection, confidentiality obligation, or objection. Please preserve potentially relevant materials even if you believe they may be privileged or otherwise protected.

Please acknowledge receipt by December 4, 2026 and identify the appropriate contact for preservation-related communications. If you anticipate material difficulty or burden in preserving any identified source, please contact us promptly, through your counsel if appropriate, so that we can discuss a reasonable approach.

We are available to further discuss if you have any questions.

Very truly yours,



Michael Margulies

cc: Charles Brown, Esq. (by email)

Exhibit A | Email transmission

Forwarded message header, reproduced in part

From: Margulies, Michael D. [redacted] Date: Thu, Nov 19, 2026 at 1:49 PM Subject: SecurityScorecard, Inc. v. Jason Thompson and Factor Cybersecurity, Inc. To: [redacted] Cc: Charles Brown [redacted] DL Security Scorecard < [redacted]

Source

Recipient-forwarded email dated November 19, 2026. Time reproduced as displayed in the forwarding chain.

CARLTON FIELDS

ATTORNEYS AT LAW

[redacted]

Atlanta
Hartford
Los Angeles
Miami
New York
New Jersey
Orlando
Tallahassee
Tampa
Washington, DC
West Palm Beach

Michael Margulies
Shareholder
[redacted]

November 19, 2026

By Email [redacted]
[ADVISOR A]

Re: *SecurityScorecard, Inc. v. Jason Thompson and Factor Cybersecurity, Inc.*

Dear Mr. [ADVISOR A]:

We are counsel for SecurityScorecard, Inc. ("SSC") in the above-referenced proceeding against Jason Thompson and Factor Cybersecurity, Inc. (together, "Factor"). This dispute concerns alleged breaches of Thompson's agreements and contractual and policy obligations to SSC, as well as disparagement of SSC, competitive harm to SSC, unauthorized use of SSC's intellectual property, bad faith, and breach of fiduciary duty.

We understand that you are a Strategic Advisor to Factor. You may therefore possess records relevant to this dispute. Please promptly take reasonable steps to preserve all documents, data, and electronically stored information. You are expected to promptly take reasonable steps to preserve such documents, data, and information within your possession, custody, or control, for the period January 1, 2017 to the present, and preserve any subsequently created or received records. Please do not destroy, delete, or materially alter such records and take reasonable steps to prevent their loss through routine deletion or other processes.

Please also preserve relevant paper records and electronic information, including email, text messages, messaging application communications, shared drive and cloud workspace records, and records on devices or accounts used for the relevant engagement. And please preserve native files and associated metadata, materially different versions, annotated copies, and unique attachments. Please avoid preservation methods that strip metadata or replace native records with printouts or screenshots alone.

Also, to the extent applicable, please notify any of your personnel reasonably likely to hold relevant records and coordinate with appropriate IT personnel or service providers to suspend routine deletion, auto-delete, ephemeral-message settings, or other processes to the extent reasonably necessary to prevent loss of relevant information. If potentially relevant information exists only in a backup or other source that presents a material preservation burden, please contact us promptly to discuss an appropriate approach before it is lost.

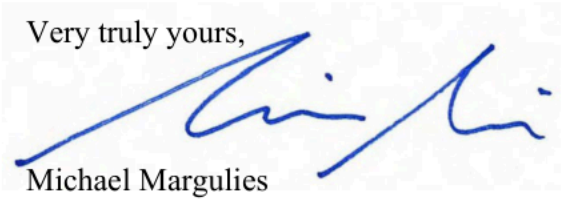
Relevant materials may be sought through appropriate formal process. This letter requests preservation only; it does not request production of documents or disclosure of privileged or

protected information, or ask you to waive any privilege, protection, confidentiality obligation, or objection. Please preserve potentially relevant materials even if you believe they may be privileged or otherwise protected.

Please acknowledge receipt by December 4, 2026 and identify the appropriate contact for preservation-related communications. If you anticipate material difficulty or burden in preserving any identified source, please contact us promptly, through your counsel if appropriate, so that we can discuss a reasonable approach.

We are available to further discuss if you have any questions.

Very truly yours,



Michael Margulies

cc: Charles Brown, Esq. (by email)

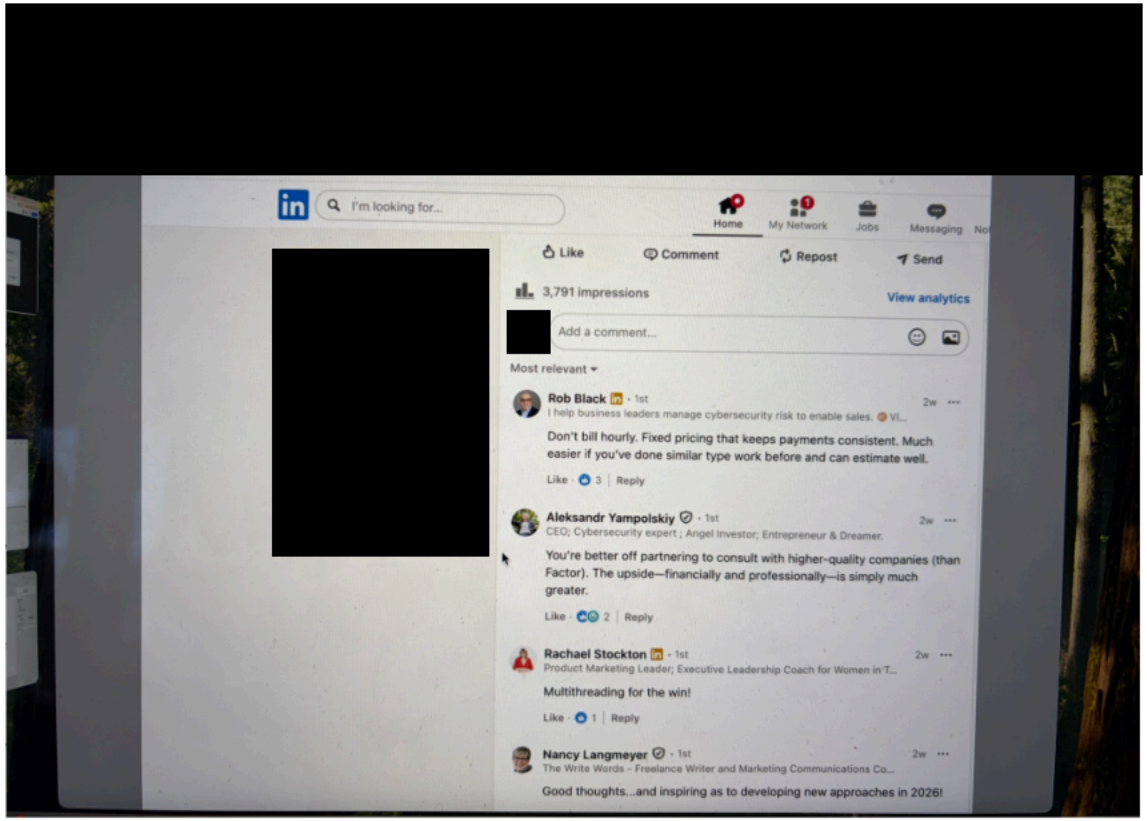
Exhibit B | Email transmission

Forwarded message header, reproduced in part

From: Margulies, Michael D. [redacted] Date: Thu, Nov 19, 2026 at 10:47 AM Subject: SecurityScorecard, Inc. v. Jason Thompson and Factor Cybersecurity, Inc. To: [redacted] Cc: Charles Brown [redacted] DL Security Scorecard < [redacted]

Source

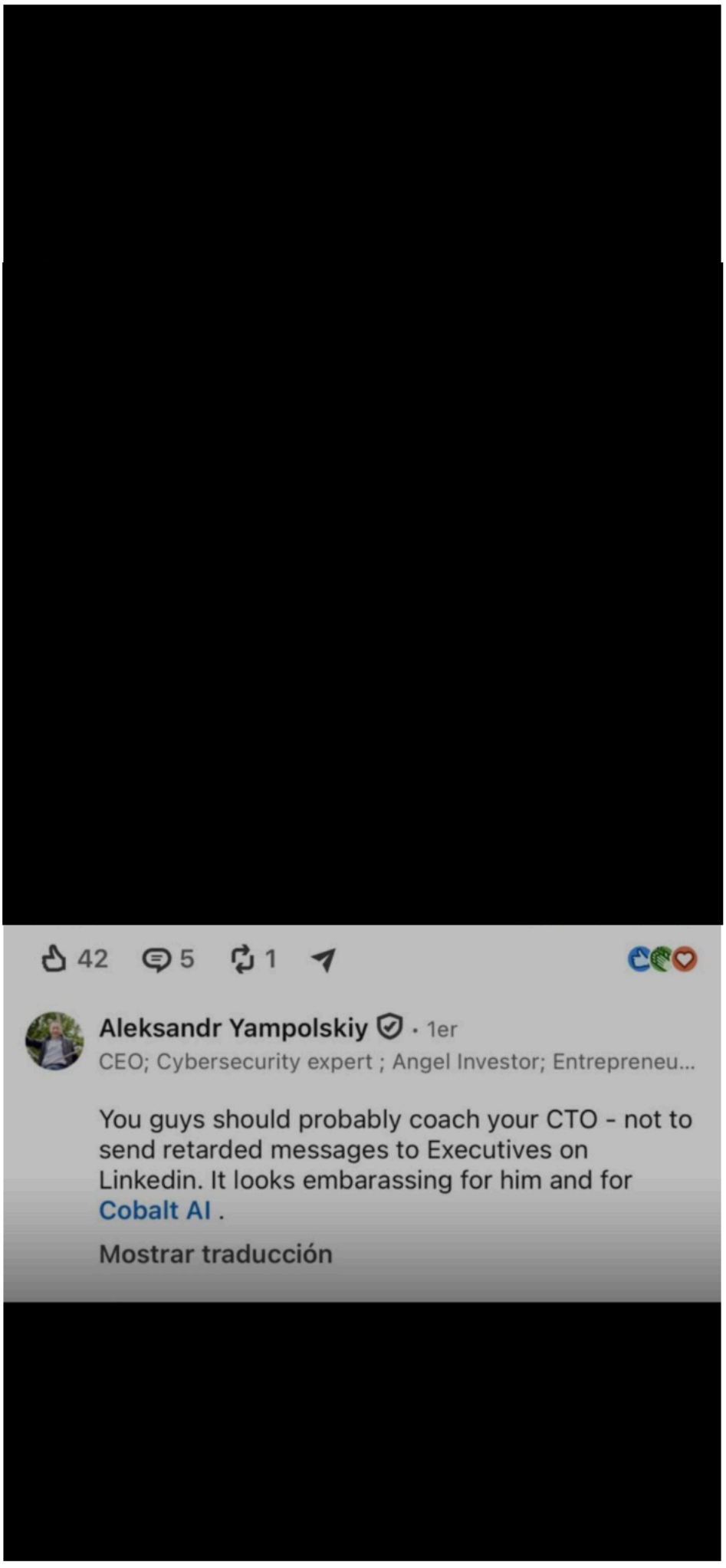
Recipient-forwarded email dated November 19, 2026. Time reproduced as displayed in the forwarding chain.

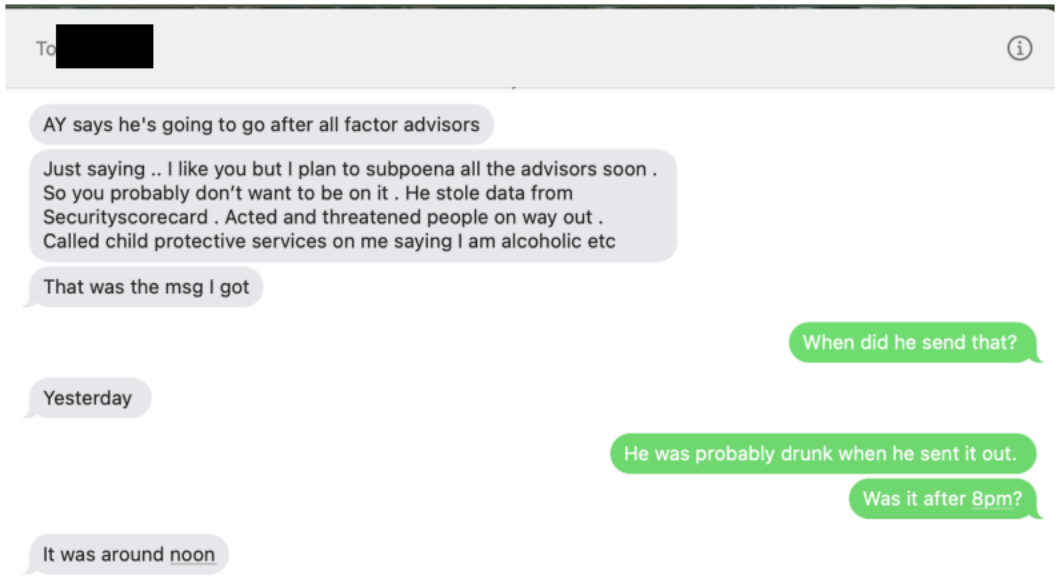


On or about 12/18/2025, Yampolskiy posts negative comments on Factor- then consultant and now VP of Growth LinkedIn page

Exhibit D | [ADVISOR A] appointment and Yampolskiy comment

Post: June 18, 2026 | Comment: on or about June 28, 2026 (Eastern time)





On or about July 12, 2026 Yampolskiy sent a message to [ADVISOR B] threatening action against all of Factor's advisors. There is no merit to his claims. At this point he has now met or sent messages to 4 of 6 associates of Factor listed on the website [redacted] In addition, to reaching out to a business partner, Mo, who I shared a photograph with while at the Gartner event in June 2026.

4. Threat to “Shoot Me Like a Dog”

Before the July 2, 2025 written exchange, Yampolskiy told me that he would:

> “Take you out back and shoot you like a dog.”

I understood this as a threat of violence.

At approximately 9:20 p.m. on July 2, 2025, I reminded Yampolskiy in writing that he had made this statement.

He did not deny making it.

Instead, he responded by listing conduct he claimed I had engaged in, including adding my business incubator to my LinkedIn profile. Other SecurityScorecard employees openly listed outside activities, organizations, hobbies, and business interests on their LinkedIn profiles.

Yampolskiy repeatedly described me as bizarre, erratic, and off track. He then wrote that I would be fired in the “most compassionate and collaborative way” and stated that it was his duty to protect the company.

This exchange occurred after I reported discrimination, nonpayment of compensation, questionable financial practices, and the company’s use of my intellectual property.

---

5. Retaliation and Statements to Other Executives

After I raised these concerns, Yampolskiy began making negative statements about me to other executives.

Chief Technology Officer Avesta Hojjati sent me messages indicating that Yampolskiy had said I was “acting like an idiot” and that he had already notified the board.

Yampolskiy also disclosed personal and health-related information about me to other people. Some of the information was false. For example, he told people I was getting divorced even though I was not married.

Yampolskiy knew I was receiving medical treatment for anxiety that had become progressively worse because of the work environment and his treatment of me.

His most aggressive communications commonly occurred after approximately 8:00 p.m. and when he had been drinking.

6.23 The July 2, 2025 Slack exchange records Yampolskiy proposing that Thompson move onward and warning that, if a collaborative departure could not be found, it would be his duty to control communications and next steps. The outer viewer of the supplied photograph displays July 2, 2025 at 9:54 p.m. The exchange followed Thompson's written complaints and included Yampolskiy's acknowledgment of his contributions. Employment Exhibits E-02 and E-02A preserve the communications.

6.24 The photograph shows Thompson writing: "I mean you did say you would take me out back and shoot me on a call at 8:30 AM". Thompson clarifies that "AM" was a typing error and that he meant approximately 8:30 p.m. Thompson's witness statement reports that Yampolskiy made the statement that evening and that he understood it as a threat. Under Thompson's corrected account, the 9:33 a.m. email preceded the evening call and the displayed Slack confrontation followed it. The photograph records Thompson's contemporaneous report; it is not an audio recording or an independent verification of the oral words.

Victim Notification and the Black Hat Presentation

1.71 The public presentations addressed an enterprise cybersecurity concern: companies using SSC's products and services, including major financial institutions, should be able to assess credible evidence that persons directing their security provider engaged in unauthorized competitor access and used the resulting information commercially. SSC publicly identifies major U.S. banks among its customers. The investigative account states that the reported conduct bears on provider trust, governance, data handling, product provenance, and the reliability of representations made to enterprise buyers.

1.72 On August 5, 2026, at Black Hat in Las Vegas, Nevada, Thompson publicly presented the alleged intermediary-account access, internal distribution and subsequent pressure on reporting

Conversation with Josh Fazio, former Illinois law enforcement and former SecurityScorecard employee. Also a witness in this case and provided information on Yampolskiy's activities. This is a live computer generated transcript not a recording of audio. I accidentally left the Zoom on a call where [redacted] did not show up because he is on vacation. [redacted] below is actually Josh.

Josh <> Jason

Enhanced | Today | 2 | Add to folder

Ongoing Situation with Alex

- Federal case progressing; Alex continuing to hire law firms to send threatening letters
  - Each firm backs off once informed of the federal case
  - Hired one firm specifically to take down an AI-generated drawing; that also failed
- All supportive VC/Richard Seyd posts about Alex have been deleted
  - Evolution Equity's entire team was on Jason's LinkedIn at 10:30pm, likely an emergency call
- Alex's board has not yet removed him as CEO; [redacted] believes removal would hurt more than jail
  - Strips his ability to weaponize law firms and resources

Threat Against [redacted]

- [redacted] received a blocked call Saturday morning (July 18) with a voice-masked threat: "If you help Jason Thompson, we will kill you"
  - Happened en route to Green Lake, Wisconsin; [redacted] wife witnessed it
  - FBI could not trace the call; [redacted] attributes it to Alex with high confidence
- [redacted] unconcerned personally; noted his home has cement walls and bulletproof windows
- Alex unlikely to obtain firearms legally given active federal investigation

communications," and you asked him to cease "publishing, republishing, or amplifying false, misleading, harassing, or defamatory statements concerning SSC, its officers, directors, employees, business partners, or other affiliated persons."

Contrary to your assertions, Mr. Thompson's statements are not defamatory and are supported by documents in Mr. Thompson's and SSC's possession and by third party witnesses. As a non-limiting example, there is ample evidence and witnesses who would testify concerning SSC's efforts to improperly obtain information about competitor products, including BitSight, Black Kite, and others. Josh Fazio, a former SecurityScorecard employee, is a witness to Mr. Yampolskiy's conduct and his unauthorized access to BitSight. In July 2025, Mr. Fazio received a blocked, voice-masked telephone call that was witnessed by his wife where the caller stated words to the effect of "if you help Jason Thompson, we will kill you." SSC has evidence that would confirm whether this call came from Mr. Yampolskiy, and we demand that you preserve all such evidence, including but not limited to Mr. Yampolskiy's phone records.

Nonetheless, Mr. Thompson already told you he will "refrain from making any further public commentary until" the issues discussed in this letter are resolved "[s]o long as you keep Yampolskiy in check." We remain open to such a compromise.

* * *

We are happy to discuss these issues with you. We look forward to your response.

Sincerely,

/s/ Benjamin J. Schladweiler

Benjamin J. Schladweiler

Wilton Manors Police Department

Incident Case Number: 43-2607-008675

Reporting Agency: Wilton Manors Police

Print Date/Time: 07/29/2026 16:32:03

Disclaimer: The information contained within this report is reflective of the investigation at the date and time of its printing.

INCIDENT/INVESTIGATION REPORT

Agency Name	*Wilton Manors Police Department*
ORI	*0060900*
Case#	*43-2607-008675*
Date / Time Reported	*07/13/2026 10:45 Mon*
Last Known Secure	*07/13/2026 10:45 Mon*
At Found	*07/13/2026 10:45 Mon*

INCIDENT DATA

Location of Incident	Gang Relat	Premise Type	Zone/Sector
[redacted]	NO	*Residence/home*	4301

	Crime Incident(s)		Weapon / Tools	Activity	Entry	Exit	Security
#1	*Information INFO*	(Com)					
#2	Crime Incident	( )					
#3	Crime Incident	( )					

MO

VICTIM

of Victims *0* | Type: | Injury: | Domestic: NO

	Victim/Business Name (Last, First, Middle)	Victim of Crime #	DOB / Age	Race	Sex	Relationship To Offender	Resident Status	Military Branch/Status
V1								

Home Address	Email	Home Phone

Employer Name/Address	Business Phone	Mobile Phone

VYR	Make	Model	Style	Color	Lic/Lis	VIN

OTHERS INVOLVED

CODES: V- Victim (Denote V2, V3) WI = Witness IO = Involved Other RP = Reporting Person (if other than victim)

Type: INDIVIDUAL (NOT A LE OFFICER) Injury:

Code	Name (Last, First, Middle)	Victim of Crime #	DOB / Age	Race	Sex	Relationship To Offender	Resident Status	Military Branch/Status
RP	*THOMPSON, JASON DANIEL*		[redacted] Age *47*	*W*	*M*		*Resident*	

Home Address	Email	Home Phone
[redacted]		[redacted]

Employer Name/Address	Business Phone	Mobile Phone

Type: Injury:

Code	Name (Last, First, Middle)	Victim of Crime #	DOB / Age	Race	Sex	Relationship To Offender	Resident Status	Military Branch/Status

Home Address	Email	Home Phone

Employer Name/Address	Business Phone	Mobile Phone

PROPERTY

1 = None 2 = Burned 3 = Counterfeit / Forged 4 = Damaged / Vandalized 5 = Recovered 6 = Seized 7 = Stolen 8 = Unknown
("OJ" = Recovered for Other Jurisdiction)

VI #	Code	Status Frm/To	Value	OJ	QTY	Property Description	Make/Model	Serial Number

Officer/ID# *ELISTIN, J. (PATR, PATR) (318)*

Invest ID# *(0)* Supervisor *FINDLAN, W. (PATR) (265)*

Status | Complainant Signature | Case Status *Inactive* *07/13/2026* | Case Disposition:

INCIDENT/INVESTIGATION REPORT

Wilton Manors Police Department

Case # *43-2607-008675*

Status Codes L = Lost S = Stolen R = Recovered D = Damaged Z = Seized B = Burned C = Counterfeit / Forged F = Found

	UCR	Status	Quantity	Type Measure	Suspected Type	Up to 3 types of activity
DRUGS						

Assisting Officers

Suspect Hate / Bias Motivated: *NONE (NO BIAS)*

INCIDENT/INVESTIGATION REPORT

Narr. (cont.) OCA: 43-2607-008675 *Wilton Manors Police Department*

NARRATIVE

Time received: 1045 Time dispatched: 1045 Time arrived: 1045 Time cleared: 1130

On 07/13/2026, I spoke with (RP) Jason Thompson over the phone in reference to a former employer (IO) Alexander Yampolskiy, owner of Factor Cyber Security, who has been reaching out to prospective clients of Thompson and making false claims about him. Thompson claims that he parted ways with Yampolskiy a year ago after finding out his company was dealing in illegal transactions. Thompson advised that since parting ways, his former employer has actively reached out to Thompson`s current clientele via LinkedIn and spread false allegations about Thompson. A link was sent to Thompson to upload the messages received by his clients and other harassing correspondence from Yampolskiy. Thompson was provided with the case number and the steps to obtain a restraining order.

NFAT

BWC was activated.

Page	Report Date	Agency	Complaint Number
001	08/25/2026	TROOP 7 STATE POLICE	07-26-056846

Reported Date and Time	Initial Crime Report	Occurred
Wed 08/19/2026 2055		Wed 08/19/2026 2055

Location:
[redacted] of [redacted]

M.O. and Incident Overview:
Jason Thompson reported alleged threats connected to an ongoing cybersecurity matter and requested stalking charges against Aleksandr Yampolskiy. Insufficient evidence existed to identify the caller or establish probable cause.

Grid	Sector	County	Domestic Related	Gen Broadcast Sent?	Gang Related?	Gun Related?
202 - 096	72	Sussex	☐ Yes ■ No	☐ Yes ■ No	☐ Yes ■ No	☐ Yes ■ No

Investigating Officer Email
[redacted]

Emergency Order Related:	Hero Help Referral:	PDP Referral/DSAMH Notification:	Officer Response To Resistance:
☐ Yes ■ No	☐ Yes ■ No	☐ Yes ■ No	☐ Yes ■ No

Victim Information

Victim Number	Name					
001	THOMPSON, JASON					
Type	Sex	Race	Ethnic Origin	Age	D.O.B	
Individual	Male	White	Not Hispanic/Latino	47	[redacted]	
Address			Resident Status	Home Telephone	Cell Phone	
[redacted]			Full-Time Resident		[redacted]	

Reporting Person?	Victim Injured?	Victim Deceased?
■ Yes ☐ No	☐ Yes ■ No	☐ Yes ■ No

Crimes and Associated Information

Victim Number	Crime Seq	Statute	Crime Description		
001	001	MISCELLANEOUS	Miscellaneous Investigation, Industrial Accident, Lost Property		
Location of Offense		Status	Involvement		General Offense
Residence/Home/Garage		Pending-Inactive	☐ Alcohol ☐ Drugs ☐ Computer		
Suspected Hate/Bias	[redacted]	Crime Code			
☐ Yes		8198 - Miscellaneous Investigation			

Reporting Officer	Pending Supervisory Review
TPR HUDSON - 02354 0	

SUMMARY OF CRIME VICTIMS' RIGHTS

This is a summary of your rights under Delaware's Crime Victims' Bill of Rights (Title 11, Chapter 94). Not every right applies in every case and not every right is listed here. These rights exist to support and protect you throughout the criminal justice process. Victims have the right to:

- Confidentiality
- Safety
- To speak with a prosecutor about their case
- Notification
- Return of Property
- To be present at all stages
- A voice in the process
- Support of a victim advocate
- Information about services
- Status of Rape Kit
- Notice of Rights

Victims' Rights include limitations on employers of victims (§ 9409), a right of a victim of an alleged sex offense not to be polygraphed (§ 9420), and victims and witnesses cannot be detained or reported to immigration authorities without a court order (§ 9404 and § 9425). If you feel your rights have been violated, you can file a complaint pursuant to § 9402 of Title 11.

The Delaware Victims' Rights Task Force (a collective of service providers in Delaware) with the support of the Delaware Department of Justice has created a website with more information and resources.
Please visit: **https://www.delawarevictimservices.org**. Available in English, Spanish, and accessible formats.

**** Victims must provide changes in contact information to the police and the Department of Justice ****

Statewide Victim Assistance Resources

The Victims' Compensation Assistance Program (VCAP) can provide financial assistance to help cover the costs of a variety of services including lost wages, medical expenses, payment for mental health counseling, and funeral expenses. Information can be found at **https://attorneygeneral.delaware.gov/VCAP/** or calling 302-255-1770.

Domestic Violence 24/7 Hotlines
New Castle County/Child Inc.: 302-762-6110
Kent/Sussex Co/Peoples Place: 302-424-2420
Sussex/Bilingual: Abriendo Puertas: 302-745-9874

Sexual Assault 24/7 Hotlines
YWCA Sexual Assault Resource Center
New Castle/Sussex: 800-773-8570
ContactLifeline Rape Crisis Service
Kent/Sussex County: 800-262-9800

Other 24/7 Hotlines
Child Abuse Report Line: 800-292-9582
Adult Mobile Crisis
Northern DE: 800-652-2929
Southern DE: 800-345-6785
Child Mental Health Mobile Crisis: 1-800-969-4357
Delaware State Police Crime Victims Center
800-VICTIM-1 / 800-842-8461

VINE (offender custody status)
877-338-8462 / www.vinelink.com

National Guard (DENG)
Sexual Assault Prevention and Response:
24/7 Hotline: 302-326-7272
DENG Domestic Violence Reporting: 302-329-7582

Police Based Victim Services
*police agencies not listed utilize the Delaware Victim Center for victim services
Delaware State Police / Delaware Victim Center
800-VICTIM-1 / 800-842-8461
Dover Police: 302-736-7134
Georgetown Police: 302-856-6613
Millsboro Police: 302-934-8174
New Castle County Police: 302-395-8000
Newark Police: 302-366-7100 x3137
Smyrna Police: 302-223-7024
Wilmington Police: 302-576-3622

Attorney General's Office Victim Services
New Castle County: 302-577-8500
Kent County: 302-739-4211
Sussex County: 302-856-5352

Department of Correction
Victim Services: 302-857-5440

Dover Air Force Base
Family Advocacy Program: 302-677-2711
Security Force: 302-677-6666
Sexual Assault Prevention and Response:
24/7 Hotline: 302-363-7272

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

FACTOR CYBERSECURITY, INC. and JASON THOMPSON, *Plaintiff,* v. SECURITYSCORECARD, INC. and ALEKSANDR YAMPOLSKIY, *Defendants.*	C.A. No. _____ **JURY TRIAL DEMANDED**

COMPLAINT

Plaintiffs Factor Cybersecurity, Inc. ("Factor") and Jason Thompson ("Thompson" and jointly with Factor, "Plaintiffs"), by and through their undersigned counsel, bring this action against Defendants SecurityScorecard, Inc. ("SSC") and Aleksandr Yampolskiy ("Yampolskiy" and jointly with SSC, "Defendants"), and allege as follows:

NATURE OF THE ACTION

1. This action arises from Defendants' campaign to interfere with the business, reputation, and commercial relationships of Factor, a Delaware corporation founded by Thompson in July 2021. Defendants have falsely accused Factor and Thompson of misappropriating SSC's intellectual property, questioned Plaintiffs' ownership of their technology and name, and threatened litigation despite lacking a factual basis for those assertions.

2. While employed by SSC, Thompson witnessed improper conduct by certain SSC employees and Yampolskiy, including efforts to steal the technology of its competitors. Shortly before he resigned from SSC he reported this conduct to SSC's board of directors. Defendants

intellectual property. These false accusations were made publicly on social media and in communications with Factor's employees, advisors, and business partners listed on Factor's website.

40. In his communications, Yampolskiy threatened Factor's employees and partners with "reputational or legal complications," subpoenas, and other adverse actions if their association with Factor continued. These communications appear to have been designed to frighten Factor's employees, advisors, and partners, discourage people from working with Factor, damage Factor's professional reputation, imply that anyone associated with Factor will become involved in baseless litigation, and interfere with Factor's employment, advisory, investment, and commercial relationships.

41. By way of nonlimiting example, Factor advisor [redacted] received the following threat from Yampolskiy in May 2026:

> I wanted to flag something sensitive. I saw your name listed as an advisor on Jason's/Factor's website. I don't know the nature of your involvement, but I would encourage you to be careful before lending your name publicly. From SecurityScorecard's perspective, there are serious unresolved concerns involving Jason and Factor, including potential IP/misappropriation issues that may become the subject of legal action. There were also serious concerns around his conduct when he left the company.
>
> I'm not asking you to take my word for it, and I'm not trying to put you in the middle of anything. I just wanted to make sure you were aware that association with the company could potentially create unwanted reputational or legal complications. -Alex

42. On May 15, 2026, Thompson sent a cease and desist notice to SSC's board of directors requesting that SSC stop contacting Factor's employees, advisors, customers, investors,

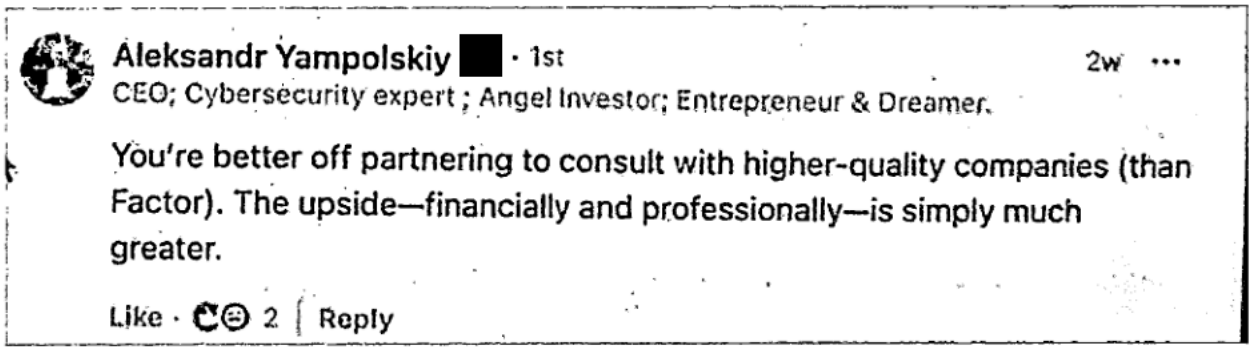
and affiliates. SSC, however, seemingly took no action as Defendants' tortious and defamatory conduct not only continued, but it increased.

43. On June 9, 2026, a Factor business partner reported that Yampolskiy had contacted him immediately after Thompson posted event photographs showing him with Thompson at a Factor booth at an event, and reported that Yampolskiy made false claims that Plaintiffs stole intellectual property to him.

44. In July 2026, Yampolskiy sent a message to [redacted] a BitSight senior vice president and Factor advisor, making similar false allegations about data theft and other defamatory statements about Thompson.

> Just saying .. I like you but I plan to subpoena all the advisors soon . So you probably don't want to be on it . He stole data from Securityscorecard . Acted and threatened people on way out . Called child protective services on me saying I am alcoholic etc

45. As shown below, Yampolskiy (holding himself out as SSC's CEO) also made disparaging comments about Factor on the public social media pages of Factor's employees and business associates.



46. In total, Yampolskiy has threatened most of Factor's associates listed on its website. Indeed, by July 12, 2026, he had met with or sent messages to four of the six Factor associates

displayed at [redacted] He has also made threats against other business associates of Factor.

47. Defendants' copying allegations are not only false, but they are also implausible on their face. Thompson never had access to SSC's code during his employment, and SSC has yet to produce any evidence supporting its baseless allegations such as the MDM logs in SSC's possession that could definitively show that such copying did not occur.

48. SSC and Yampolskiy's false statements were made to damage Factor and its business relationships. For instance, these false statements caused Factor to lose out on prospective business opportunities that likely would have happened but for Defendants' interference, including a partnership which Factor targeted at $3M in revenue. The interference has also caused issues with fundraising and delayed a planned fundraising round targeted at $25M.

V. SSC THREATENS BASELESS LITIGATION

49. On or about July 14, 2026, SSC's legal department sent a demand letter to Thompson, asserting that Factor, its name, technology, work product, and other assets belonged to SSC and threatening litigation. (**Exhibit C**). On August 10, 2026, Factor's counsel sent a letter to SSC denying SSC's allegations and asking for evidence (including MDM logs) that could definitively determine whether SSC's allegations were true or false. (**Exhibit D**). SSC refused to provide the requested information and ignored Plaintiffs' requests to retract its tortious and defamatory statements.

50. As described above, SSC's allegations are unfounded as Thompson never had access to SSC source code or trade secrets, and Factor has never possessed or used them. Additionally, SSC never had any right to the FACTOR CYBERSECURITY name.

Exhibit J | FBI Boston and witness cooperation

What I reported and what the FBI did

I reported alleged unauthorized access to BitSight and the involvement of Aleksandr Yampolskiy. On November 4, 2026, an FBI official advised me that a Boston supervisory special agent was taking over the matter and that my reports would be shared. Boston confirmed receipt, asked whether the activity was ongoing, and discussed assignment and speaking to BitSight. On November 12 the supervisor requested a discussion. I spoke with the FBI and on November 16 sent an updated report, presentation and links to supporting evidence. The correspondence documents these investigative steps. It gives no formal case classification or list of other witnesses already interviewed.

What the FBI knew about pressure before November 19

On November 5, I told the Boston supervisor that I believed Yampolskiy was using successive lawyers and threatened legal expense to impair our ability to cooperate. I identified [ADVISOR B] as the lead BitSight investigator who could confirm the account findings, and told the FBI that Yampolskiy had targeted him personally. This email records my contemporaneous report to the FBI.

Alleged witness intimidation

I allege an ongoing scheme directed by Yampolskiy and carried out with the participation of his attorneys to intimidate witnesses and people supporting Factor's cooperation. Exhibit E records [ADVISOR B]'s relay of the advisor warning. Josh Fazio, a former Illinois law enforcement officer and SecurityScorecard executive, provided information for the BitSight investigation. The caller threatened to kill him if he helped me (Exhibit F). Exhibits C and D identify earlier public attacks affecting the same two people Margulies contacted in November. On November 19, three days after my investigative follow-up, Margulies used their personal addresses to demand action.

Exhibit J | Dated correspondence excerpts

November 4, 2026 | FBI handoff and acknowledgment

An FBI official said the Boston supervisor was “taking this over” and added: “I’ll share the reports you have provided to them.” The Boston supervisor replied: “is there any ongoing activity or is this historic?” and referred to taking “time to talk to BitSight and get a better understanding.”

November 5, 2026 | Thompson to FBI Boston, “Latest Escalation from Yampolskiy/SecurityScorecard”

“This is the latest in more than a half dozen threats we have received from him via various counsel.” I identified [ADVISOR B]’s technical role and stated: “[ADVISOR B] was also one of the direct targets of Yampolskiy’s threats.”

November 12, 2026 | FBI Boston to Thompson, SecurityScorecard/Yampolskiy matter

The Boston supervisor asked: “do you have time to talk through this matter?”

November 16, 2026 | Thompson to FBI Boston, “Updated presentation and investigative report”

“Thank you for taking the time to speak with me. I appreciate the opportunity to walk through this with you.” I provided links to the updated presentation and investigative report and wrote that the report linked to “the relevant sections and supporting evidence.”

Source

Excerpts transcribed from the November 4, 5, 12 and 16 email messages. Agent names, direct contact details and access links are omitted. Original messages are identifiable by date, direction and subject.

Exhibit dates and sources

A and B | November 19, 2026 | pp. 9–14

Margulies's letters and emails to [EMPLOYEE B] (A) and [ADVISOR A] (B). December 4 was the requested acknowledgment deadline.

C | On or about December 18, 2025 | p. 15

[EMPLOYEE B] LinkedIn comment. The approximate date comes from the caption in my witness statement.

D | June 18–28, 2026 | p. 16

Cobalt AI posted the announcement June 18 at 9:00 a.m. Eastern. [ADVISOR A] posted his response June 28 at 11:39 p.m. Eastern and described the conduct as occurring on Sunday evening. These times are derived from the two public LinkedIn activity identifiers. June 28 is the apparent date of the comment; its own timestamp is not visible.

E | On or about July 12, 2026 | p. 17

[ADVISOR B] identified the advisor warning as having arrived around noon the previous day. The calendar date comes from my chronology.

F | July 2025–August 2026 | pp. 18–21

Threat to Thompson: July 2, 2025. Fazio call: the meeting summary gives Saturday, July 18, consistent with 2026; counsel's August 10, 2026 letter instead gives July 2025.

G and H | July and August 2026 | pp. 22–27

Florida: reported July 13; printed July 29. The officer misidentified Yampolskiy as Factor's owner on p. 25. See my correction on p. 8. Delaware: incident reported August 19; report dated August 25.

I | September 3, 2026 | pp. 28–31

Delaware federal complaint, filing date shown in the docket header.

J | November 4–16, 2026 | pp. 32–33

FBI correspondence of November 4, 5, 12 and 16.

K | October 30–November 19, 2026 | pp. 3–5

Proceedings and letters discussed: October 30 demand, November 3 federal filings and November 19 direct contacts. Page 4 states the Rule 3.1 grounds. Page 5 reproduces sections 20 and 21 of the May 17, 2023 contractor agreement.

Cobalt AI announcement [ADVISOR A] response