Idaho Department of Finance Financial Innovation Lab

Emerging Technology Advisory Committee Report

Business Email Compromise:
A Growing Cybercrime in Need of an AI Policy Solution

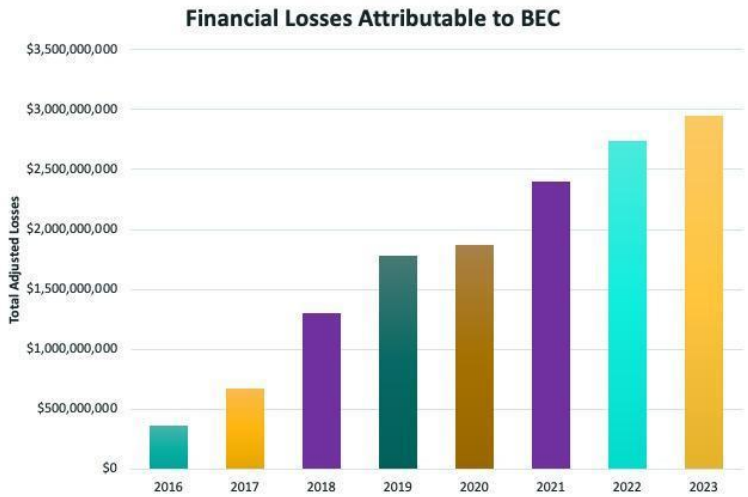
Executive Summary

Over the past decade, business email compromise (BEC) attacks were the costliest form of cybercrime in the United States and the vast majority of BEC attacks can be stopped by simply requiring fund transfer beneficiary names match recipient account holder names through the use of basic artificial intelligence (AI) name matching tools. In 2023, BEC victims reported approximately $3 billion in verified losses that led to a significant amount of small business closures. These facts make it vital for policymakers to craft a solution that protects financial institutions from civil litigation if they adopt a risk-based AI name matching program.

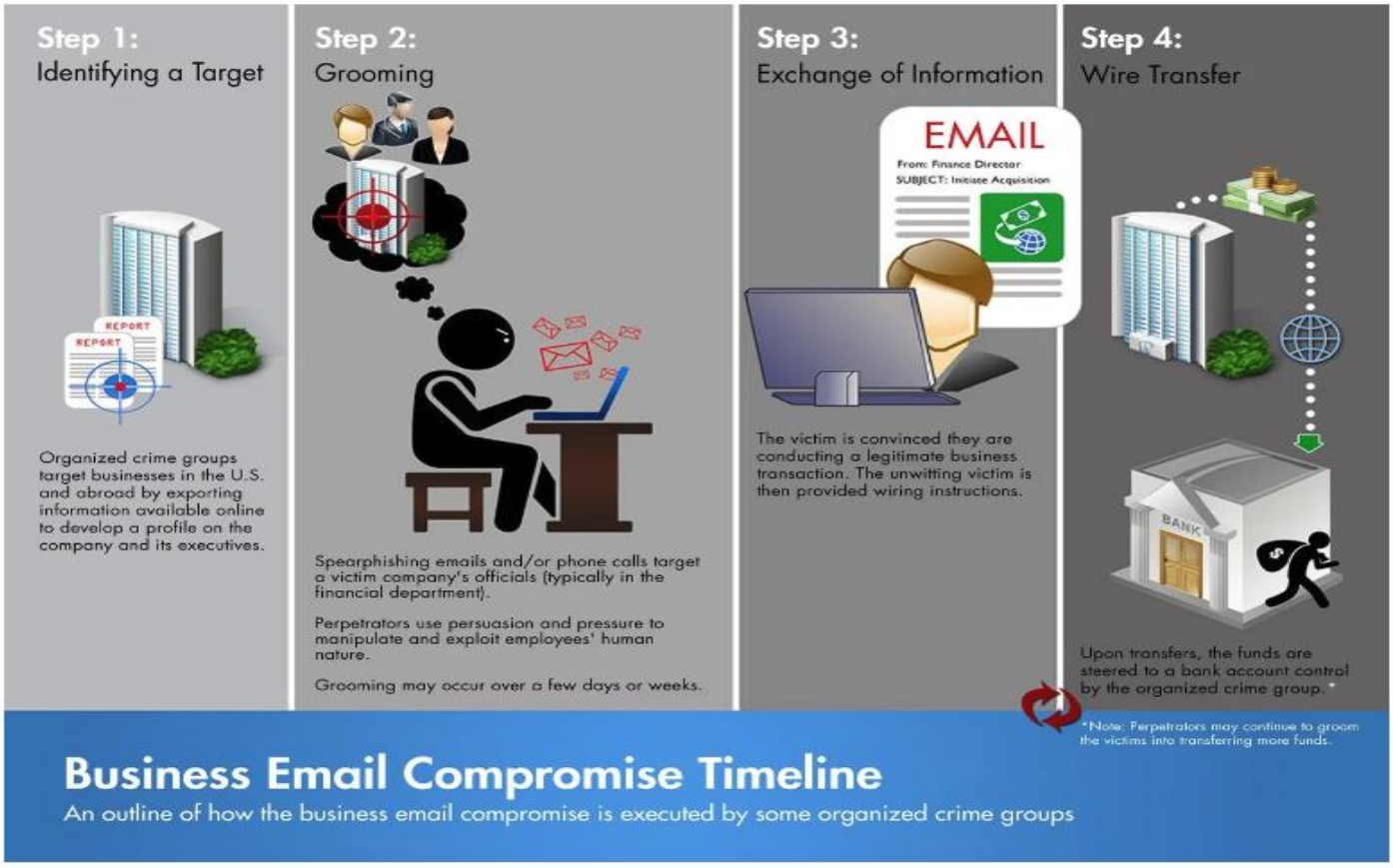
In addition to an AI name matching program, increased information sharing between financial institutions and enhancements to the Financial Crimes Enforcement Network's (FinCEN) Rapid Response Program (RRP) and the Federal Bureau of Investigation's (FBI) Financial Fraud Kill Chain (FFKC) can help significantly decrease the success of BEC attacks and better protect the public.

BEC: A Growing Cybercrime Issue

BEC attacks have led to the largest cybercrime financial losses in the United States over the last decade (see chart below). Illicit actors who conduct BEC attacks use email correspondence to induce victims to initiate wire transfers to accounts controlled by the criminals. Typically, an attacker has either gained illegal control of a victim or trusted party's email via social engineering, a phishing attack and/or the use of malware.



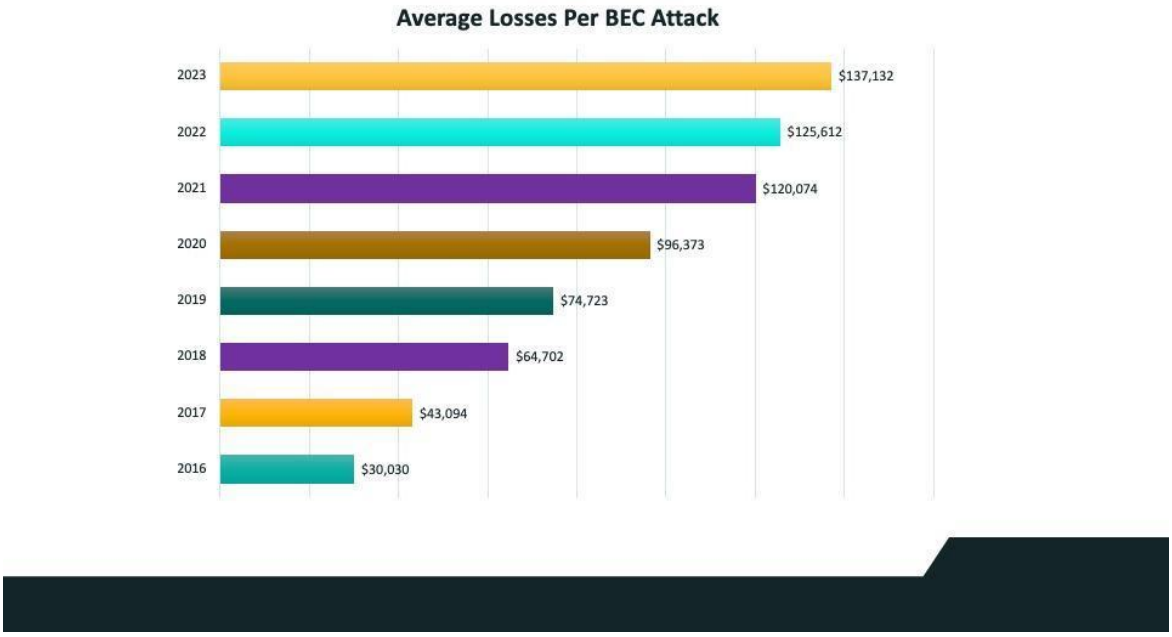
BEC attackers have developed a sophisticated methodology for conducting these attacks. The following illustration from the FBI demonstrates some of the features of a BEC attack methodology:



BEC is a Small Business Killer

BEC losses are business killers, especially to small businesses who lack the financial cushion to survive a successful BEC attack. Research shows that 60% of small businesses close within six months of a cyber-attack, which makes BEC one of the leading causes of small business closures.[i] The reason for this is that BEC losses are typically uninsured (only policies that have specific coverage for social engineering fraud, invoice manipulation, and/or network security may be covered).[ii] Financial institutions do not reimburse BEC victims for losses since the institution was simply following the account holder's instructions for processing the wire transfer.

Research reveals that executives and employees of commercial entities are most often targeted in BEC attacks.[iii] The most attractive targets for attackers are businesses that conduct large transactions through financial institutions, lending entities, real estate companies, and law firms.[iv] While commercial entities are most often targeted, consumers are increasingly being targeted when they are involved in large transactions such as home purchases. Statistics highlight that financial losses per BEC attack are increasing for both businesses and individuals and will likely continue to grow unless new solutions and mechanisms are adopted (see chart below).



Transaction Name Matching a BEC Vulnerability

Successful BEC attacks rely on bad actors controlling bank accounts and these accounts rarely match the beneficiary's name on the requested funds transfer making this a key BEC scam vulnerability. However, since financial institutions do not need to have a name match to accept incoming funds transfers, many bad actors are able to receive their ill-gotten gains. This reality is what enables illicit actors to manipulate the financial system in their BEC schemes to the detriment of the public and businesses.

Accounts used in BEC attacks are often short lived and can only be used for very brief periods of time before they are frozen or closed due to the resulting complaints of fraud and/or potential law enforcement action. Because of attribution risks, attackers will seldom use their own identity to open accounts for BEC attacks and due to anti-money laundering (AML) know your customer (KYC) constraints, bad actors require a clean cover identity to receive funds.

It should be noted that attackers prefer domestic (US) accounts as they function for a broader variety of attacks than foreign (non-US) accounts. Additionally, bad actors may use money mules as account holders who also become victims of the fraud to distance themselves from the illicit money trail.

It is extremely difficult to recover funds unless the victim, financial institutions involved, or law enforcement act extremely quickly because illicit actors typically move the funds from the initial deposit account as rapidly as possible to prevent the victim from being able to recover them. This means timely information sharing and communication are essential for retrieving stolen funds, since the window for recovering the funds is often 24 hours or less.[v]

Keys to Defeating BEC:
Name Matching Requirements, AI, Information Sharing, and Stronger Anti-Fraud Programs

Despite its consistent status as one of the top forms of cybercrime, BEC attacks could be almost entirely thwarted through the development of new policies/statutes, innovative uses of technology, and enhancements to already existing government programs:

- **Enforce Name Matching for Wire Transfers and Develop AI Verification Programs** – A policy/statute requiring wire beneficiary names to match recipient account holder names for wire transfers (e.g., amending Uniform Commercial Code 4A-207) is essential for disrupting BEC scams on a massive scale.

  Any policy/statute should also include a clause for the development of AI name matching verification programs at financial institutions that use basic AI tools to verify wire transfer names. AI name matches should not have to be exact matches but should meet an agreed upon threshold (e.g., perhaps a 70% match) to stop the blatant name mismatches BEC scams rely upon.

- **Liability Protection for Adopting AI Name Matching Verification Programs**- Any financial institution that implements a risk-based AI name matching verification program for wire transfers should receive protection from potential liability in BEC cases. Enforcing name matching for wire transfers is vital for preventing successful BEC attacks and financial institutions should receive protection for adopting risk-based AI verification programs capable of disrupting a large percentage of these frauds.

- **Clarify That Section 314b Should Be Used for Fraud Information Sharing** – Information sharing is critical for stopping BEC scams. Guidance to financial institutions should be provided clarifying that Section 314b of the Patriot Act allows for information sharing between financial institutions when there is a reasonable basis to believe that specified unlawful activities including BEC attacks, wire fraud generally, money laundering and other specified crimes are occurring. Currently, many financial institutions do not share fraud information with each other because they are not sure that fraud relates directly to the money laundering clause found in Section 314b.

- **Enhance the Financial Fraud Kill Chain (FFKC) and Rapid Response Program (RRP)** - By expanding the FBI's FFKC and FinCEN's RRP and improving their information sharing capabilities, more stolen BEC funds will be frozen and seized. More resources will enable both the FBI FFKC and FinCEN RRP to address more cases in a timely manner for victims, while developing better tools and mechanisms for information sharing with critical state, local, international, and industry partners/stakeholders will facilitate stronger cooperation and lead to an increase in the prevention, detection, and interdiction of BEC fraud.

The adoption of these solutions will result in the prevention of many successful BEC attacks and save victims billions of dollars. These solutions will facilitate the recovery of more stolen funds and will disrupt the BEC operations of illicit actors for the benefit of the American public and businesses.

Endnotes

[i] https://www.inc.com/joe-galvin/60-percent-of-small-businesses-fold-within-6-months-of-a-cyber-attack-heres-how-to-protect-yourself.html

[ii] Raver, Carrie and Godes, Scott. "Gone Phishin': How Does Insurance Apply to Business Email Compromise Losses?" 2020 Barnes and Thornburg LLP.

https://btlaw.com/en/insights/blogs/policyholder-protection/2020/gone-phishin-how-does-insurance-apply-to-business-email-compromise-losses

[iii] "FinCEN Advises Financial Institutions on Fighting Email Compromise Fraud." *Teller Vision*, no. 1471, Aspen Publishers, Inc, 2016, pp. 1-4.

[iv] *Ibid.*

[v] These findings are based upon the investigations of BEC attacks and interviews with BEC suspects and money mules during the author's service with the United States Secret Service's Los Angeles Electronic Crimes Task Force and the FBI's Los Angeles Cyber Crime Task Force and as commanding officer of the Los Angeles County District Attorney's Office Cyber Crime Section.