



SITUATIONAL INFORMATION REPORT FEDERAL BUREAU OF INVESTIGATION

Tradecraft Alert BOSTON DIVISION

Approved for Release: 12 August 2016

SIR Number: SIR-00108662570

(U) Business E-mail Compromise Schemes Targeting Colleges and Universities through Payment Diversion Fraud, as of August 2016

SOURCE: (U) An FBI Agent.

FBI Boston is releasing this Situational Information Report for operational awareness of tactics used by business e-mail compromise (BEC) perpetrators to defraud colleges and universities in the Boston area of responsibility through payment diversion fraud. The perpetrators purported to be a construction company with an ongoing vendor relationship with the college or university and provided alternate payment instructions for an electronic funds transfer to a different bank account than typically used.

(U) As of August 2016, FBI Boston identified three BEC incidents over the past month where perpetrators submitted fraudulent electronic funds transfer authorization forms to divert payments to bank accounts controlled by the perpetrators. Several similarities between these incidents include:

- The perpetrators portrayed themselves as existing vendors;
- The perpetrators portrayed themselves as construction companies;
- The victims' accounts payable departments were initially contacted (either via telephone or e-mail) requesting a change to the existing vendors' bank coordinates. The initial contact was followed up with either an e-mailed or faxed authorization form for an electronic funds transfer (EFT) denoting the perpetrator's bank account as the designated payment location;

(U) Warning: This is an information report, not finally evaluated intelligence. It is being shared for informational purposes but has not been fully evaluated, integrated with other information, interpreted or analyzed. Receiving agencies are requested not to take action based on this raw reporting without prior coordination with the FBI.

(U) Note: This product reflects the views of the BOSTON Division.

UNCLASSIFIED//FOUO

- The preferred method of payment was via the Automated Clearing House (ACH); and
- The perpetrators waited for payments on legitimate vendor invoices to be directed to the newly provided bank accounts.

(U) These similarities are provided as potential “red flags,” but they are not all-inclusive nor are they all required to be present for a transaction to be deemed suspicious.

(U) Colleges and universities are encouraged to remain vigilant regarding the vendor creation, vendor modification and vendor payment processes as the scheme is currently active in the Boston area. You are further encouraged to verify each of these processes via a known telephone number or in person with the purported company/vendor making the request. Given the potential of compromised e-mail systems involved in this scheme, e-mail is not the recommended method of validating payment requests.

(U) Report instances of fraud to the FBI’s Internet Crime Complaint Center (www.ic3.gov) as soon as possible, regardless of whether funds were sent. If funds were sent, immediately alert your financial institution of the fraud and request either an ACH reversal or SWIFT recall. Also request that they prepare a Hold Harmless letter to be sent to the beneficiary bank.

(U) This report has been prepared by the BOSTON Division of the FBI. Comments and queries may be addressed to the BOSTON Division at 617-742-5533.

UNCLASSIFIED//FOUO

Distribution

Domestic Security Alliance Council
Financial Institutions within the FBI Boston AOR
Community Outreach Program
Boston Regional Intelligence Center
Commonwealth Fusion Center
Maine Information and Analysis Center
New Hampshire Information and Analysis Center
Rhode Island Fusion Center
FBI Intranet
Law Enforcement Online

FBI Customer Satisfaction Survey

Please take a moment to complete this survey and help evaluate the quality, value, and relevance of our product. Your response will help us serve you more effectively and efficiently in the future. Thank you for your cooperation and assistance. Please return to:
Federal Bureau of Investigation
BOSTON DIVISION
One Center Plaza
Suite 600
Boston MA 02108
Fax: (617) 223-6327

Customer and Product Information

SIR Tracking ID: SIR-00108662570

Product Title: (U) Business E-mail Compromise Schemes Targeting Colleges and Universities through Payment Diversion Fraud, as of August 2016

Dated: _____

Customer Agency: _____

Relevance to Your Intelligence Needs

1. The product increased my knowledge of an issue or topic. (Check one)
- 5. Strongly Agree
 - 4. Somewhat Agree
 - 3. Neither Agree or Disagree
 - 2. Somewhat Disagree
 - 1. Strongly Disagree

Actionable Value

2. The product helped me decide on a course of action. (Check one)
- 5. Strongly Agree
 - 4. Somewhat Agree
 - 3. Neither Agree or Disagree
 - 2. Somewhat Disagree
 - 1. Strongly Disagree

Timeliness Value

3. The product was timely to my needs. (Check one)
- 5. Strongly Agree
 - 4. Somewhat Agree

- 3. Neither Agree or Disagree
- 2. Somewhat Disagree
- 1. Strongly Disagree

Comments (please use reverse or attach separate page if needed):
