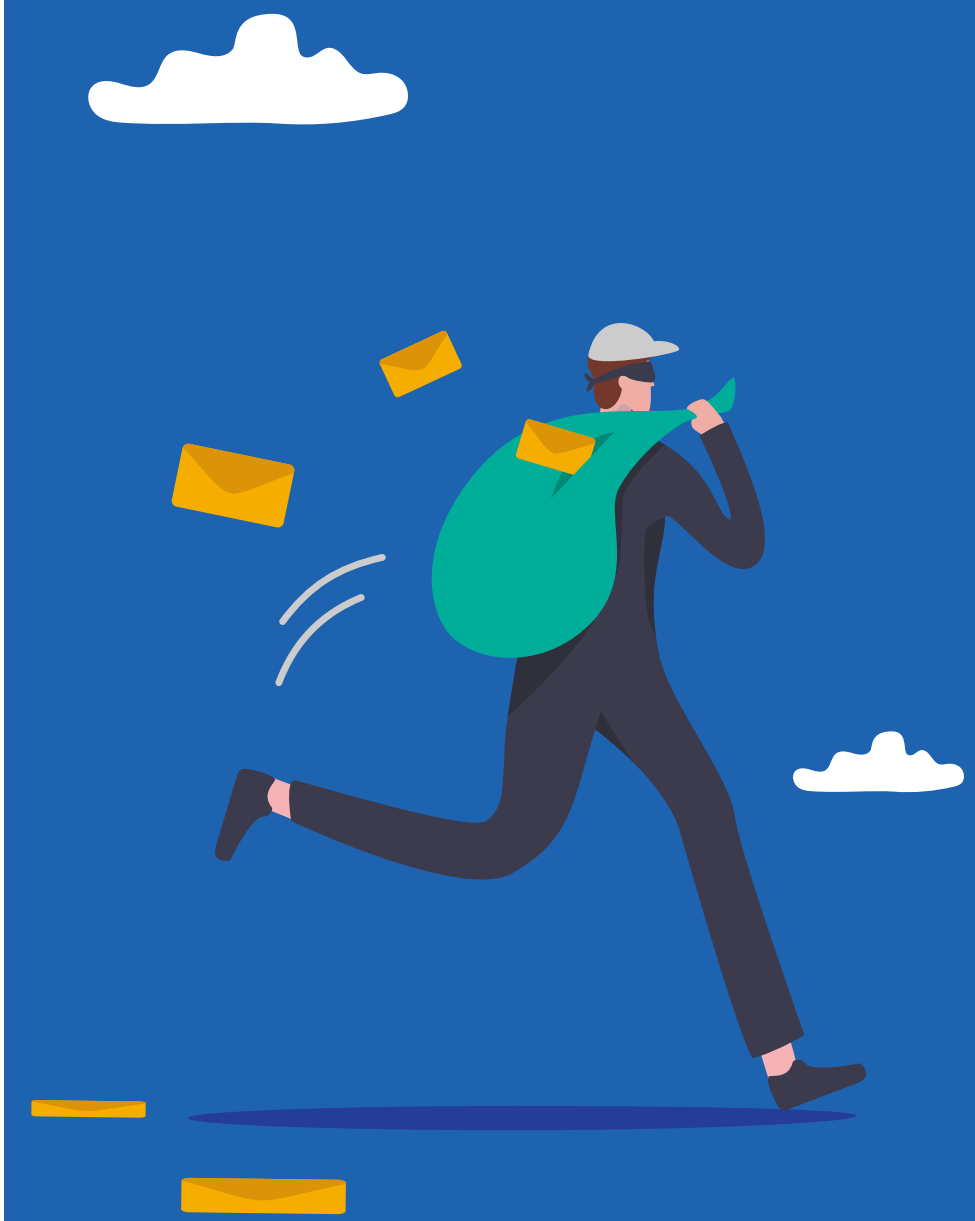
E-BOOK

You've Got Email Fraud!

A roundup of the biggest, boldest and most brazen business email compromise attacks

2023 Edition



proofpoint.

Introduction

Business email compromise (BEC) fraud affects organizations of all sizes across every industry around the world, exposing them to billions of dollars in potential losses. The FBI's *2022 Internet Crime Report* says that BEC schemes caused about $2.7 billion in losses. That's $300 million higher than 2021.[1]

Many of today's BEC schemes are highly sophisticated, well-funded and backed by careful planning and research. They're also very difficult to detect because they don't include the usual payloads—malicious URLs or file attachments—to analyze. Instead, fraudsters rely on impersonation and other social engineering techniques to trick people.

A growing number of attackers are focusing their efforts on supplier invoicing fraud and the large business-to-business (B2B) transactions they can hijack. Here's how they work:

1. First, BEC attackers pose as a person or entity that a recipient should trust, such as a colleague, boss or vendor.
2. The attacker sends an email directing recipients to take some action that siphons money or sensitive financial information from the organization. These could include fraudulent wire transfers, bogus invoices, diverted paychecks, changed banking details for future payments and countless other schemes.
3. By the time the organization discovers the error, it's often too late to recover the money.

This e-book looks at just some of the most egregious examples of BEC attacks seen in 2022 and 2023. This collection is meant to illustrate just how varied, targeted, lucrative—and heartless—these campaigns can be. They also show how almost anyone, without the right security controls, can fall for an expertly crafted campaign.

1 FBI. 2022 Internet Crime Report. March 2023.

PUBLISHING WORLD THEFTS

Book 'Em, Dano

A mystery was solved in January 2022 that had baffled the book world for years. Since 2016, someone had been stealing unpublished manuscripts, many of which were written by famous authors. And they'd done it by impersonating literary professionals via email.

Details of the scam came to light after Filippo Bernardini was arrested by FBI agents at New York's JFK airport.[2] Between August 2016 and the summer of 2021, Bernardini had tricked hundreds of people into sending him their novels and unpublished works. High-profile novelists like Ian McEwan, Margaret Atwood and Sally Rooney had been targeted. And so had manuscripts from obscure authors.

According to federal prosecutors, Bernardini's scheme involved registering more than 160 fake internet domains to send emails from slightly altered, official-looking email addresses.[3] So an email that appeared to come from penguinrandomhouse.com actually read penguinrandornhouse.com—with the "m" changed to "rn."

The reason Bernardini was so successful largely came down to his insider knowledge of the publishing world. At the time of his arrest, he was working in London for the publisher Simon & Shuster. This experience meant he was well-versed in industry shorthand, making it easy to convince recipients he was the real deal.

What made the whole scheme so mystifying was that Bernardini seemed to lack a motive. He had never demanded any money or leaked the manuscripts online.

In January 2023, Bernardini pled guilty to one count of wire fraud. Before his sentencing in March 2023, he revealed the reason he'd worked so hard to defraud so many people. His motive was simple: He had wanted to "be one of the fewest to cherish them before anyone else."[4]

While he had faced a maximum sentence of 21 months in prison, the court ordered him to be deported and pay $88,000 in restitution instead.

Industries: Publishing

Location: U.S.

Thousands

of unpublished manuscripts stolen

2 Vulture.com. "The Talented Mr. Bernardini: A Young Italian Is Accused of Pulling Off the Book World's Most Perplexing Crime. Who is He?." February 2022.
3 BBC. "Filippo Bernardini: Italian Admits Stealing Unpublished Books." January 2023.
4 The Guardian. "Book Thief Who Stole More Than 1,000 Manuscripts 'Wanted to Cherish Them Before Anyone Else." March 2023.

‘CEO FRAUD’ GANG

The French Connection

In February 2023, news broke that Europol had busted an international email “CEO fraud” gang. While taking down international crime networks is nothing new, the size of the theft itself was breathtaking. The gang had stolen €38 million from a single company—and they’d done it in a matter of days.

According to Europol, Paris-based real estate developer Sefri-Cime fell victim to this gang in late December 2022.[5] The scheme started with the company's CFO being emailed by someone claiming to be a lawyer at a well-known French accounting firm. Within a few days, the fraudster had gained the CFO's trust and began requesting large, urgent transfers of millions of euros. Altogether, the gang stole €38 million, which they quickly laundered through various European countries, China and then Israel.

After the fraud was reported, investigators from multiple European countries were on the case. They started with Europol, which helped track the funds through the pre-existing money laundering network. It was during this investigation that a previous unsuccessful scheme by the same group was uncovered.

Earlier in December 2021, an accountant at a French metallurgical company had been emailed by someone pretending to be the company's CEO. The fraudster had asked for an urgent, confidential transfer of €500,000. Luckily, the company spotted the scam in time and blocked the payment.

Investigators across multiple European countries worked in a joint operation to bring the network down. Over the next 12 months, six suspects in France and two in Israel—including the alleged gang leader—were arrested. And while the bulk of the money was not recovered, they did seize about €5 million in multiple bank accounts and €350,000 in digital currency.[6]

Industries: **Real estate, manufacturing**

Location: **EMEA**

€38 Million

($40.3 million) in damages

5 Europol.Europa.eu. "Franco-Israeli Gang Behind EUR 38 Million CEO Fraud Busted." February 2023.
6 Ibid.

EAGLE MOUNTAIN CITY, UTAH

Misdirection on Main Street

Eagle Mountain City, Utah, is a master-planned community that's expanding fast. In the past 25 years, it has grown from 250 residents to more than 50,000. That's a lot of new construction. With so many projects going on, it can be difficult to stay vigilant. Which is how the city may have become a prime target for BEC scammers.

The best laid plans often go awry—something Eagle Mountain City officials learned the hard way. While they made detailed plans for housing and infrastructure projects, they didn't plan to stop cyber criminals. Unfortunately, this cost the city's taxpayers nearly $1.13 million.

The theft took place in August 2022. At the time, the city was in the middle of a construction project to widen its main arterial road, Eagle Mountain Boulevard. During an email exchange between city officials and its construction vendor, BEC cyber criminals inserted themselves into an email thread and impersonated the vendor—and persuaded a staff member to transfer an electronic payment to them instead.

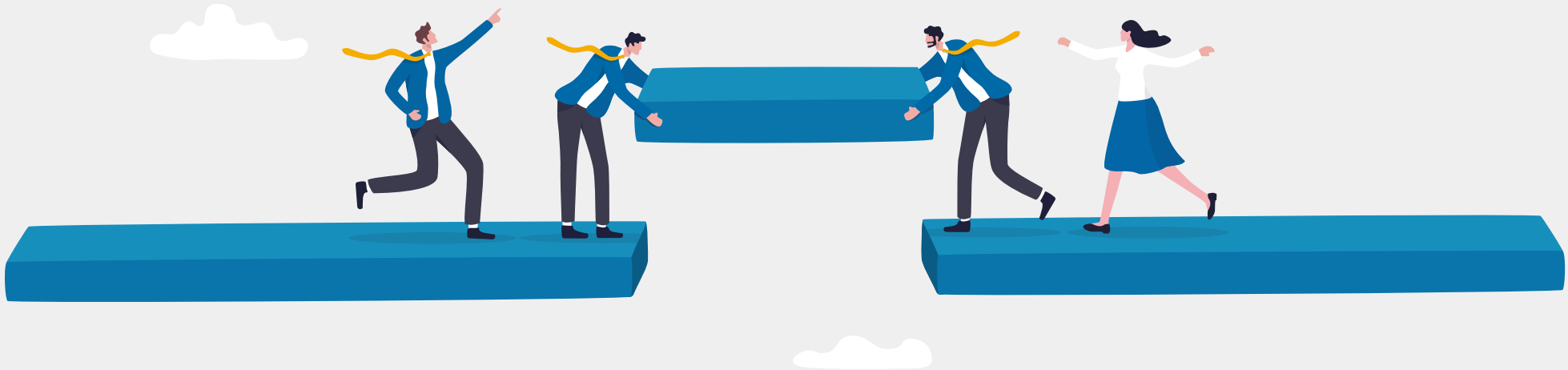
Two weeks later, the city realized what had happened and contacted the FBI and Utah County Sheriff's Office. Unfortunately, the money was long gone.[7]

Industries: Public Agency

Location: U.S.

$1 Million

in damages

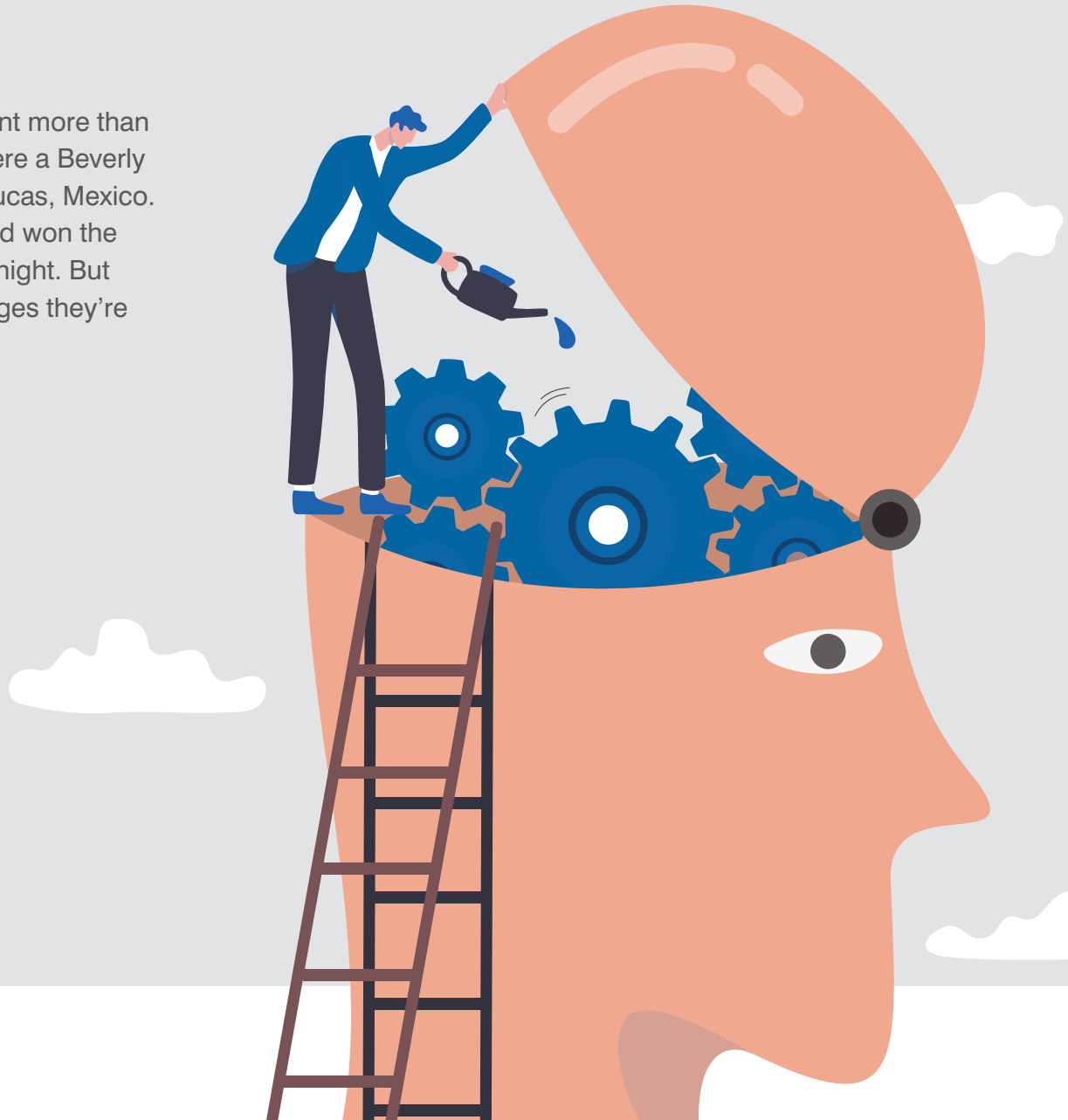


7 ABC4. "Eagle Mountain, Residents Respond to Million Dollar Cyber Scam." September 2022.

GRAND RAPIDS PUBLIC SCHOOLS, MICHIGAN

Lessons in Larceny

In a span of less than two months, a California couple spent more than $100,000 in the summer of 2021. Among their splurges were a Beverly Hills shopping spree and a luxury vacation in Cabo San Lucas, Mexico. If you looked at their bank account, you might guess they'd won the lottery—it jumped from less than $300 to $1.4 million overnight. But there was no winning ticket. Instead, law enforcement alleges they're BEC scammers.



According to a search warrant application filed in federal court, the couple stole $2.8 million by defrauding Grand Rapids Public Schools. The theft was traced to them in 2022 during a joint investigation by the Secret Service, the Grand Rapids police and the Beverly Hills police's High Tech Crime Task Force.

Here's how it went down. Someone gained access to the email account of the school district's benefits manager. Once in, they regularly monitored correspondence between the district and its health insurance vendor about monthly insurance payments.

Then, they sent an email to a district finance specialist asking them to change the wiring information for those payments—to the bank account of a California nail salon that the couple just happened to own. Two payments were subsequently sent to that account totaling more than $2.8 million.[8]

A few months later, when the insurance company inquired about the missing funds, school officials discovered the fraud. Fortunately, Chase Bank was able to recall $1.4 million.

But there's an unexpected twist in this story. After the funds were recalled, a man who identified himself as the husband went on the offensive, calling the district's financial specialist about the missing funds. The employee said they were part of a fraud and told him to contact a Grand Rapids police detective.

When he got in touch with the detective, he complained that his account was locked and assets were seized. And he texted him a photo of a letter that supposedly proved he was supposed to receive the funds. When that didn't work, he later claimed that someone named "Dora" was the mastermind of the whole scheme and that he "just wanted to make a buck."[9] And when that didn't work, he said he needed to hire an attorney.

Besides this scheme, the couple is also suspected of defrauding two other businesses. They deny any wrongdoing, and in the spring of 2023 they had yet to be charged.

Industries: Public agency

Location: U.S.

$2.8 Million

in damages

7 MLive.com. "Beverly Hills Couple 'Spending Spree' Funded with $2.8M Scheme Targeting Grand Rapids Public Schools, Investigator Says." February 2022.
8 Fortune. "Accounts Deceivable: Email Scam Costliest Type of Cybercrime." April 2022

CHILDREN'S HEALTHCARE OF ATLANTA

Taking Off the Kid Gloves

Children's Healthcare of Atlanta works hard to give families and their children happy endings. This just may have earned it some good karma. While the organization lost $3.6 million to BEC scammers in 2018, by 2022 it had beaten the odds and gotten most of it back. For a bonus: the perpetrator had been indicted by a grand jury.

It's likely that Children's became a target of a BEC scammer soon after it kicked off a project to build a new 70-acre campus. The construction firm with the winning bid, J.E. Dunn, made a big announcement that it would be the project's general contractor. A major construction project could mean a large payout. And soon after a scammer kicked off his own project—to divert the firm's payments to his own accounts.

It was a familiar BEC scam. But the attacker didn't stop at spoofing the company's email address by changing .com to .org. He went the extra mile by sending a letter requesting the company send payments to another account by using fraudulent J.E. Dunn letterhead signed by himself—as the company's CFO.

One month after the $3.6 million payment was transferred to the wrong account, Children's discovered the fraud. That's when the FBI was called in to investigate. They tracked the payment to Adeniyi Ajao who was later indicted and pled not guilty.

According to court records, Children's recovered nearly $2.6 million. And in May 2022 it was working to recover $800,000 more in accounts frozen by the FBI.[10]

Industries: Healthcare

Location: U.S.

$3.6 million

in damages

10 KMBC. "Scammer Steals Millions from Atlanta Health Care Provider Posing Employees From KC's JE Dunn." May 2022.

SILVERTERRIER GANG

Invoices, Inboxes and Impersonation

In May 2022, Interpol arrested an unnamed man who is believed to be a group ringleader in SilverTerrier (aka TMT), a BEC gang based in Nigeria. By catching someone at the top levels of the organization, the group's massive attack infrastructure was exposed. And it lost some of its power.

The latest arrest came after a roundup of 11 other suspects connected to the group in December 2021.[11] It's believed that more than 400 people are involved in the gang, which has targeted tens of thousands of companies and individuals worldwide since it launched in 2014.

According to Interpol, this is a breakdown of SilverTerrier's BEC approach:[12]

1. The gang conducts mass phishing campaigns in English, Russian and Spanish using MailChimp, Gammadyne Mailer and Turbo-Mailer.

2. Emails appear to be coming from representatives of legitimate companies. Instead, they distribute malicious code through bogus purchasing orders business, product inquiries and other attachments.

3. Messages spread 26 malware programs, spyware and remote access tools. These include Agent Tesla, Loki, Azorult, Spartan and the nanocore and Remcos Remote Access Trojans.

4. Every opened message is tracked. Once the gang knows it has infiltrated a victim's system, it monitors system activity, tricks the victim with new scams and steals funds.

Multiple cybersecurity companies assisted law enforcement in making these arrests. Here's what cybersecurity researchers say the group does next: After a patient zero is compromised, the gang analyzes that person's email correspondence. Special filters redirect any emails sent to that person—which contain payment information—to fake inboxes controlled by the gang, or those messages are hidden in service directories.[13]

The ringleader likely owned infrastructure that served as the command-and-control (C2) for malware like ISR Stealer, Pony and LokiBot. It also identified more than 240 domains the threat actor registered under various aliases—50 of which were used as C2 infrastructure for the malware.[14]

Industries: Multiple

Location: Global

50,000

companies in 150 countries targeted

11 Info-Security.com. "Eleven Arrested in Bust of Prolific Nigerian BEC Gang." January 2022.
12 Info-Security.com. "Nigerians Arrested Over International BEC Scam." November 2020.
13 Forbes. "800,000 Passwords, 50,000 Targets: A Huge Nigerian Fraud Operation Busted." January 2022.
14 BleepingComputer.com. "Interpol Arrests Alleged Leader of the SilverTerrier BEC Gang." May 2022.

ELKIN VALLEY BAPTIST CHURCH

Nothing Is Sacred

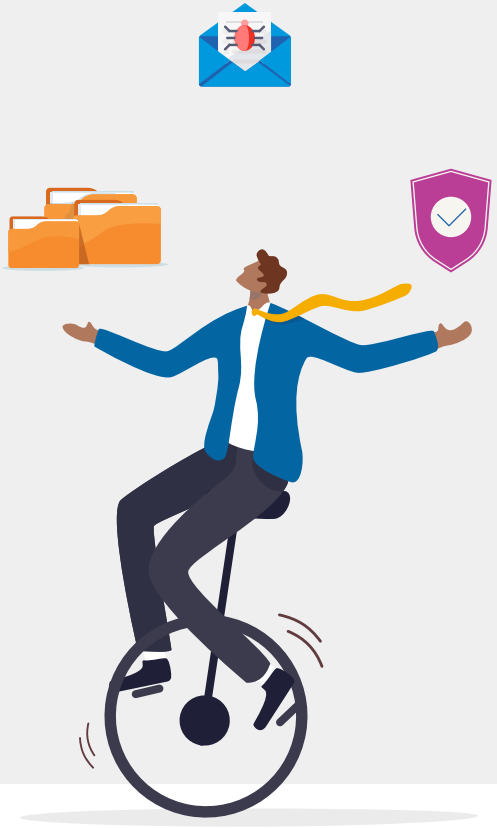
If you run a small church in North Carolina, raising enough money for a construction project can take years. Over the past decade, church members at Elkin Valley Baptist Church scrimped, saved and fundraised enough money build a new worship center. And in September 2022, they finally had what they needed—$1.5 million—to break ground. Unfortunately, that's when BEC scammers swooped in.

The theft took place in November 2022. On a Friday night, after the church's office had closed, two emails were sent to its financial secretary back to back. One of them was sent by the church's builder asking for the first half of its payment, including transfer instructions. The second was from a BEC scammer.

The scammer's message was virtually identical to the real one. Not only did it feature the construction company's real logo, but it included the previous email thread in the body of the message below. The only differences between the two messages were one letter in the email address at the top and, of course, the payment transfer details below.[15]

On Monday, a church representative saw both emails and followed the payment instructions in the second email. Almost a week later, an alarm was raised when the construction company followed up about their missing $793,000 payment. Soon after, the church learned it had been robbed.

The incident was reported to the Elkin Police Department and the FBI. But authorities said it was unlikely that any of the funds would ever be recovered.



Industries: Religious organization

Location: U.S.

$793,000

in damages

15 Elkin Tribune. "$793K Stolen from Elkin Valley Baptist Church." January 2023.

VIRGINIA COMMONWEALTH UNIVERSITY

A Degree in Deception

BEC attacks often come from abroad. Sometimes that means justice never comes. Fortunately, when one string of BEC attacks cost multiple businesses, government agencies and schools millions, the U.S. never gave up trying to extradite the culprits. In September 2022, Virginia Commonwealth University (VCU) was the first to get justice.

In 2019, three Nigerian nationals living in the U.K. were indicted for U.S. cyber fraud crimes that took place between 2017 and 2019. Although they were arrested in 2020, it took a long time for them to come to trial in the U.S. That's because they fought extradition, filing multiple appeals to avoid facing their day in court. Finally, in the fall of 2022, they lost that battle.

The three stood accused of stealing approximately $5 million in a series of BEC fraud scams that had targeted multiple organizations across Texas, North Carolina and Virginia. One of them, Olabanji Egbinola, was accused of stealing $470,000 from VCU.

A fraudster with convictions dating back to 1999, Egbinola knew how to play the long game. Over nearly three months, he worked on building trust with VCU by posing as an employee of Kjellstrom + Lee—a construction company with an ongoing project with VCU—called "Rachel Moore."[16] Eventually VCU trusted Rachel, and she submitted new banking details.

Soon after the first payment, VCU was informed that the wire transfer was fraudulent and that Rachel was not a real person.

Egbinola pled guilty and cooperated. While he'd spent 85 days in a London jail and two years on supervised release, during his sentencing the judge held his extradition fight against him.[17] Only 85 days were deducted from his 48-month sentence. And with none of the funds ever recovered, Egbinola was also on the hook to repay them in full.

Industries: Higher education

Location: U.S.

$470,000

in damages

16 Department of Justice. "Extradited UK Citizen Pleads Guilty to Defrauding VCI in Business Email Compromise Scheme." September 2022.
17 Richmond Times-Dispatch. "U.K. Citizen Sentenced to 4 Years for Swindling VCU out of $470F." February 2023.

CITY OF COTTAGE GROVE, MINNESOTA

Impersonating the Company President

More often than not, recovering funds stolen in a BEC scam is impossible. Unfortunately, the City of Cottage Grove learned this lesson when fraudsters stole more than $1.2 million and the city had a tough time clawing it back—even with the help of the U.S. Attorney's Office.

In August 2022, five federal seizure warrants detailed the scheme.[18] In mid-2021, Cottage Grove hired Genslinger & Sons for a sewer project. A few months later, the city's accounting specialist emailed the company's office manager at an email address that ended "genslingerandsons.com." Five days later, someone pretending to be the company's president, Jeff Genslinger, emailed the accounting specialist from "genslingerandsonsinc.com" to update the payment information.

The city subsequently sent two payments of $813,250 and $462,810 to that new account. Two months later, when the office manager at Genslinger & Sons reached about its missing payments, the city replied that its accounting specialist had been emailing Jeff—only to learn that Jeff had been on vacation for weeks.

When the bank was asked to freeze the fraudulent account, only $538 remained. The scammer had quickly dispersed the money to multiple accounts belonging to other people.

U.S. Magistrate Judge John Docherty approved the warrants in August 2022. Their goal was to seize up to $852,337 linked to the fraud."[19] The funds were allegedly in six bank accounts held by the fraudster's relatives, a co-conspirator and a lawyer who claimed the money was for "legitimate business purposes."[20] It's not clear whether any funds were ever recovered.

Industries: Public agency

Location: U.S.

$1.2 Million

in damages

18 Star Tribune. "Feds Investigating $1.2 Million E-Mail Fraud Scheme That Targeted City of Cottage Grove." August 2022.
19 Pioneer Press. "Federal Investigation Underway into Sham Emails That Led to City of Cottage Grove Losing $1.2M." August 2022.
20 Star Tribune. "Feds Investigating $1.2 Million E-Mail Fraud Scheme That Targeted City of Cottage Grove." August 2022.

MEDICARE AND MEDICAID SCAMS

Hijacking Hospital Payments

Officially, the annual fraud for Medicare and Medicaid programs tops $100 million.[21] But many investigators believe it's likely much higher. While there are multiple ways to steal millions from these programs, BEC scams are increasingly popular.

21 CNBC. "Inside the Mind of Criminals: How to Brazenly Steal $100 Billion from Medicare and Medicaid." March 2023.

In 2022, the U.S. Department of Justice November (DOJ) brought an end to a few of these scams. That's when it charged 10 BEC fraudsters for a series of schemes that resulted in more than $11.1 million in losses.[22] Five state Medicaid programs, two Medicare contractors and two private health insurers were duped into wiring payments to the defendants and their co-conspirators.

In most of the schemes, the defendants created email accounts that looked almost identical to legitimate businesses and hospitals. The unwitting victims were tricked into updating bank account details for reimbursement payments. Many of these bank accounts were fraudulent. To hide their ill-gotten gains, seven defendants used stolen identities to open them in the name of shell companies.

In June 2022, one defendant pled guilty and was sentenced to four years in prison. At the end of 2022, the remaining nine were awaiting trial and faced a maximum sentence of 20 to 30 years in prison.

Industries: Healthcare

Location: U.S.

$11.1 Million

in damages

22 Department of Justice. "10 Charged in Business Email Compromise and Money Laundering Schemes Targeting Medicare, Medicaid, and Other Victims." November 2022.

CONCLUSION

Lessons Learned

BEC attacks prey on human nature. They exploit people's trust. Defending against them requires a multi-layered, fully integrated, people-centric approach that includes:

1. Detecting and blocking BEC threats before they enter
2. Preventing your brand from being spoofed in BEC attacks
3. Getting visibility into BEC threats—and how vulnerable your users are to them
4. Identifying suppliers that pose a risk to your organization
5. Making your users more resilient
6. Automating incident response and remediation

Learn about Proofpoint solutions for protecting your organization from BEC attacks at proofpoint.com/us/solutions/bec-and-eac-protection.

LEARN MORE

For more information, visit **proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media and the web. More information is available at **www.proofpoint.com**.

proofpoint.

0503-003-01-04 06/23