IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Microsoft Corporation, a Washington State Corporation, NGO-ISAC, a New York State Non-Profit Organization, Plaintiffs, v. John Does 1-2, Controlling A Computer Network and Thereby Injuring Plaintiff and Its Customers, Defendants.	Civil Action No. **FILED UNDER SEAL PURSUANT TO LOCAL RULE 5.1**

DECLARATION OF YOTARO SHERMAN IN SUPPORT OF APPLICATION FOR AN EMERGENCY *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

I, Yotaro Sherman, declare as follows:

1. I am the Associate Director of Information Technology (IT) of the Carnegie Corporation of New York ("Corporation"). I make this declaration in support of Plaintiffs' Application for an Emergency *Ex Parte* Temporary Restraining Order and Order to Show Cause re Preliminary Injunction. I make this declaration of my own personal knowledge or on information and belief where noted. If called as a witness, I could and would testify to the truth of the matters set forth herein.

2. I have been employed by the Corporation since 2009. In my role at the Corporation, I manage the organization's cybersecurity initiatives, technology architecture, security software and monitoring, incident response planning, policies, procedures and staff training/awareness. In this role, my responsibilities include the internal investigation of reports associated with a variety of IT issues impacting the Corporation, its employees, and associated partners. This includes

investigating reports of phishing or spear phishing emails.

3. I am also responsible for coordinating complex technology systems, facilitating development and maintenance of internal- and external-facing applications, and directing IT projects to meet business objectives, operational goals and key business priorities. Prior to joining the Corporation, I served as the Director of Information Technology at an organization that was an independent entertainment distributor and collector of independent digital content. A current version of my curriculum vitae is attached to this declaration as **Exhibit 1.**

I. CARNEGIE CORPORATION OF NEW YORK

4. The Carnegie Corporation of New York is an NGO-ISAC member organization, and one of America's oldest grantmaking foundations. It was established by Andrew Carnegie in 1911 "to promote the advancement and diffusion of knowledge and understanding," is one of the oldest, largest and most influential of American foundations. Some notable contributions of the Corporation include: (i) expansion of higher education and adult education, (ii) advancement of research on learning and cognitive development in early childhood, (iii) promotion of educational and public interest broadcasting, (iv) advancement of minorities and women in precollege and higher education, (v) heightening public understanding of the education and health needs of children and adolescents, (vi) investigation of risks of superpower confrontation, nuclear war, and ethnic and civil strife. Today, the Corporation promotes the advancement and diffusion of knowledge and understanding. In keeping with this mandate, the Corporation's work focuses on the issues of international peace,[1] the advancement of education and knowledge, and democracy.

[1] The Corporation's grant program on International Peace and Security focuses on global issues, including Russia. In 2022, the Corporation issued a report analyzing how Russia's invasion of Ukraine has adversely affected US-based Russian Studies efforts. Wilfred Chan, *How Russian Studies Is Grappling with the War in Ukraine*, Carnegie Corporation of New York, available at https://www.carnegie.org/our-work/article/how-russian-studies-is-grappling-with-the-war-in-ukraine/ (May 3, 2024).

5. The Corporation has helped establish or endowed a variety of institutions, including the Carnegie libraries, the National Research Council, the Russian Research Center at Harvard, and the Children's Television Workshop, and for many years heavily supported Carnegie's other philanthropic organizations, especially Carnegie Endowment for International Peace (CEIP), the Carnegie Foundation for the Advancement of Teaching (CFAT), and the Carnegie Institution of Washington (CIW). It has funded the writing of books and studies, as well as the organization of conferences and international exchanges, radio shows, legal proceedings and other activities. Through its activities, the Corporation has had a great impact on the information and knowledge available to citizens and government alike. Its work and that of its grantees has exerted a substantial influence on public discourse and policy.

II. OVERVIEW OF THE STAR BLIZZARD THREAT

6. My declaration concerns the spear-phishing attacks targeting nonprofits and NGOs, and as it applies here, regarding the Star Blizzard phishing operation. *See* Declaration of Sean Ensz in Support of Plaintiffs' Application For An Emergency *Ex Parte* Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction ("Ensz Decl.") ¶ 1. Star Blizzard Defendants are believed to be a Russia-based operation that engages in spear phishing resulting in the online impersonation of individuals and organizations, the infiltration of email accounts, and the exfiltration of sensitive and confidential information from those online accounts. Complaint ¶ 3. Star Blizzard Defendants are formerly known as SEABORGIUM and also known in the cybersecurity community as the Callisto Group, COLDRIVER, and BlueCharlie.

7. According to Microsoft's investigations, the Star Blizzard Defendants' campaigns target over 30 organizations, in addition to personal accounts of people of interest. Star Blizzard Defendants primarily target NATO countries, particularly the United States and the United

Kingdom, and other countries in the Baltics, the Nordics, and Eastern Europe. Complaint ¶ 18.

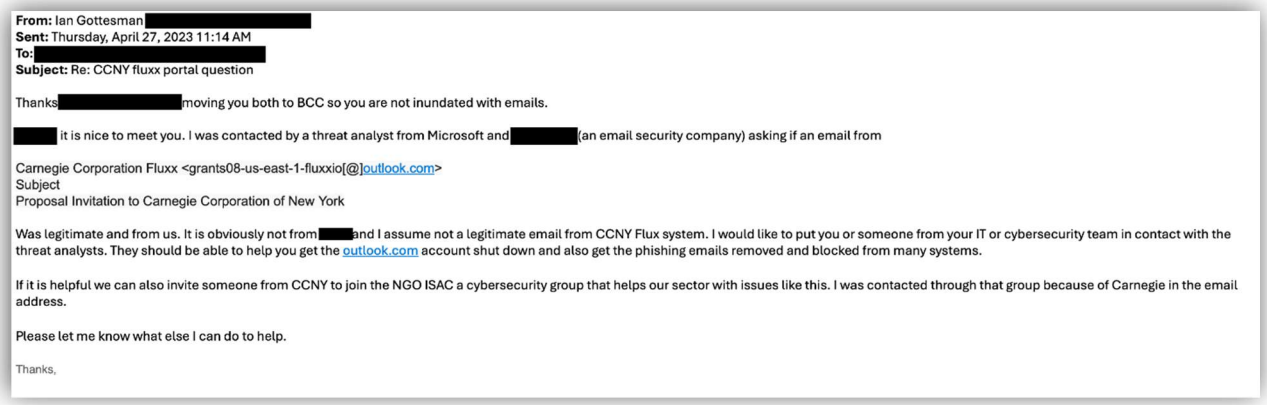
8. Microsoft has observed the Star Blizzard Defendants' campaigns continue to target NGOs, think tanks, government employees, and personal accounts belonging to current and former military and intelligence officials and policy advisors. The individuals targeted by these attacks predominately reside in the U.S., in and around the Washington, D.C. area. Complaint ¶ 14.

III. IMPACT ON THE CORPORATION

9. As discussed earlier, the Corporation's promotes the advancement and diffusion of knowledge and understanding around the issues related to international peace, the advancement of education and knowledge, and democracy. It has done so by establishing a grant program that provides financial support to applicants whose projects are focused on these areas. Once the Corporation issues a grant, the grant recipient (also called a grantee) is issued a grant number. This grant number is not public information. The grantee has a shared responsibility with the Corporation to manage the projects and its finances responsibly. As part of this process, a grantee is required to submit a report about the project's finances and status. The Corporation uses a grant management software called Fluxx and one of its features is the ability for grantees to submit reports through Fluxx's online portal associated with the Corporation's Fluxx account.

10. The Corporation and its grantees have been targeted by Star Blizzard Defendants by impersonating the Corporation in spear phishing emails to grantees. The Corporation was first made aware of Star Blizzard Defendants' spear phishing operation by Ian Gottesman, the current Chief Executive Officer of the NGO Information Sharing and Analysis Center ("NGO-ISAC"), who was at that time, with the Carnegie Endowment for International Peace ("CEIP"). **Figure 1** below is an email from Mr. Gottesman detailing the fake email and efforts by a threat analyst from the Microsoft Corporation ("Microsoft") in investigating the authenticity of an email purportedly

sent by the Corporation.



From: Ian Gottesman [redacted]
Sent: Thursday, April 27, 2023 11:14 AM
To: [redacted]
Subject: Re: CCNY fluxx portal question

Thanks [redacted] moving you both to BCC so you are not inundated with emails.

[redacted] it is nice to meet you. I was contacted by a threat analyst from Microsoft and [redacted] (an email security company) asking if an email from

Carnegie Corporation Fluxx <grants08-us-east-1-fluxxio[@]outlook.com>
Subject
Proposal Invitation to Carnegie Corporation of New York

Was legitimate and from us. It is obviously not from [redacted] and I assume not a legitimate email from CCNY Flux system. I would like to put you or someone from your IT or cybersecurity team in contact with the threat analysts. They should be able to help you get the outlook.com account shut down and also get the phishing emails removed and blocked from many systems.

If it is helpful we can also invite someone from CCNY to join the NGO ISAC a cybersecurity group that helps our sector with issues like this. I was contacted through that group because of Carnegie in the email address.

Please let me know what else I can do to help.

Thanks,

Figure 1.

11. As part of our investigation into the issues, our team was also made aware of a blog Microsoft issued around Star Blizzard Defendants' activities that impersonated the Fluxx grant management system. **Figure 2** below is the Star Blizzard Defendants' phishing email example in the blog – it referenced that a "report is overdue" and purportedly comes from the Fluxx grant system.

Date: Thu, 18 May 2023 11:21:46 +0000
From: [redacted]
Return-Path: grants07us-east@fluxx-east.com
To: [redacted]
Message-ID:
<CABjCnfCX=j=rc5pdBqGJcCBZnw+8DChjAuO_5Fcuizr34fMZ5g@mail.gmail.com>
Subject: Report Overdue - [redacted]

Figure 2.

12. Since the Corporation uses the Fluxx grant management system, the Corporation issued a notice to all 2,600 grantee contacts of the Corporation's active grants to alert them of potential spear phishing attempts. Grantees began reporting receiving emails with the same identifying features, which they initially believed to be a legitimate communication from the Corporation. True and correct snapshots of these phishing emails are included with this declaration as **Exhibit 2** (identifying information contained within the Images included in the Exhibit have been redacted for privacy of the targets and victims of the Star Blizzard Defendants). Among those who reported receiving the Star Blizzard Defendants' spear phishing emails are grantees at universities as seen in **Images 1 – 3** in Exhibit 2 attached to this declaration.

13. The Corporation investigated the spear phishing reports and found that Star Blizzard Defendants' spear phishing emails to the Corporation's grantees impersonated the Corporation's grant program, referenced that reports were overdue, identified the need for a Fluxx grant portal submission, and even referenced grant numbers associated with the issued grants. A link to log into the Fluxx report submission system was included in the spear phishing emails. An examination of the sender email addresses in the reported phishing emails showed that they were not issued by the authentic email address associated with the Corporation's Fluxx grant system. The Star Blizzard Defendants also used the Corporation's trademarked name "Carnegie Corporation of New York" on the subject line of their malicious emails. In the examples shown in Exhibit 2, Star Blizzard Defendants referenced the correct grant numbers for two of the grantee victims and referenced two incorrect grant numbers for the other two grantee victims. *See* **Appendix C** to the Complaint for the Corporation's trademarks.

14. The Star Blizzard Defendants, by referencing specific features like a grant number and a real document type, demonstrates that the Star Blizzard Defendants had access to and were

able to view non-public information in its victim's accounts. Given this level of specificity, the Corporation is harmed because grantee victims are tricked into believing the legitimacy of the email and will be more likely to engage with the lure that the Star Blizzard Defendants include in the spear phishing email. Since two of the four spear phishing emails referenced incorrect grant numbers, the Star Blizzard Defendants likely only had access to information in their target's emails and not the Corporation's secured, internal grant management system or any other of the Corporation's internal systems.

15. The Corporation invested a significant amount of resources and time in order to mitigate the risks that Star Blizzard Defendants posed and additionally, to strengthen the Corporation's data security and IT system totaling approximately $200,000 since 2023. My team spent over forty hours to investigate the Star Blizzard Defendants' spear phishing activities (which included outreach to the Corporation's 2,600 grantee contacts), engaged Fluxx to assess the grant management system, engaged an outside firm to conduct a risk assessment, and then committed additional resources and time to implement additional security recommendations to protect the Corporation, its grantees, and other partners from the Star Blizzard Defendants' activities. Since the grantees rely on the Corporation for funding the important work they do to advance the knowledge and understanding around the issues related to international peace, the advancement of education and knowledge, and democracy, any diversion of the Corporation's resources and time has a direct impact on achieving the Corporation's mission and a grantee's work.

16. The Star Blizzard Defendants' activities irreparably harm the Corporation by damaging its reputation, brand, and goodwill cultivated with its grantees and organizational partners. The spear phishing attacks that the Star Blizzard Defendants perpetrated against the Corporation's grantees are incorrectly attributing their activities to the Corporation. To be an

effective partner within the nonprofit and non-governmental affairs community, the Corporation must be seen as a trusted organization by its grantees and organizational partners. The Corporation has invested significant resources and time to establish itself, its brand, and develop relationships over time both domestically and internationally, and are determined to ensure that its reputation remains intact.

IV. CALL FOR LEGAL ACTION

17. Given the severe implications of the Star Blizzard Defendants' campaign, I strongly support the application for an emergency temporary restraining order and preliminary injunction. Such legal action is crucial to disrupting the Star Blizzard Defendants' spear phishing operations and safeguarding the Corporation, its grantees, and its partners. Without the Court's intervention, the Corporation, its grantees, and its partners will continue to suffer from harm caused by the Star Blizzard Defendants' actions.

18. The Court's swift and decisive action is necessary to address the threats posed by the Star Blizzard Defendants, ensuring that the Corporation can continue its vital work to support work advancing international peace, education and knowledge, and democracy.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge. Executed on September 24, 2024 in New York, New York.

/

_____

Yotaro Sherman

Associate Director of Information Technology
Carnegie Corporation of New York

Yotaro Sherman

PROFESSIONAL EXPERIENCE

Carnegie Corporation of New York **2009 – Present**

Associate Director of Information Technology *2016 – Present*
Business Application Delivery Manager *2009 – 2016*

Roles and Responsibilities

- Directly oversees the department's business application support. This includes identifying and implementing enhancements, performing upgrades, developing reports and interfaces, servicing end user requests, addressing any issues and managing vendor relationships.
- Researches, analyzes, documents, designs, and implements improvements and additions to existing workflow procedures. Promotes the use of data analysis/management tools throughout the organization.
- Manages Carnegie Corporation's cloud-based infrastructure. Monitors ongoing resource requirements, conducts application and data migrations, performs problem resolution and proposes the adoption of new tools and services.
- Provides significant contributions to the organization's cybersecurity mandates, encompassing our technology architecture, security software and monitoring, incident response planning, policies, procedures and staff training/awareness.
- Partners with all departments on adopting innovative ways technology can improve the delivery of Carnegie's mission and goals. Develops and deploys metrics to inform business decisions.
- Conducts vendor evaluations and negotiations. Audits software usage to ensure compliance with associated licensing agreements.
- Supervises the Application Support Engineer, Network Specialist and End-User Support Analyst. Establishes performance goals, conducts performance appraisals and provides ongoing mentoring.
- Manages and coordinates various technology projects as required, ensuring company resources are utilized appropriately and within budget. Identifies and analyzes systems requirements and defines project scope and deliverables.
- Develops and promotes the adoption of internal I.T. governance policies based on the ITIL framework.
- Provides general, technology support to meet the day-to-day needs of Carnegie's end user community.

New Video Group, Inc. – New York, New Yorklocation **2000 – 2008**

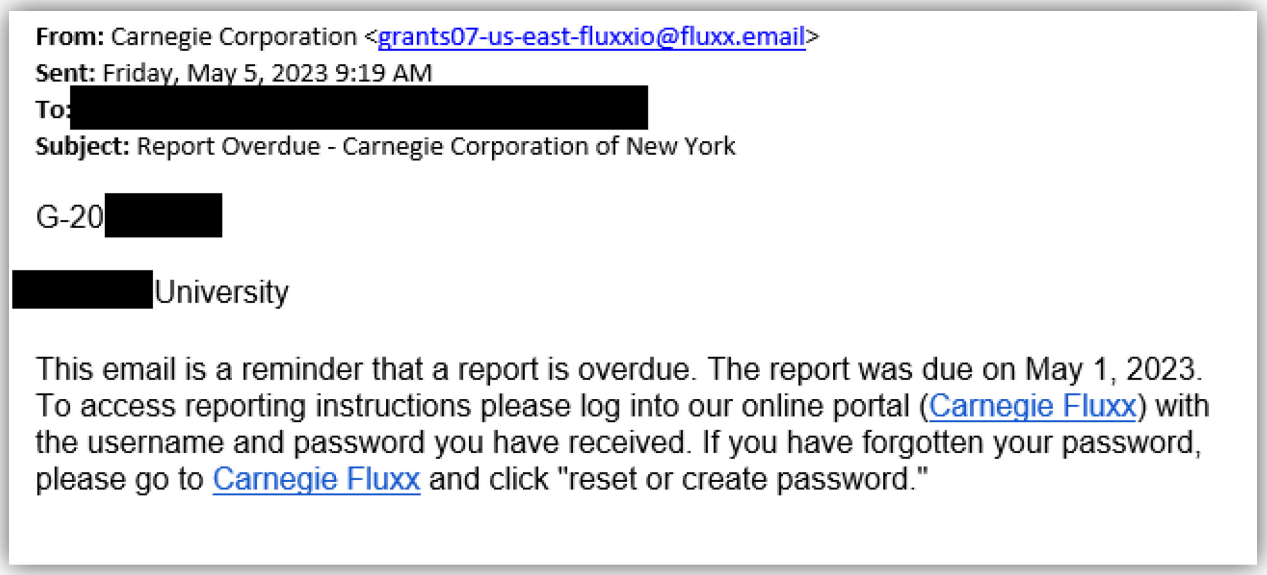
Director of IT *2006 - 2008*
IT Manager *2000 - 2006*

EDUCATION

The Cooper Union - Albert Nerkin School of Engineering **2000**

Bachelor of Science, Engineering

EXHIBIT 2



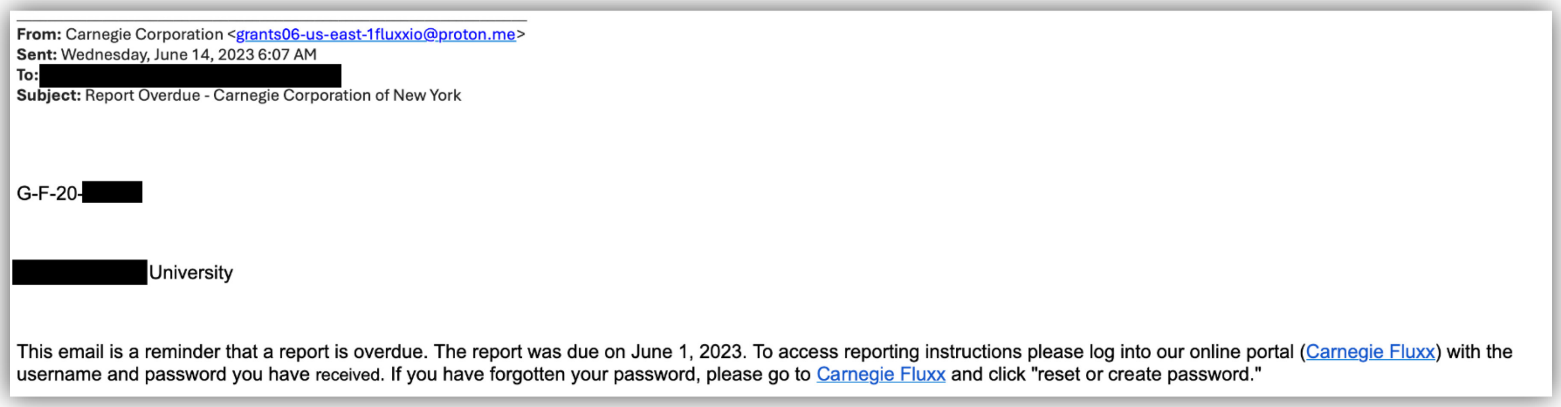
From: Carnegie Corporation <grants07-us-east-fluxxio@fluxx.email>
Sent: Friday, May 5, 2023 9:19 AM
To: [redacted]
Subject: Report Overdue - Carnegie Corporation of New York

G-20[redacted]

[redacted] University

This email is a reminder that a report is overdue. The report was due on May 1, 2023. To access reporting instructions please log into our online portal (Carnegie Fluxx) with the username and password you have received. If you have forgotten your password, please go to Carnegie Fluxx and click "reset or create password."

Image 1.



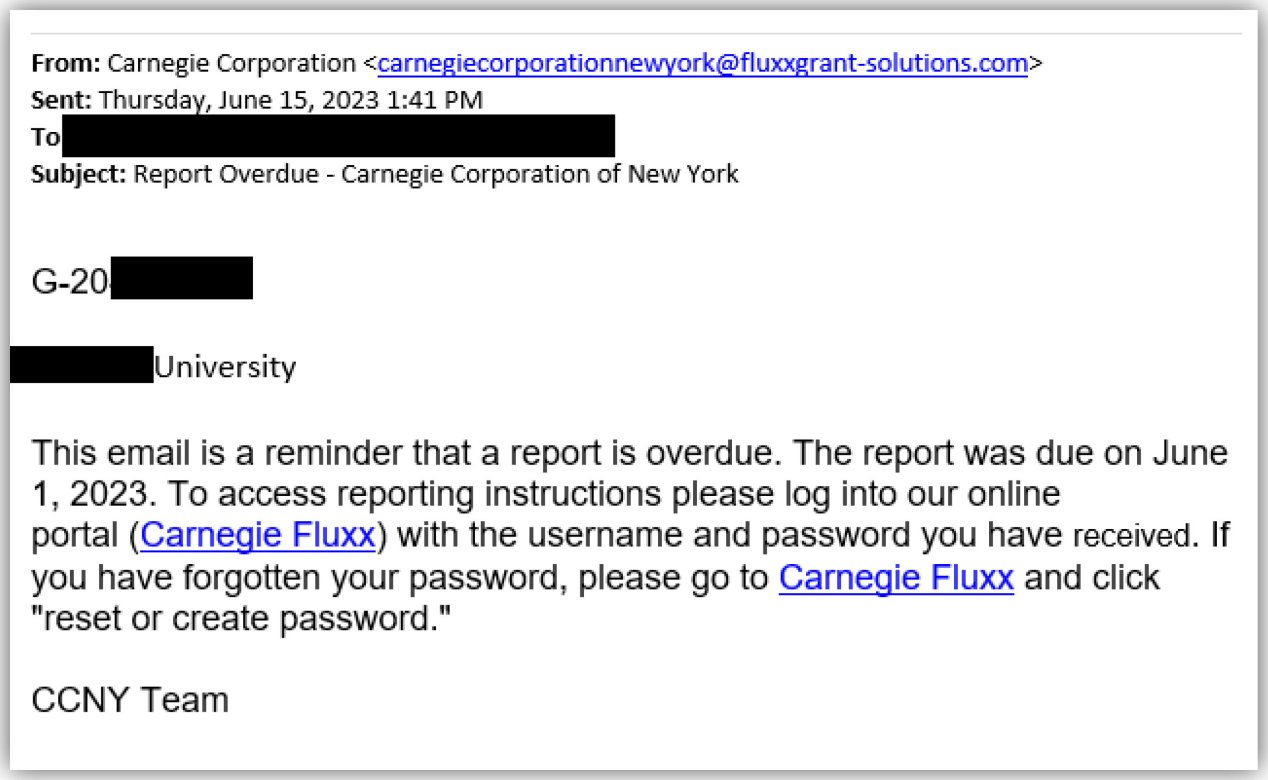
From: Carnegie Corporation <grants06-us-east-1fluxxio@proton.me>
Sent: Wednesday, June 14, 2023 6:07 AM
To: [redacted]
Subject: Report Overdue - Carnegie Corporation of New York

G-F-20-[redacted]

[redacted] University

This email is a reminder that a report is overdue. The report was due on June 1, 2023. To access reporting instructions please log into our online portal (Carnegie Fluxx) with the username and password you have received. If you have forgotten your password, please go to Carnegie Fluxx and click "reset or create password."

Image 2.



From: Carnegie Corporation <carnegiecorporationnewyork@fluxxgrant-solutions.com>
Sent: Thursday, June 15, 2023 1:41 PM
To [redacted]
Subject: Report Overdue - Carnegie Corporation of New York

G-20[redacted]

[redacted]University

This email is a reminder that a report is overdue. The report was due on June 1, 2023. To access reporting instructions please log into our online portal (Carnegie Fluxx) with the username and password you have received. If you have forgotten your password, please go to Carnegie Fluxx and click "reset or create password."

CCNY Team

Image 3.

From: Carnegie Corporation <grants06+2Dus+2Deast+2D1fluxxio=proton.me@bf01.eu1.hubspotfree.net>
August 7, 2023 1:44 AM
To: [redacted]
Subject: Report Overdue - Carnegie Corporation of New York

G-20-[redacted]

[redacted]

Dear [redacted]

This email is a reminder that a interim report is overdue. The report was due on August 1, 2023. To access reporting instructions please log into our online portal (Carnegie Fluxx) with the username and password you have received. If you have forgotten your password, please go to Carnegie Fluxx and click "reset or create password."

Image 4.