Business Email Compromise

The Effective Evolution of Nigerian Fraud

Agenda

- What is BEC?
- Why should you care (statistics)?
- Why is it so hard to stop?
- Apprehension *is* possible
- Join the fight!

What is BEC?

- Historically unsophisticated scams have evolved into highly effective fraud

Nigerian Prince Scams ⟶ BEC

What is BEC?

- Scam carried out by compromising or spoofing legitimate business email account(s) to conduct unauthorized transfers of funds

- Other Names for BEC:
  - Business Email Spoofing (BES)
  - Email Account Compromise (EAC)
  - CEO Fraud / CEO Spoofing
  - Man In the Email
  - “Wire Wire”

Why Should You Care?

Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

Jul 12, 2018

Alert Number

I-071218-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations: www.fbi.gov/contact-us/field

BUSINESS E-MAIL COMPROMISE THE 12 BILLION DOLLAR SCAM

This Public Service Announcement (PSA) is an update and companion to Business E-mail Compromise (BEC) PSA 1-050417-PSA posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center (IC3) complaint information and updated statistical data for the time frame October 2013 to May 2018.

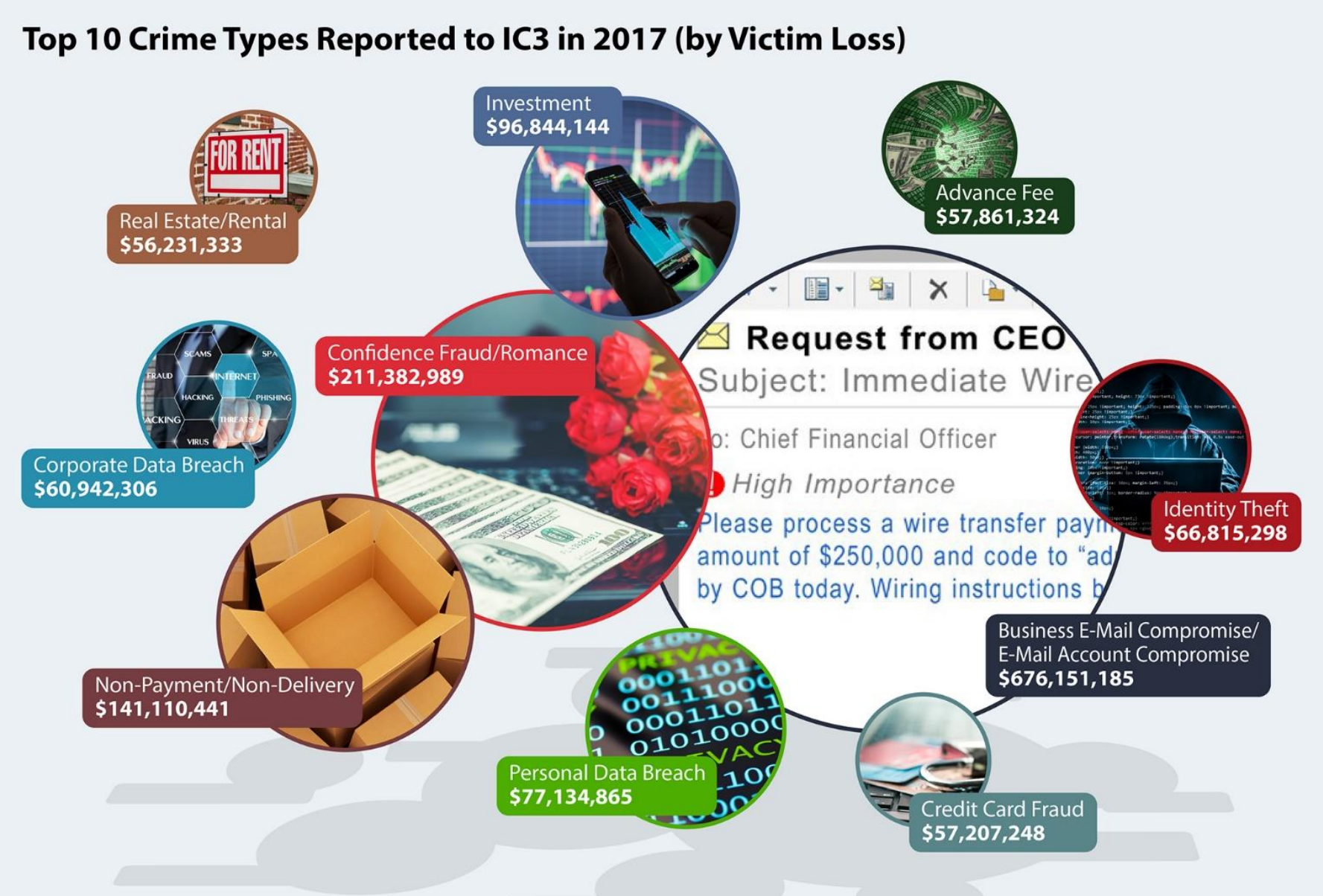
DEFINITION

Business E-mail Compromise (BEC)/E-mail Account Compromise (EAC) is a sophisticated scam targeting both businesses and individuals performing wire transfer payments.

Why Should You Care?

- BEC victim complaints submitted to IC3.gov from October 2013 to May 2018:
  - U.S. victims: 41,058
  - U.S. losses: $2,935,161,457

IC3 - 2017 Losses Grouped by Crime Type



The Many Varieties of BEC

- Vendor Fraud (“Man-in-the-Email”)
  - Invoice payments
  - Real estate sales
- Compromised or spoofed email account used to request wire transfer
  - Fraudster emails victim business employee or bank employee
- Requests for Personally Identifying Information (PII), for example W-2’s
- Other Similar Schemes:
  - Intrusion resulting in changes to payroll system
  - Requests for annuity distributions

How are new targets identified?

How do they communicate with victims?

Spoofed email:

From: john.smith@domain.com

Reply-To: bad.guy@scammer.com

Look-alike domain registered:

john.smith@do**m**ain.com legitimate

john.smith@do**rn**ain.com fraudulent

Compromised email account:

Phishing or malware used to steal credentials for john.smith@domain.com

Where does all this money go?

- Romance Scam Victims
- Online Job Scam Victims
- Street Gang Members (“cash out crews”)
- Co-conspirators that accept cash deposits
- U.S. businesses that sell products to Nigeria or other foreign nations (trade-based money laundering)

Successful Prosecutions

Department of Justice

U.S. Attorney's Office

Western District of Wisconsin

SHARE

FOR IMMEDIATE RELEASE

Tuesday, November 21, 2017

Three Sentenced in Cyber Fraud Schemes Involving More Than $17 Million

MADISON, WIS. – Jeffrey M. Anderson, Acting United States Attorney for the Western District of Wisconsin, announced that three individuals involved in an international romance fraud scheme were sentenced this week.

Richard Ugbah, 36, a Nigerian citizen living in Atlanta, was sentenced yesterday by U.S. District Judge James D. Peterson to 12 years in federal prison for his role the scheme. Ugbah pleaded guilty on March 15, 2017 to wire fraud. Ugbah was also ordered to forfeit a Mercedes Benz automobile and two bank accounts.

Successful Prosecutions

Department of Justice

U.S. Attorney's Office

District of Nebraska

SHARE

FOR IMMEDIATE RELEASE

Friday, February 8, 2019

Nigerian Business E-mail Scammer Sentenced for Fraud

United States Attorney Joe Kelly announced that Adewale Aniyeloye, age 32 from Nigeria, was sentenced today for Wire Fraud. United States District Court Judge Robert F. Rossiter, Jr., sentenced Aniyeloye to a 96-month term of imprisonment. After his release from prison, Aniyeloye will begin a 3-year term of supervised release. The restitution amount is to be determined and will be ordered at a later date.

Successful Prosecutions

Department of Justice

U.S. Attorney's Office

District of Nebraska

SHARE

FOR IMMEDIATE RELEASE

Monday, March 25, 2019

Nigerian Business E-mail Scammer Sentenced for Fraud

United States Attorney Joe Kelly announced that Pelumi Fawehinmi, age 38, of Nigeria, was sentenced Friday, March 22, 2019, for Wire Fraud. United States District Court Judge Robert F. Rossiter, Jr., sentenced Fawehinmi to a 72-month term of imprisonment. After his release from prison, Fawehinmi will begin a 3-year term of supervised release. The restitution amount is to be determined and will be ordered at a later date.

Operation Wire Wire

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Monday, June 11, 2018

74 Arrested in Coordinated International Enforcement Operation Targeting Hundreds of Individuals in Business Email Compromise Schemes

42 Alleged Fraudsters Arrested in the United States

Federal authorities announced today a significant coordinated effort to disrupt Business Email Compromise (BEC) schemes that are designed to intercept and hijack wire transfers from businesses and individuals, including many senior citizens. Operation Wire Wire, a coordinated law enforcement effort by the U.S. Department of Justice, U.S. Department of Homeland Security, U.S. Department of the Treasury and the U.S. Postal Inspection Service, was conducted over a six month period, culminating in over two weeks of intensified law enforcement activity resulting in 74 arrests in the United States and overseas, including 29 in Nigeria, and three in Canada, Mauritius and Poland. The operation also resulted in the seizure of nearly $2.4 million, and the disruption and recovery of approximately $14 million in fraudulent wire transfers.

If You Are a Victim of a BEC Attack

- Report incidents to IC3 (with or without losses)
- If money is sent, contact your bank and the FBI immediately

How to Prevent BEC

- Use multi-factor authentication
- Implement policies and procedures for verifying significant transactions/changes (like wire transfers or vendor payment instructions)
- Add banner/warning to external messages
- Configure SPF, DKIM, and DMARC
- Educate and train employees

BEC-International Slack Channel

25 OCT 18

How Do You Fight a $12B Fraud Problem? One Scammer at a Time

The fraudsters behind the often laughable Nigerian prince email scams have long since branched out into far more serious and lucrative forms of fraud, including account takeovers, phishing, dating scams, and malware deployment. Combating such a multifarious menace can seem daunting, and it calls for concerted efforts to tackle the problem from many different angles. This post examines the work of a large, private group of volunteers dedicated to doing just that.