

**UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS**

UNITED STATES OF AMERICA)	
)	
v.)	Criminal No. 09-10382-DPW
)	
ALBERT GONZALEZ,)	<u>FILED UNDER SEAL</u>
)	
Defendant.)	

**MEMORANDUM OF COMPANY B IN SUPPORT OF MOTION TO INTERVENE
UNDER CRIME VICTIMS' RIGHTS ACT, 18 U.S.C. § 3771, FOR ENTRY OF A
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 B, a victim of the criminal activity alleged in this case, submits this memorandum in support of its motion to intervene and for a protective order prohibiting the United States Attorneys' Office for the District of Massachusetts (the "Massachusetts USAO"), a transferee district under Rule 20, Fed. R. Crim. P., and the defendant from publicly identifying Company B in this matter. Company B also respectfully requests that Company B's submissions in this matter be sealed and that, in the event the Court schedules a hearing on this matter, the hearing be conducted in camera.

Another similarly situated victim of the criminal activity alleged in this case, Company A, filed a motion to intervene and memorandum of law in support of that motion on December 28, 2009 (Dkt. Nos. 9-10).¹ Company B joins in the legal arguments set forth in Company A's memorandum of law and incorporates them by reference. Company B submits this

¹ In order to limit unnecessary and repetitive briefing, counsel for Company A provided a redacted copy of Company A's motion to intervene and memorandum of law to counsel for Company B. The redactions removed information that might identify Company A.

memorandum to provide the Court with relevant background information about Company B and to further highlight why, under the circumstances, the Court should continue to keep Company B's identity from being publicly disclosed.

I. BACKGROUND FACTS²

Company B is a publicly traded company and a major national retailer that processes credit and debit card payments of customer purchases through its computer network. Company B was identified in the Indictment in this matter, which was originally filed in the District of New Jersey, as “the victim of a SQL Injection Attack that resulted in the placement of malware on its network.” Indictment, ¶ 1(m). Like Company A, Company B was not identified by name, and there are no allegations that any customer data was taken from Company B. *Id.* ¶ 1(l).

Since May 2008, when Company B was first contacted by the government in connection with its investigation into the attack on Company B's computer system, Company B has fully cooperated with the government's investigation. In part because the government was not aware of any evidence that Company B's customers' credit or debit card data had been taken, the government employees who communicated with Company B assured Company B that they would do their best not to disclose the identity of Company B. Company B relied on these assurances and has not previously made any disclosures to its customers or shareholders regarding its identity as Company B, which disclosures Company B understood were unnecessary because Company B is not aware of any evidence that Company B's customers' information was taken in connection with the attack on Company B's computer system. To date, there has been no public disclosure of Company B's identity in connection with this matter.

² These facts are based on public filings and the attached Declaration of Ackneil M. (Trey) Muldrow, III.

See, e.g., 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”).

Despite this history, the Massachusetts USAO recently disclosed Company B’s identity in a partially sealed Rule 12.4 submission and requested that the submission be sealed only until January 5, 2010. If that seal is allowed to expire, Company B will suffer harm resulting from the confusion and alarm that will undoubtedly follow from the disclosure of Company B’s identity. Keeping the seal in place, on the other hand, will not harm others or deprive the public of any information necessary to alert potential victims because none of Company B’s customers’ credit or debit card information was stolen. Further, disclosure of Company B’s identity may deter victims from cooperating with the government in future investigations for fear of the retribution and reputational damage that may arise from a policy of disclosure for disclosure’s sake. Accordingly, Company B asks this Court for a protective order maintaining the government’s Rule 12.4 disclosure statement under seal and prohibiting the government or defendant from publicly disclosing Company B’s identity.

II. ARGUMENT

A. Company B’s Limited Intervention Is Appropriate To Protect Its Rights Under The Crime Victims Rights Act

As this Court recognized in granting Company A’s motion to intervene, the Crime Victims’ Rights Act provides Company B 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); see also Electronic Clerk Notes, United States v. Gonzalez, No. 09-cr-10382-DPW (D. Mass. Dec. 29, 2009). Similarly, other courts in this District have permitted victims in criminal cases – like Company B – 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). Here, intervention is necessary for Company B to protect its interests. Further, Company B’s counsel has contacted each of the parties represented in this action, and no party opposes Company B’s intervention. Company B, therefore, should be permitted to intervene for the limited purpose of seeking a protective order as contemplated by the protections found in 18 U.S.C. § 3771.

B. Company B’s Privacy Interest Outweighs Any Theoretical Public Interest In Access To Company B’s Identity, Entitling Company B To A Protective Order

As set forth in Company A’s memorandum of law, there is no justification for the Massachusetts USAO to abandon its sister jurisdiction’s practice of protecting Company B’s right to privacy in this prosecution. See 18 U.S.C. § 3771(a)(8), (c)(1). Maintaining Company B’s identity under seal will not undercut the purposes of Rule 12.4 – or any other Massachusetts-specific policy or practice – and, in fact, is consistent with the practice in the ongoing prosecution of this defendant that originated in this District. See Rule 112.4 Corporate Disclosure Statement, United States v. Gonzalez, No. 08-cr-10233-PBS (D. Mass. Sept. 11, 2008) (Dkt. No. 8).

Further, there is no public interest that outweighs Company B's right to privacy. See United States v. Salemme, 985 F. Supp. 193, 195 (D. Mass. 1997) (identifying factors that favor non-disclosure as: "(i) prejudicial pretrial publicity; (ii) the danger of impairing law enforcement or judicial efficiency; and (iii) the privacy interests of third parties"). Company B was the only victim in the defendant's attack on Company B's computer network. The attack did not result in any lost customer information or harm to anyone other than Company B. In other words, there is no third party who will in any way be affected by non-disclosure. Disclosure of Company B's identity at this stage, however, will likely cause unnecessary alarm for Company B's extensive customer base and its shareholders, and additional expenses for Company B to address these concerns, while providing no attendant public benefit.

Moreover, permitting the government to change its position at this time and disclose Company B's identity would be unnecessarily and unfairly prejudicial. Had the government not made the determination at the outset that Company B's identity would be kept confidential, Company B could have limited any reputational harm by making the disclosure itself at the time of the indictment. However, in reliance on the government's decision that Company B's identity would not be made public, it did not do so. The government should not now be able to reverse course and create a misleading impression that Company B is at fault for delaying disclosure.

In addition to the factual and policy reasons outlined above and in Company A's memorandum, the general policy of public disclosure under federal law safeguards other victims in this case, eliminating any danger that non-disclosure will harm victims in this or any other similar prosecution. Throughout this prosecution, the government has identified victims whose computer networks were attacked and from which customer information was stolen. Those potential victims and the public have been made aware of the risk of harm. This policy is

consistent with state laws that require companies to disclose unauthorized security breaches only when private information is actually acquired or used. See, e.g., Cal. Civ. Code § 1798.29(d) (defining a security breach as the “unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency”).³ State legislatures have considered when disclosure is necessary under identical circumstances and have determined that it is only necessary when there is a potential victim; not simply when an individual accesses a company’s computer system.

A policy of disclosure for disclosure’s sake serves no purpose and does not justify disclosure of Company B’s identity when such disclosure would result in no public benefit. Accordingly, continuing to protect Company B’s privacy interests outweighs any public interest in disclosure, and, therefore, a protective order should be entered prohibiting the government and the defendant from publicly identifying Company B in this matter.

III. CONCLUSION

For the foregoing reasons, Company B should be permitted to intervene for the purpose of proposing a protective order to prohibit either the government or the defendant from publicly disclosing Company B’s identity, the Court should grant the protective order and maintain the Government’s Rule 12.4 disclosure under seal. Company B also respectfully requests that, in the

³ Company B’s principal place of business is in California. Massachusetts law is consistent with California law. See M.G.L. c. 93H (defining a breach as “the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth”).

event the Court schedules a hearing on this matter, the hearing be conducted in camera and that Company B's submissions in this matter be sealed.

Respectfully submitted,

COMPANY B

By its attorneys,



Ben T. Clements (BBO #555802)
Clements & Pineault LLP
24 Federal Street
Boston, MA 02110
Tel. (857) 445-0133
Fax. (857) 366-5404
bclements@clementspineault.com

Dated: January 4, 2010

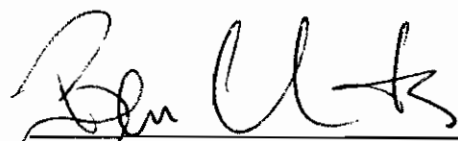
CERTIFICATE OF SERVICE

I hereby certify that this document was served via electronic mail this 4th day of January 2010:

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

Michael Ricciutti
K&L Gates LLP
One Lincoln Street
Boston, MA 02111-2950
michael.ricciuti@klgates.com



Ben T. Clements