ISBA MUTUAL INSURANCE

Business Email Compromise & Wire Fraud

How you can prevent BEC attacks and Wire Fraud before it happens, and what to do if you're a victim.

Mat Kresz, Esq.

Mat Kresz, Attorney
605 N. Michigan Ave. FL 4
Chicago, Illinois 60611

☎ 312-967-5900 (Office)
312-986-9600 (Cell)
MBK@KreszLaw.com

- Mat Kresz is a Cybersecurity, Data Privacy, and Technology attorney in Chicago.
- Notably, Mat's practice is informed and enhanced by his background in technology and business, having served as a Chief Information Officer (CIO) at a mid-size enterprise that served Fortune 500 customers.
- Through the business and technology experience he gained in technology and leadership roles, Mat is better equipped to identify opportunities, solve problems, and mitigate risk in sensible business terms.

My Mission, and

Today's Agenda

I. Common Terms

II. BEC & Wire Fraud Case Studies and recent developments regarding BEC

III. What you can do to prevent a BEC and Wire Fraud

IV. What to do if you're a victim

V. Ethical (and legal) notification responsibilities

I. Common Terms

- **Phishing**
  Practice of sending fraudulent emails that purport to be authentic to induce recipient to take actions that leads to fraud.
- **Spear Phishing**
  Phishing that targets specific individuals.
- **SPAM** (in Contrast to Phishing)
  Junk email. Unwanted, unsolicited, and sent in bulk, but not necessarily malicious.
- **BEC**
  "Business Email Compromise." Incidents where an email account becomes compromised –whether a "business" email account, or otherwise.
- **Tenant** (Also Email Tenant or Tenant Account)
  A company account within Office 365, G-Suite, Zoho, etc., that contains one or more email boxes. The account that is designated to be the "Admin" account usually provides access and visibility to all email boxes and their configuration within the Tenant Account.
- **Mailbox Rules**
  Email handling rules that perform one or more actions on an email message when a certain condition is met. Example: A mailbox rule could be established to forward any email that contains "wire" or "money" to fraudster@gmail.com.
- **2FA**
  Two Factor Authentication. Commonly, this is the code you receive via text message from a service provider that serves as the second authenticator (in addition to your password) that validates your identity.
- **MFA**
  Multi-Factor Authentication. Encompasses 2FA,but includes many other elements that a service provider could consider in the course of authenticating a user, including for instance, the IP address through which you're attempting to authenticate, patterns in the way you typically use the service, or keystroke dynamics.
- **Credential Stuffing**
  A tactic to attempt to gain access to a target system by trying to log in with passwords to other systems. For example, attempting to log in to Office 365 by trying to log in with passwords to the user's Amazon, Netflix, and AOL accounts.
- **Session Cookie**
  A small file saved to a computer that a website uses to remember that the user was previously authenticated (after a recent successful login-in). Without this, a website would need to request the user's credentials to re-authenticate him/her when the user clicks a link while in that session. Note: this is not the "remember me" feature.
- **Threat Actor**
  The bad guy. Usually part of a gang that specializes in certain types of cyber crime.

II. BEC & Wire Fraud Case Studies

- A) Small Law Firm BEC
- B) Targeted Real Estate Transaction Resulted in $380,000 Loss
- C) Law Firm Mis-Wired $63,000 Settlement Payment to Fraudster

Note: Some facts were changed and some cases were merged.

II. a) Small Law Firm BEC

- **Facts**
  - Small law firm of about 5 attorneys with a wills, trusts, and estates practice.
  - By chance, the estates attorney observed mailbox rules that she did not set. She inquired to the IT person.
  - IT confirmed they did not set the mailbox rules. and called Microsoft.
- **Investigation**
  - Attorney & IT called Microsoft. Microsoft confirmed several off-shore logins.
  - Forensics firm was retained to investigate.
  - Investigation determined that 3 of 5 email accounts within the tenant were compromised.
  - And that the threat actor likely gained access to at least one account by Credential Stuffing.
  - The Firm certified that only one mailbox could have contained personally identifiable client information, and there was no likelihood of other such information.
- **Outcome**
  - A fulsome investigation was successfully conducted because logs were available to analyze.
  - The firm had a strict practice not to receive or retain sensitive information in email. Only one client's information was at issue.
  - The firm notified that client and out of an abundance of caution, provided credit monitoring to the individual for 18 months.

b) Targeted Real Estate Transaction

- **Facts**
  - Residential home purchase transaction.
  - Buyers wired to sellers a substantial down payment on a home, approximately $380,000.
  - Just before closing, it was discovered that the $380,000 was mis-wired. It never reached the sellers.
- **Investigation**
  - A forensic investigation was substantially inconclusive.
  - Any of the buyers' or sellers' email accounts could have been compromised. Any of their attorneys' email accounts could have been compromised.
  - Some of the email messages were examined, and those appeared to be authentic.
  - Some theories:
    - Domain registrar could have been compromised, allowing a bad actor to send authentic emails through a domain.
    - Consumer email accounts could have been compromised, which lacked sufficient logs.
- **Conclusion**
  - Nothing in the investigation pointed to a clear indicator of compromise.
  - The parties were deadlocked.

c) Law Firm Mis-Wired $63,000 Settlement Payment to Fraudster

- **Background**
  - In the case of Bile v. RREMC, LLC, Civil Action No. 3:15cv051, 2016 U.S. Dist. LEXIS 113874 (E.D. Va. Aug. 24, 2016), a settlement agreement was reached in a wrongful termination case.
  - Plaintiff pressured his attorney to attempt to collect on the settlement.
  - While exchanging payment instructions, Plaintiff's attorney received emails from an actor that apparently attempted to meddle with the transaction. The attorney showed them to his client, but not the Respondent's attorney.
  - Some time had passed and the Plaintiff had not received his settlement, so his attorney inquired as to the status on payment. Respondent's attorney confirmed that payment was made.
  - It was then discovered that a BEC lead to the Respondent's attorney mis-wiring $63,000 to a fraudster.
  - Next, the plaintiff sued for specific performance.

c) Law Firm Mis-Wired $63,000 Settlement Payment to Fraudster

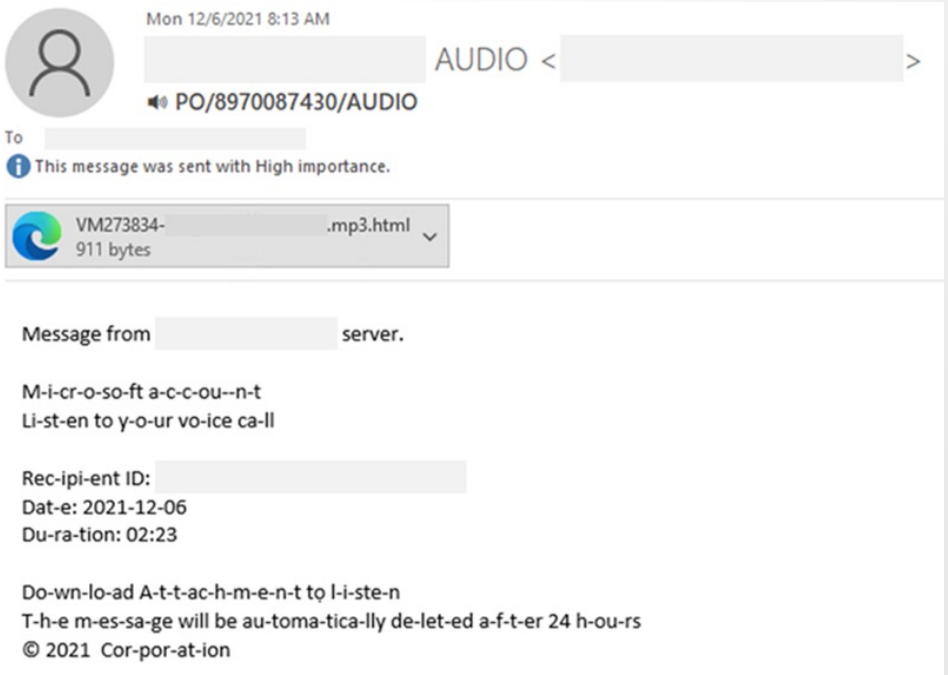
- **Issue**
  - Who should shoulder the loss?
    - The Plaintiff's attorney?
      - He knew the transaction was being targeted, but didn't raise it with Respondent's attorney.
      - However, he ultimately did not wire the money to the wrong account.
    - The Respondent's attorney?
      - He ultimately caused the wire to be sent to the wrong account.
      - But he had no reason to know since he suspected no foul play.
      - In addition, he meticulously followed internal procedures to confirm wires.

c) Law Firm Mis-Wired $63,000 Settlement Payment to Fraudster

- **Result**
  - Court Found that:
    - Plaintiff's attorney failed to exercise ordinary care when he had actual knowledge of a fraudster's attempt to meddle with the transaction but failed to warn the Respondent's attorney;
    - Respondent's attorney did not fail to exercise ordinary care because it had no indication that the transaction was targeted, and opined that since he followed corporate procedures closely, he would not have initiated the wire had he known that the transaction was being targeted by a fraudster.
  - Court Held that:
    - The party that was in the best position to prevent the fraud but failed to attempt to verify the wire instructions failed to exercise reasonable care, and should be liable.

Trending Now: AiTM Phishing Scheme Used to Bypass MFA

Email with Purported Voicemail Attached (below):



https://www.microsoft.com/en-us/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/

- Fraudsters can overcome MFA by stealing the session cookie.
- How does it work?
  - Fraudster causes a user to access a legitimate website (such as Office 365) through the Fraudster's proxy. (User receives an email purporting to have a voicemail attachment that requires login to retrieve.)
  - When the user logs in to the true service provider, the Fraudster is able to intercept the session cookie, since the login occurs through the Fraudster's proxy.
  - Later, the Fraudster can return to the legitimate website to access the user's account without logging in (because he has the session cookie that tells the site that authentication has occurred).
- Take-aways:
  - MFA and 2FA are not bullet-proof. Always use caution when accessing any links.
  - If you suspect that your account was compromised, contact your IT provider.

III. What you can do to prevent a BEC and Wire Fraud

- Conduct Security Awareness Training. Keeping up with security threats and trends is very effective to prevent BEC and Wire Fraud (and ransomware).
- Stay out of financial transactions if you can. Let the payor and payee work directly to work out remittance plans. Then, confirm with the parties that the transaction was made.
- Verify wire instructions by phone if you have to be involved in the transaction, even if the wire instructions by email appear to be true.
- If you suspect that the transaction is being “targeted,” immediately warn the other party by phone, not email. Remember: your emails might be seen and intercepted by a bad actor.
- Use a strong passwords that are unique for your email account to prevent credential stuffing.
- Use a commercial email service provider such as Office 365 or G Suite because they have better technical support, better logging, and built-in security tools compared to consumer accounts.
- Implement 2FA / MFA. It’s included in many services.
- Consider cyber liability insurance that covers wire fraud.

IV. What to do if you're a victim

- Move Quickly
  The faster you take action, the more likely it is that you can prevent a bad wire or recover money that was mis-wired.
  - *Immediately contact the financial institutions and the parties involved.*
  - *Law enforcement may also be able to assist with recovering lost funds.*

IV. What (else) to do if you're a victim

- Engage Cyber / Data Privacy Counsel to assist you.
- Initiate a claim to your cyber liability carrier.
- Contact local law enforcement and make a police report. (Local law enforcement might refer you to another agency.)
- Contact the FBI's Internet Crime Center to report the incident.
- Assess your legal & ethical responsibilities post-incident.

V. Ethical Notification Responsibilities

- **ABA's Formal Opinion 483.** "[T]he American Bar Association Standing Committee on Ethics and Professional Responsibility reaffirm[ed] that lawyers have a duty to notify clients of a data breach…."
  - Data compromise might prejudice a client's matter
  - Data compromise might cause confidential information to become known

- **Notify Opposing Counsel.** "[A]ttorneys have 'an obligation to contact opposing counsel when and if they receive suspicious emails instructing them to wire settlement funds to a foreign country where such [a] request has never been made during the course of performance of the parties."
  Bile v. RREMC, LLC, Civil Action No. 3:15cv051, 2016 U.S. Dist. LEXIS 113874, at *34 (E.D. Va. Aug. 24, 2016).

V. Additional Notification Obligations

- **Data Privacy Laws**
  - Several laws and rules require notice to affected individuals
    - State Data Privacy Laws
    - Federal Data Privacy Laws
    - Agency Rules
  - The definition of a “breach” will vary
  - The entities to be notified will vary
  - The content of the notice will vary

- **Contractual Notification Obligations**
  - Your clients may have agreed to contact others in case access to their data is compromised.

Questions & Comments

Mat Kresz, Attorney

312-967-5900 (Office)
312-986-9600 (Cell)

MBK@KreszLaw.com