

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

UNITED STATES OF AMERICA	:	
	:	
v.	:	CRIMINAL NO. 23-cr-239 (CKK)
	:	
ILYA LICHTENSTEIN, <i>et al.</i>,	:	
	:	
Defendants.	:	

**CONSENT MOTION FOR ORDER AUTHORIZING ALTERNATIVE
NOTIFICATION PROCEDURES OUT OF AN ABUNDANCE OF CAUTION**

The United States of America, by and through the United States Attorney for the District of Columbia, respectfully moves this Court for an Order authorizing the government to use reasonable alternative notification procedures pursuant to 18 U.S.C. § 3771(d)(2). The government is seeking to notify the public regarding the offenses to which the defendants have pled guilty to permit any person who claims status as a potential crime victim to assert any rights under the Crime Victims’ Rights Act (CVRA), 18 U.S.C. § 3771. The government is not aware of any person who qualifies as a victim under the CVRA or for restitution under the MVRA, beyond perhaps Bitfinex, the Victim Virtual Currency Exchange (“VICTIM VCE”), but seeks such relief out of an abundance of caution, in order to provide notice to members of the public—in particular, to former accountholders of the Victim VCE—and to give them an opportunity to advance potential claims for victim rights and/or restitution under the CVRA, Mandatory Victim Restitution Act (MVRA), and related statutes.¹

¹ Because the offenses of conviction are 18 U.S.C. § 1956(h) (Money Laundering Conspiracy) and 18 U.S.C. § 371 (Conspiracy to Defraud the United States), the government’s position is that such individuals are not “victims” under the CVRA or for restitution purposes. The Court, however, may elect to allow individuals to submit comments for sentencing.

Counsel for the defendants have been consulted about this motion. Defendant Ilya Lichtenstein and Defendant Heather Rhiannon Morgan do not oppose the motion and maintain that the only potential victim for CVRA or MVRA purposes, if any, is Bitfinex.

PROCEDURAL HISTORY

The defendants, Ilya Lichtenstein and Heather Rhiannon Morgan, were charged by criminal complaint on February 7, 2022, with violations of 18 U.S.C. § 1956(h) (Money Laundering Conspiracy) and 18 U.S.C. § 371 (Conspiracy to Defraud the United States). These charges relate to a hack into the Bitfinex virtual currency exchange, the VICTIM VCE, resulting in the theft of approximately 119,754 Bitcoin (BTC) in August 2016. On August 3, 2023, Defendant Lichtenstein pled guilty to one count of Money Laundering Conspiracy, in violation of 18 U.S.C. § 1956(h), and Defendant Morgan pled guilty to one count of Money Laundering Conspiracy, in violation of 18 U.S.C. § 371, and one count of Conspiracy to Defraud the United States, in violation of 18 U.S.C. § 371. Sentencing is scheduled for November 14, 2024 (Lichtenstein) and November 15, 2024 (Morgan).

BACKGROUND REGARDING THE HACK AND THEFT

Before the conspiracy to launder money and the related offense—that is, the offenses to which defendants pled guilty—as alleged in the criminal complaint, and as agreed to in the Statement of Offense filed in connection with the plea agreements, beginning in or around late winter and early spring of 2016, Lichtenstein knowingly and willingly devised a scheme to defraud VICTIM VCE by means of materially false or fraudulent pretenses, representations, or promises - that is, the hack of VICTIM VCE. Lichtenstein conducted online research and reconnaissance of the computer infrastructure used by VICTIM VCE. While physically located in the United States,

Lichtenstein identified and compromised computer servers belonging to VICTIM VCE outside the United States.

Lichtenstein ultimately gained access to the private keys, or credentials, used to authorize transactions involving virtual currencies held by VICTIM VCE. In or about August 2016, Lichtenstein used his access to VICTIM VCE's private keys to fraudulently authorize more than 2,000 transactions in which approximately 119,754 BTC was transferred from VICTIM VCE's wallets to an outside wallet ("Wallet 1CGA4s") under Lichtenstein's custody and control. At the time of the hack, the stolen virtual currency was valued at approximately \$71 million.

During the reconnaissance phase of the hack of VICTIM VCE, Lichtenstein gained unauthorized access to VICTIM VCE's customer login credentials. Lichtenstein used these customer credentials to engage in credential spraying—that is, using the customer credentials stolen from VICTIM VCE to attempt to log into other accounts—targeting user accounts at other virtual currency exchanges. As a result of these efforts, Lichtenstein fraudulently obtained access to customer accounts at a second virtual currency exchange, "VCE A," and stole an estimated several hundred thousand dollars' worth of funds from VCE A customer accounts. Lichtenstein commingled these funds with the funds stolen from VICTIM VCE.

BACKGROUND REGARDING VICTIM VCE'S RESPONSE TO THE THEFT

According to information provided by the VICTIM VCE, after the hack and theft of funds, VICTIM VCE (through its parent company, iFinex Inc. (iFinex)) allocated the losses from the hack across all customer accounts. This resulted in an approximately 36% reduction in account value across all accounts. In exchange, VICTIM VCE issued tokens called "BFX" tokens to customers at a ratio of one BFX token for each \$1 of loss. According to iFinex, as well as public reporting in or around late 2016 and early 2017, customers holding BFX tokens then had the choice

of (1) selling their BFX tokens on the secondary market for the prevailing market price, (2) redeeming their BFX tokens for a cash payment from Bitfinex, at a rate of \$1 per BFX token, or (3) exchanging their BFX tokens for shares of the capital stock in iFinex, again valuing BFX tokens at \$1 per token. Any customers who chose to exchange their BFX tokens for iFinex stock also received, in addition to the iFinex stock, new tokens called Recovery Right Tokens (RRTs), with each RRT redeemable for up to \$1 of recovered stolen funds, in the event sufficient funds were ever recovered.

In short, according to iFinex, all customers on VICTIM VCE's platform immediately following the hack had the same options: sell their BFX tokens on the market or back to VICTIM VCE for cash or exchange their BFX tokens for iFinex stock plus the possibility of getting \$1 in recovered funds per RRT token. All customers holding BFX tokens chose to exercise one of those options, and as of April 3, 2017, all BFX tokens were fully redeemed. In other words, according to iFinex, within eight months of the hack, all customers holding BFX tokens had sold those tokens, redeemed them for cash from VICTIM VCE at 100 cents on the dollar, or exchanged them for iFinex stock plus RRTs. There are currently approximately 30 million RRT tokens outstanding, so iFinex has indicated that approximately \$30 million of any recovered funds would be used by iFinex to redeem those RRT tokens in full.

According to information provided by counsel for iFinex, iFinex believes that it is the sole victim with sustained financial losses from the hack.

DISCUSSION

The CVRA provides certain rights to victims in federal criminal proceedings. The CVRA defines a "crime victim" in relevant part as "a person directly and proximately harmed as a result of the commission of a Federal offense." 18 U.S.C. § 3771(e)(2)(A). This definition is offense-

specific. “[I]n determining whether one qualifies as a victim, a sentencing court can only consider the offense or offenses for which the defendant was convicted.” *United States v. Battista*, 575 F.3d 226, 231 (2d Cir. 2009); *see also In re McNulty*, 597 F.3d 344, 351 (6th Cir. 2010) (“The CVRA ‘instructs the district court to look at the offense itself only to determine the harmful effects the offense has on parties.’”) (quoting *In re Stewart*, 552 F.3d 1285, 1289 (11th Cir. 2008)).² In other words, the Court must look to the offense of conviction in order to determine who qualifies as a “victim” for purposes of the CVRA’s notice, right to be heard, and other crime victims’ rights provisions.

In this case, *for CVRA purposes*, the government’s position is that there are no “victims” of the offenses of conviction. The defendants were convicted of Money Laundering Conspiracy (in violation of 18 U.S.C. § 1956(h) for defendant Lichtenstein, and in violation of 18 U.S.C. § 371 for defendant Morgan) and Conspiracy to Defraud the United States (in violation of 18 U.S.C. § 371 for defendant Morgan). Neither defendant was convicted of the underlying intrusion into VICTIM VCE’s network or the theft of cryptocurrency therefrom, as those acts were committed in 2016 and were time-barred when the government brought charges in 2022. Thus, at least under the circumstances here, neither the VICTIM VCE nor its accountholders were “directly and proximately harmed,” 18 U.S.C. § 3771(e)(2)(A), by the conduct underlying the counts of

² Similarly, the MVRA defines “victim” in offense-specific terms as “a person directly and proximately harmed as a result of the commission of an offense for which restitution may be ordered including, in the case of an offense that involves as an element a scheme, conspiracy, or pattern of criminal activity, any person directly harmed by the defendant’s criminal conduct in the course of the scheme, conspiracy, or pattern.” 18 U.S.C. § 3663A(a)(2). *See United States v. Benns*, 740 F.3d 370, 377 (5th Cir. 2014) (“[R]estitution to victims of the offense . . . can encompass only those losses that results directly from the offense for which the defendant was convicted.”); *United States v. Lutz*, 237 Fed. Appx. 849, 852 (4th Cir. 2007) (“it is the ‘offense of conviction,’ not the ‘relevant conduct,’ that must be the cause of losses attributable as restitutionary liability”) (quotation, citation omitted); *United States v. Murry*, 395 F.3d 712, 721 (7th Cir. 2005) (“restitution may not be ordered for relevant conduct”).

conviction, that is, defendants' laundering conduct or their conspiracy to defraud U.S. government agencies.

That said, even if a "person" does not meet the definition of "victim" under the CVRA, a sentencing court may still receive victim impact statements at sentencing from that person. *See, e.g., United States v. Fata*, 650 F. App'x 260, 265 (6th Cir. 2016) (holding that the district court had discretion to consider oral and written statements from the defendant's patients, whose status as "victims" had not been determined, at a sentencing for health care fraud); *United States v. Weiner*, 518 F. App'x 358, 367 (6th Cir. 2013) (finding that the testimony of the mother of a victim of unrelated and uncharged sexual assault was relevant to the background, character, and conduct of the defendant regardless of whether she was technically a "victim" under the CVRA); *United States v. Ortiz*, 636 F.3d 389, 393–94 (8th Cir. 2011) (holding that the district court properly permitted merchants' statements as to retail theft losses suffered nationwide in an organized shoplifting scheme because limiting statements to the scope of the offense "would deprive the district courts of information which could aid them in determining whether to vary from the Guidelines based upon policy considerations"); *United States v. Spiwak*, 377 F. App'x 319, 323 (4th Cir. 2010) (per curiam) (finding no error in the government presenting prior sexual abuse victim's testimony to support upward departure in child pornography possession case, even though witness was not a victim under the CVRA).

Because the Court may still hear from those who do not meet the statutory definition of "victim" in the CVRA, the government is filing this motion out of an abundance of caution. In this case, there are potentially thousands of VICTIM VCE accountholders whose accounts lost value in 2016 as a result of this hack. The government has attempted to locate those victims, including by requesting a list of all accountholders from VICTIM VCE, but such efforts have been

unsuccessful. Under analogous circumstances, the CVRA recognizes that for crimes involving multiple victims and where individual notification is “impracticable,” the Court has discretion to adopt procedures to accord victim rights without unduly interfering with the criminal proceedings:

In a case where the court finds that the number of crime victims makes it impracticable to accord all of the crime victims the rights described in subsection (a), the court shall fashion a reasonable procedure to give effect to this chapter that does not unduly complicate or prolong the proceedings.

18 U.S.C. § 3771(d)(2). The CVRA places no limitations on the alternative procedures that a Court may fashion other than requiring that the procedures be reasonable to effectuate the Act and not unduly complicate or prolong the proceedings. *Id.*; *United States v. Bondarenko*, No. 2:17-CR-306-JCP-PAL, 2018 WL 1413972, at *2 (D. Nev. 2018).

District courts have discretion to determine what is a “reasonable procedure” under the CVRA. *In re W.R. Huff Asset Mgmt. Co.*, 409 F.3d 555, 563 (2d Cir. 2005) (“Most of the rights provided to crime victims under the CVRA require an assessment of ‘reasonableness’” and “[t]he district court is far better positioned to make these assessments and to determine what constitutes ‘a reasonable procedure’ for effecting these rights than a court of appeals.”) (citations omitted); *see United States v. Schessel*, No. CR 22-0374 (ES), 2022 WL 17094777, at *2 (D.N.J. Nov. 21, 2022). “Reasonable procedure” determinations thus may vary with each case given a district court's “‘proximity to the particular facts and needs of victims that also will likely vary with each case.’” *Schessel*, 2022 WL 17094777 at *2; (quoting *United States v. Rubin*, 558 F. Supp. 2d 411, 422 (E.D.N.Y. 2008); citing *In re Huff*, 409 F.3d at 562–63).

Justification for Proposed Alternative Notification Procedure

In this case, although VICTIM VCE and several individuals and groups of accountholders have come forward to self-identify as victims, the government does not know the identity or

contact information for all VICTIM VCE accountholders. Accordingly, the government proposes to use—with the Court’s permission—the Department of Justice’s website for large cases, <http://justice.gov/largecases>, to direct potential individuals claiming such status to a case-specific website where all required notices would be posted. The case-specific website would contain the notices required under the Act and provide people with the opportunity to complete a statement to relay information about how they may have been harmed by the conduct and/or offenses here. On entry of the proposed order, the United States also would issue a press release informing individuals and entities who believe that they may be victims to access the Department of Justice website for more information.

Ample precedent exists to use alternative notification procedures under the CVRA in such a situation. Courts have routinely allowed the United States to use similar alternative methods to notify potential victims in cases where the government could not determine precisely which entities and individuals would qualify as victims under 18 U.S.C. § 3771(d)(2) and where large numbers of such potential victims were involved. *See, e.g., United States v. Penn*, No. 20-CR-00152-PAB, 2020 WL 4057589, at *1 (D. Colo. July 20, 2020) (finding that alternative notification procedures were appropriate and granting government’s motion to notify victims pursuant to the CVRA via the Justice Department’s website in case involving thousands of victims); *Bondarenko*, 2018 WL 1413972 at *2 (granting government’s motion to notify victims pursuant to the CVRA via the Justice Department’s website in case involving the “large-scale trafficking of compromised credit card data”); *United States v. Babich*, 301 F. Supp. 3d 213, 217–18 (D. Mass. 2017) (granting in part government request for alternative notification procedures in healthcare fraud prosecution but restricting information repeating allegations in pleadings); *United States v. Merrill*, No. 14-40028-TSH, 2014 WL 6387368, at *2 (D. Mass November 14, 2014) (similar); *United States v.*

Saferstein, No. 07-CR-557, 2008 WL 4925016, at *3–4 (E.D. Pa. November 18, 2008) (finding publication of notice in national newspaper and through a government website to be “reasonable procedures” under the CVRA).

Here, despite the government’s position that, for CVRA and MVRA purposes, such individual accountholders could not be considered “victims” of the offenses of conviction, out of an abundance of caution, the government nonetheless requests such notice to permit such persons to raise any claims to CVRA status or restitution under the MVRA should they choose to do so in advance of the sentencing.

CONCLUSION

Accordingly, the United States respectfully requests that the Court authorize the use of alternative notification methods, out of an abundance of caution.

Respectfully submitted,

MATTHEW M. GRAVES
United States Attorney
D.C. Bar No. 481052

By: /s/CHRISTOPHER B. BROWN
Christopher B. Brown, D.C. Bar No. 1008763
Special Assistant United States Attorney
Jolie F. Zimmerman, D.C. Bar Number 465110
Assistant United States Attorney
United States Attorney’s Office for the District of
Columbia
601 D Street, N.W.
Washington, DC 20530
(202) 252-7220 (Zimmerman)
Jolie.Zimmerman@usdoj.gov
(202) 353-0018 (Brown)
Christopher.Brown8@usdoj.gov

C. Alden Pelker, Maryland Bar
Jessica Peck, N.Y. Bar Number 5188248
Trial Attorneys

U.S. Department of Justice Computer Crime &
Intellectual Property Section
1301 New York Ave., N.W., Suite 600
Washington, D.C. 20005
(202) 616-5007 (Pelker)
(202) 353-9455 (Peck)
Catherine.Pelker@usdoj.gov
Jessica.Peck@usdoj.gov