

**UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS**

UNITED STATES OF AMERICA)	
)	
v.)	Criminal No. 09-10382-DPW
)	
ALBERT GONZALEZ,)	
)	
Defendant)	

**MEMORANDUM OF COMPANY A IN SUPPORT OF MOTION TO INTERVENE
UNDER CRIME VICTIMS’ RIGHTS ACT, 18 U.S.C. § 3771, FOR THE
LIMITED PURPOSE OF SEEKING ENTRY OF PROTECTIVE ORDER AND TO SEAL**

Pursuant to the Crime Victims’ Rights Act, 18 U.S.C. § 3771(a)(8) and (d)(1), and Local Rules 7.1 and 7.2, Company A, a victim of the criminal activity alleged in this case, hereby respectfully submits this memorandum in support of its motion to intervene for the limited purpose of seeking a protective order that prohibits the District of Massachusetts, a transferee district under Rule 20, Fed. R. Crim. P., and the defendant from publicly identifying Company A in this matter. Company A also respectfully requests that it be heard by the Court on the proposed protective order and that Company A’s submissions in this matter be sealed.

I. INTRODUCTION AND FACTS¹

This case originated in the District of New Jersey. With respect to Company A, the government alleges that more than two years ago – October 23, 2007 – it “was the victim of a SQL Injection Attack the resulted in the placement of malware on its network.” Indictment, ¶ 1(l). In the Indictment, Company A and another entity, Company B, are identified only by pseudonym. *Id.* at ¶ 1(m). In both cases, there is no allegation by the government that any customer data was taken from either company. Conversely, for all of the companies that were

¹ These facts are based on public filings and Declaration of Kevin G. Walsh, submitted herewith.

publicly identified in the Indictment, the government alleges that in addition to the malware being placed on their systems, customer credit and debit card numbers and data was stolen, and thus customers were victimized. *Id.*, ¶¶ 1(i)-(k).

As this reflects, the District of New Jersey, the district in which brought this case, decided not to publicly identify Company A in response to Company A's request pursuant to the Crime Victims' Rights Act because there was no evidence that customers of Company A were harmed as the result of the criminal activity alleged in this case. Thus, the only victim with respect to the crimes committed against Company A, and which thus has a protectable privacy right under the Crime Victims' Rights Act, was Company A. See 18 U.S.C. § 3771(e)(defining "crime victim" as "a person directly and proximately harmed as the result of the commission of a Federal offense"); § 3771(a)(8)(crime victim has the "right to be treated ...with respect for the victim's...privacy"). Non-disclosure of Company A's identity was thus a considered decision by the Department of Justice, which reached it after lengthy discussions with Company A and its counsel; one of several reasons it agreed not to disclose Company A's identity publicly was that there was no evidence that Company A's customers' credit card data had been "exfiltrated" to computer servers controlled by defendant Gonzalez and his co-conspirators.

And it was a decision that was honored by the Department; the United States Attorney in New Jersey did not disclose Company A in the Indictment, in its subsequent public statements or subsequent filings. See District of New Jersey Press Release, "Three Men Indicted for Hacking into Five Corporate Entities, including Heartland, 7-Eleven, and Hannaford, with Over 130 Million Credit and Debit card Numbers Stolen," August 17, 2009 (in addition to the named victims, "the Indictment describes two unidentified corporate victims as being hacked by the coconspirators"). Further, no corporate disclosure under Rule 12.4 was filed in the District of

New Jersey. The government went so far as to agree with Company A that it would enter into a protective order with Mr. Gonzalez to protect the Company's information produced to the defendant in discovery from improper disclosure. Not surprisingly, despite some speculation in the "blogosphere,"² there has been no wide press publication of Company A's identity, largely because there has been no disclosure of it by the most authoritative source, the government.

Until now. Solely as the result of the transfer of this case to this district for plea and disposition, the Department of Justice now has reversed course and abrogated the agreement reached in New Jersey. Company A has been informed by the government that it intends to disclose Company A's identity in an in camera Rule 12.4 submission in this case, and will request that the seal over that filing expire on or about January 5, 2010.³ As Company A understands it, the government's rationale is that the public has the right to know that Company A, two years ago, was attacked, regardless of the opposite decision reached by a sister district. The government's view is fundamentally flawed, for at least three reasons.

First, this District does not write on a clean slate. The District of New Jersey agreed to forbear from publicly disclosing Company A's identity, evidently interpreting the government's obligation under the Crime Victims' Rights Act to make "best efforts" to protect Company A's

² There is evidently a lone blogger who has accurately reported Company A's identity. See <http://www.storefrontbacktalk.com/securityfraud/j-c-penney-target-added> (August 2009), <http://www.storefrontbacktalk.com/securityfraud/gonzalez-pleads-guilty-a> (December 2009). However, neither the government nor Company A has either confirmed or denied this fact. Perhaps unsurprisingly, the blogger's claims have not been widely reported. Indeed, a recent Boston Globe article about Gonzalez's expected plea discusses the New Jersey case but does not repeat the allegations about Company A's identity. See Boston Globe, December 22, 2009, "Hacker's Sentence is Likely to be 17 to 25 Years," page B9. More importantly, it is one thing for a blogger to repeat speculation on the internet; it is quite another for the United States to suddenly disclose a victim's identity after having previously maintained under seal. The latter will surely garner wide press attention.

³ Company A's repeated efforts to dissuade the government from doing so have been fruitless.

privacy to demand such treatment. See 18 U.S.C. § 3771(c)(1). The government in the District of Massachusetts has offered no cogent reason for its abrupt disavowal of that agreement, or why “best efforts” to preserve Company A’s privacy now means no effort at all. Reversing course and disclosing Company A now is not required under Rule 12.4 and would certainly undermine one of the purposes of Rule 20, which is to promote efficiency by effecting transfers of cases solely for plea and disposition, and not to undermine that efficiency by inviting reconsideration or re-litigation of issues such as this.

Second, the government’s about-face ignores Company A’s legitimate privacy interest in this case. The attack alleged here took place in 2007. The District of New Jersey issued a Grand Jury subpoena to Company A in or about late May 2009 – and obtained an Indictment in or about August 2009, electing all along not to inform the public, which was unharmed by the alleged crime, about the true identity of Company A. As the District of New Jersey recognized, Company A had a compelling interest in avoiding public exposure linking it with those companies that the government alleged lost customer data as the result of the largest computer intrusion case in history. There was thus no need to alarm cardholders and shareholders about a risk that did not occur. Nothing suggests that the balance between the public’s right to know and Company A’s interests has changed in the few weeks since this case arrived in Massachusetts from New Jersey. On the contrary, the passage of time in this case, where the alleged attack took place two years ago, shows that the balance is more firmly in Company A’s favor. Disclosure now will not arm consumers with timely data, but will cause confusion and alarm, and will result in the very harm that the District of New Jersey saw fit to forego visiting upon Company A.

Third, it is not as if Company A seeks to impose a new, broad-brush policy of its own making in this District. The policy behind its claim here was announced by Congress in the

Crime Victims' Rights Act and followed by the District of New Jersey. Further, it is a policy of protecting victim's rights that has also been followed by this District in other cases. In the District of Massachusetts' Gonzalez case, for instance, the government made a Rule 12.4 filing on September 11, 2008 in which it declined to publicly identify "numerous other businesses, which have not yet been publicly identified," offering to provide the court with "an in camera submission listing these entities" in the event the court "so desire[d]." Rule 112.4 Corporate Disclosure Statement, 08-CR-10233-PBS, Dkt. No. 8 (September 11, 2008). The government in this District has protected the identity of other victims under § 3771, as well. See United States v. Robinson, Cr. No. 08-10309-MLW, 2009 WL 137319 (D. Mass. Jan. 20, 2009) (government successfully resisted motion to disclose identity of businessman who was extorted following a sex-for-fee relationship). Disclosing Company A's identity here, after the District of New Jersey decided not to do so, may discourage other victims of cybercrimes to report the criminal activity or cooperate with enforcement officials for fear of the retribution and reputational damage that may arise from a policy of disclosure as espoused by the government in this case. Therefore, Company A's limited intervention and the protective order it seeks are both necessary and proper.

II. ARGUMENT

A. As A Victim Under The Crime Victims Rights Act, Company A's Limited Intervention Is Appropriate

Company A is identified In the Indictment as a victim of the computer crime alleged in this case. Indictment, ¶ 1(l). The Crime Victims' Rights Act provides Company A not only the right to privacy but also the authority to assert that right and the others set forth in the Act and to "be reasonably heard at any public proceeding in the district court involving ... plea [or] sentencing." 18 U.S.C. § 3771(a)(4), (d)(1).

Company A should be entitled to intervene in this action because it is otherwise “powerless to avert the mischief” arising from the disclosure of its identity. See United States v. Doe, 455 F.2d 753, 756-57 (1st Cir. 1972) (quoting Perlman v. United States, 247 U.S. 7, 13 (1918)). Although the Crime Victims’ Rights Act is silent as to the applicable procedure by which a victim is to protect its rights, this Court has permitted victims in criminal cases to intervene by motion to protect privacy interests. See Robinson, 2009 WL 137319, at *1 (permitting victim to intervene pursuant to 18 U.S.C. § 3771 to oppose motion seeking to disclose victim’s identity instead of continuing use of pseudonym); see also United States v. Doe, 332 F. Supp. 930, 932 (D. Mass. 1971) (permitting intervention of third party in criminal proceeding where subpoena was directed to another party), aff’d 455 F.2d at 756-57, vacated and remanded on other grounds sub nom., Gravel v. United States, 408 U.S. 606, 608 n.1 (1972).

This is consistent with those cases that have recognized the rights of third parties to protect confidential business information in criminal cases. See United States v. RMI Co., 599 F.2d 1186, 1190 (3d Cir. 1979). In such cases, federal courts have held “it is settled law that persons affected by the disclosure of allegedly privileged materials may intervene in pending criminal proceedings and seek protective orders.” Id. at 1186; see also United States v. Crawford Enters., Inc., 735 F.2d 174, 1176 (5th Cir. 1984) (“persons or corporations which are adversely affected by the disclosure of privileged material have the right to intervene, assuming standing, in pending criminal proceedings to seek protective orders,” citing RMI Co.); United States v. Cuthbertson, 651 F.2d 189, 193, 194 (3d Cir. 1981) (a “third party may intervene in a criminal trial to challenge production of subpoenaed documents,” citing RMI Co.). Federal courts have recognized that where the government loses interest in the continued secrecy of privileged information, as it has here, public policy favors the right of the non-party to protect its own

interests. RMI Co., 599 F.2d at 1190 (“even when the executive branch loses interest in continued secrecy, other societal interests ... remain”); United States v. Feeney, 641 F. 2d 821, 824 (10th Cir. 1981) (holding non-party had a “right to intervene to protect his interests” in criminal action and to seek protective order, relying on RMI Co.).

The RMI Co. court explained that prohibiting a witness who furnished documents to a grand jury from objecting to the subsequent production of the documents would inevitably lead to greater resistance from subpoenaed witnesses and would violate the witness’s property rights in confidential business information. RMI Co., 599 F.2d at 1190. The same concerns exist here. Precluding Company A from intervening in this action would only deter future corporate victims from cooperating in criminal investigations and violate Company A’s property and privacy rights. As described more fully below, Company A has an interest that is worthy of protection and, now that the government has decided not to honor the agreement Company A reached with the District of New Jersey to maintain the confidentiality of Company A’s identity, there is no party in this action which adequately represents – or, in fact, represents at all – Company A’s interests.

Thus, Company A should be permitted to intervene for the sole purpose of seeking a protective order as contemplated by the protections found in 18 U.S.C. § 3771.

B. Entry Of A Protective Order Is Appropriate Where, As Here, The Public Interest To Access Is Outweighed By The Victim’s Privacy Interest

Continuing to protect Company A’s privacy interests outweighs the public’s right to know, and, therefore, a protective order should be entered that prohibits the government and the defendant from publicly identifying Company A in this matter.

Company A is a crime victim, entitled a right of privacy. 18 U.S.C. §3771(a)(8). The government has an obligation under that statute to use best efforts to protect that right. 18 U.S.C.

§ 3771(c)(1). In New Jersey, it did so. Massachusetts has decided to cease doing so. Nothing explains why non-disclosure was seen by the Department as appropriate under the statute, but now, simply because of a change in venue, it is not. Cf. United States v. Goldfaden, 959 F.2d 1324, 1328 (5th Cir. 1992) (“[t]he failure of the Government to fulfill its promise, therefore, affects the fairness, integrity, and public reputation of judicial proceedings”). Indeed, no Massachusetts-specific concerns have been identified, such as victimized customers in this district. Certainly Rule 12.4 does not mandate this result. Rule 12.4 requires the government to file a disclosure of corporate organizations that are victims for the purpose of “assist[ing] judges in determining whether they must recuse themselves because of a ‘financial interest in the subject matter in controversy.’” See Notes, Rule 12.4, Fed. R. Crim. P. Filing such a disclosure with the Court in camera, as Company A requests this District do, and maintaining it under seal is completely appropriate and fulfills the purposes of the Rule. Indeed, this District did just that for other corporate victims in a prior filing in its own Gonzalez prosecution.

Moreover, prohibiting disclosure of Company A’s identity is appropriate where, as here, “the right to access is outweighed by the interests favoring non-disclosure.” United States v. Salemme, 985 F.Supp. 193, 195 (D. Mass. 1997). “Among the countervailing factors favoring non-disclosure are: (i) prejudicial pretrial publicity; (ii) the danger of impairing law enforcement or judicial efficiency; and (iii) the privacy interests of third parties.” United States v. Salemme, 985 F.Supp. 193, 195 (D. Mass. 1997); see also United States v. Madoff, 626 F.Supp.2d 420 (S.D.N.Y. 2009) (refusing to unseal identifying information concerning victims because their significant privacy interests outweighed the public’s right to know). A similar balancing analysis is followed in the D.C. Circuit regarding the analogous circumstance of disclosing confidential documents. That test, which is useful here, looks to (1) the need for public access to

the documents at issue; (2) previous public access to the documents; (3) fact of objection and identity of those objecting to disclosure; (4) strength of generalized property and privacy interests asserted; (5) possibility of prejudice to the defendant; (6) the purposes for which the documents were introduced. United States v. Hubbard, 650 F.2d 293, 317-21 (D.C.D.C. 1981) (holding third party's documents should have remained sealed).

These standards manifestly support non-disclosure of Company A's identity. Because there is no evidence that customer information was stolen by Gonzalez's alleged intrusion into Company A, there is no need or purpose in divulging the identity of the victim to the public. The public has not been granted access to Company A's identity; there is nothing but unsubstantiated speculation by a lone blogger about Company A's identity, and critically no government confirmation of those (accurate) allegations. The victim, Company A, has objected to the disclosure of its identity from the outset – an objection to which the government has acceded. And, most importantly, Company A's privacy interests are strong – disclosure of Company A's identity would stigmatize Company A and cause unwarranted alarm for its customers and shareholders by erroneously suggesting that the government has concluded its customer data was stolen when it had not, and will likely cause anger that such allegations are being disclosed by the government now after having not been for so long. Indeed, such disclosure provides the public with no useful, current information. And there seems no real possibility of prejudice to the defendant in this case by the allowance of this motion, as he has been advised of Company A's identity by the government's filing.

The government in this District has protected the identity of other victims under § 3771. Most importantly, the government – in its own case against this same defendant for the same type of conduct – saw fit not to disclose corporate victims of Gonzalez's alleged criminal

conduct. Rule 112.4 Corporate Disclosure Statement, 08-CR-10233-PBS, Dkt. No. 8 (September 11, 2008). Further, it recently successfully resisted a motion to disclose identity of businessman who was extorted following a sex-for-fee relationship. See United States v. Robinson, Cr. No. 08-10309-MLW, 2009 WL 137319 (D. Mass. Jan. 20, 2009). Disclosing the identity of a victim like Company A disregards the victim's "privacy interests [which] are important" under § 3771, and "discourages similarly situated victims from cooperating with law enforcement." Robinson, 2009 WL 137319, at *3 (citing 18 U.S.C. § 3771(a)(8)).

While public disclosure is often important to the general integrity of judicial proceedings, exceptions exist, particularly where the identity of a victim is at issue. For example, in United States v. Patkar, No. 06-00250 JMS, 2008 WL 233062, at *1 (D. Haw. Jan. 28, 2008), the court denied a request by the Associated Press to disclose the identity of an extortion victim who had agreed to cooperate with law enforcement under a pseudonym. The court held that 18 U.S.C. § 3771(a)(8) provided the victim with an "unquestionable right to ... dignity and privacy," which right provided "good cause" for the court to honor the agreement the victim had made with the government and the defendant prohibiting the distribution of "materials that ... would cause damage to the reputation of the victim." Id. at *5. Similar concerns weigh in favor of protecting Company A's identity here by permitting its continued use of the pseudonym, as was the case in Robinson. See Robinson, 2009 WL 137319, at *3; Patkar, 2008 WL 233062, at *5.

Further, providing anonymity to a corporate victim of such an attack is a strong incentive for that company to voluntarily report such crimes and thereafter cooperate with the government in these difficult cases. See RMI Co., 599 F.2d at 1188, 1190 (explaining secrecy in grand jury proceedings is often essential to encourage cooperation and to protect the "property rights in confidential business information"); see also Douglas Oil Co. of Cal. v. Petrol Stops Nw., 441

U.S. 211, 218 (1979) (“the proper functioning of our grand jury system depends upon the secrecy of grand jury proceedings”); United States v. Proctor & Gamble Co., 356 U.S. 677, 681-82 (1958) (among the critical purposes of grand jury secrecy “is to encourage all witnesses to step forward and testify freely without fear of retaliation”); Illinois v. Abbott & Assocs., Inc., 460 U.S. 557, 566 n.11 (1983) (the need to protect the reputations of the innocent extends even after the conclusion of the particular grand jury’s investigation).

Lastly, disclosing Company A’s identity would effectively, and perhaps improperly, amend the Indictment by disclosing a fact that the District of New Jersey concluded should not be made public. United States v. Khan, 822 F.2d 451, 455 (4th Cir. 1987) (citation omitted) (“[t]he transfer is then purely for the purpose of imposing sentence. Subject matter jurisdiction is, thereby, shifted from the charging district to the transferee district for the narrow purpose envisioned in the rule,” therefore, “[a]ny determinations made by a Rule 20 transferee court beyond those necessary for the acceptance of the plea and imposition of sentence are without legal effect”). In any event, it would certainly undermine the efficiency that Rule 20 seeks to achieve by re-litigating issues that have already been decided by the transferor District.

III. CONCLUSION

For the foregoing reasons, Company A should be permitted to intervene for the limited purpose of proposing a protective order to prohibit either the government or the defendant from publicly disclosing Company A's identity, and that the government's disclosure made pursuant to Rule 12.4 be made in camera for this reason. Company A should also be heard by the Court regarding that proposed protective order, and these submissions should be sealed.

Respectfully submitted,

COMPANY A

By its attorneys,

/s/ Michael D. Ricciuti

Michael D. Ricciuti (BBO #550771)

Nicole D. Newman (BBO #674074)

K&L GATES LLP

State Street Financial Center

One Lincoln Street

Boston, MA 02111-2950

Tel. (617) 261-3100

Fax. (617) 261-3175

michael.ricciuti@klgates.com

nicole.newman@klgates.com

Dated: December 24, 2009

CERTIFICATE OF SERVICE

I hereby certify that this document was served via electronic mail this 24th day of December 2009:

Stephen P. Heymann, Esq.
United States Attorney's Office
1 Courthouse Way
Suite 9200
Boston, MA 02110
Stephen.heyman@usdoj.gov

Martin G. Weinberg
Martin G. Weinberg, PC
20 Park Plaza
Suite 1000
Boston, MA 02116
owlmcb@att.net

/s/ Michael D. Ricciuti
Michael D. Ricciuti