Bottomline

Uncovering the 3 Biggest Hidden Liabilities of Business Email Compromise in Banking

Defending with Data

In a high-rise building an ocean away, an entire workforce is hard at work. Their sole KPI? To facilitate financial attacks on American companies, using sophisticated social engineering techniques to exploit the weakest link: human nature. And with the pandemic moving more transactions online, these scammers are busier than ever: BEC attacks jumped a startling 65% from July 2019 to December 2021[1].

Business Email Compromise (BEC) is defined by the FBI's IC3 as "a sophisticated scam targeting businesses that perform electronic payments such as wire or ACH transfers[2]."

In addition to diverting funds, BEC perpetrators may also target Personally Identifiable Information (PII) or W-2s, which can either be further exploited, resold, or both. This type of fraud can range from quick, one-time hits to sophisticated infiltration schemes that unfold over months or even years. And as the numbers below reveal, it is an extremely lucrative criminal pursuit.

Losses from Business Email Compromise schemes have grown every year since the FBI began tracking them in 2013[3]. **The FBI have calculated that over $43 billion in domestic and international losses were stolen from corporate victims from June 2016 - December 2021[4].**

In 2021, almost $2.4M was lost to BEC and email account compromise (EAC), with the average email fraud loss increasing by 25% from $96,373 to $120,074.[5]

The FBI has outlined five scenarios that are typically used to execute BEC scams[6].

1. PAYMENT CHANGE REQUEST:
"Bogus Invoice" or "Supplier Swindle

2. EXECUTIVE WIRE TRANSFERS:
"CEO Fraud" or "Masquerading"

3. CONTACT COMPROMISE:
to spoof a legitimate communication from existing supplier

4. EXECUTIVE OR ATTORNEY IMPERSONATION:
to provide false urgency to a fraudulent transaction

5. DATA THEFT:
request W-2s or PII data via compromised email from employee

The Hidden Liability of BEC

When it comes to fighting fraud, many FIs have prioritized their resources on preventing and detecting consumer fraud over Business Email Compromise. There are several reasons for this.

1. Phishing scams targeting consumers are more widespread and easier to execute, so they occur more frequently.

2. Consumer protection regulations typically require banks to reimburse consumer losses beyond a small limit, as long as those customers report the fraud promptly. Under the Uniform Commercial Code (UCC), business account holders have much shorter timelines to report fraud, less protections, and greater fraud liability than consumer banking customers.

3. Money moved through BEC is considered "authorized" corporate fraud, because the financial transfers—while based on false pretenses—are legitimately initiated and/or approved by the company who was targeted. This means that the bank is not responsible for covering the loss.

Bad Experiences Are Bad for Business

If FIs have maintained compliance in all areas, they are not financially responsible for reimbursing the vast majority of BEC losses. However, **allocating fraud prevention resources based strictly upon number of incidents or immediate dollars lost can be a shortsighted approach.** Consider these points:

- Commercial clients who are victims of BEC not only lose money, but—justified or not—they also lose confidence in their financial institution.

- Digital transformation has made many things easier in banking, including a customer's ability to change banks. Since commercial accounts bring in significant revenue to banks from processing fees, large lending deals and other high-ticket services, the loss of even one unhappy account can cause substantial financial impact.

- Loss of reputation is another negative consequence that unhappy customers or high-profile losses can inflict on banks.

The Takeaway?

If FIs were to shift their focus from the volume of consumer losses to the value of lost commercial customers, then BEC fraud may actually be the costlier crime. And that's without including the expenses incurred by participating in protracted litigation and working with parties impacted by BEC scams. By those calculations, BEC fraud is unquestioningly deserving of equal detection and defense.

Uncovering Vulnerabilities

Financial institutions face several challenges in taking steps to help protect their corporate customers, ranging from evolving expectations to the type of technology used.

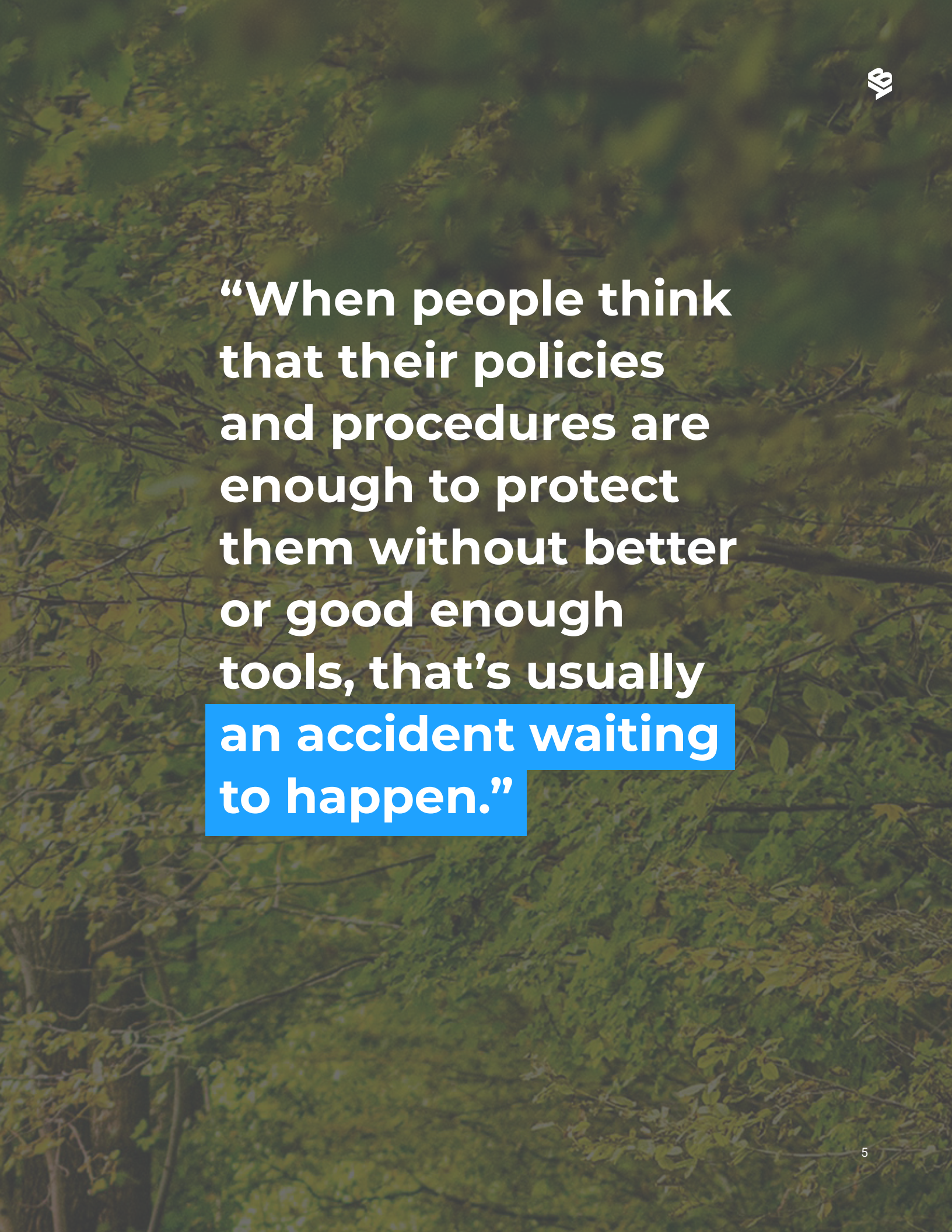
Challenge One: Payment Acceleration. Right now, the entire industry is undergoing a shift to real-time digital payments around the world. Origination and settlement used to take 48-72 hours, which provided a much larger window of time to confirm the legitimacy of a transfer request and stop a fraudulent payment. But the market now demands fast, frictionless transactions—and BEC scammers take full advantage of this atmosphere to push fraud through without question.

Challenge Two: Changes in Fraud Tactics. Initially, criminal enterprises focused on headline-grabbing thefts worth millions of dollars, but are now shifting to smaller but longer term fund diversion schemes. While there are still large-scale BEC thefts such as the $29M transferred at the request of a Nikkei U.S. parent company "executive" in November of 2019[7], often the fraud is much subtler. By starting very small, fraudsters actually "train" a corporate customer's system to accept and trust them. Over time, they start raising the amount requested but no red flags are raised—making this ongoing fraud equally costly to a single big scam if not detected.

"Trying to use a retail tool for commercial fraud prevention is a big pitfall."

Challenge Three: Consumer-Oriented Technology. Further complicating the effort for banks to protect their business customers is that most current systems are geared towards dealing with consumer fraud, not the specificity of commercial targets. These consumer-focused tools are often not as robust, rendering them unable to properly secure business banking's multiple channels and attack vectors, or understand processes that are specific to the commercial segment. Tolerances for consumer losses are also higher due to the lower cost-per-incident.

Challenge Four: An Unconnected View. Another vulnerability in defending against commercial BEC is that due to their consumer-fraud orientation, banks are often good at responding at the single-incident level—but not at the corporate level. Failure to be able to view and analyze all incidents as a whole means missing significant links or trends that could help identify a specific corporation being targeted and zero in on the root cause, such as old technology, failure to follow policy, or even employee criminal conduct.


“When people think that their policies and procedures are enough to protect them without better or good enough tools, that’s usually an accident waiting to happen.”

So how does a bank improve its BEC detection and prevention practices?

3 Steps to Safeguarding Your Institution

When it comes to BEC best practices, banks should focus on three key areas: **Recognize, Reveal and Repel.**

RECOGNIZE the risk factors and potential gaps. Humans are the weakest link in the payment chain. Social engineering has made it easier than ever to get credible details for nearly flawless impersonation. The drive to provide seamless, superior customer service can also be leveraged by fraudsters, who often create a compelling sense of urgency for transactions to be completed. **It's important to note that this is a vulnerability of not only the employees of a bank's clients, but the bank's own staff as well.** Policies and training are important tools—but the truth is that they don't always align with actual practices. Even when employees know that requesting payments or changes on an ad hoc basis such as via email is a breach of protocol, it is temptingly convenient, especially when there are time pressures or remote workforce complications. Banks must help their commercial clients help themselves by backstopping both their clients' policies and procedures—and their own—with commercial-grade payment security technology. Not only will this level of technology cover points of compromise unique to business banking, but this type of system should be able to understand commercial segment-specific qualities such as multiple approvers, template deviation and batch level analytics. **For the strongest level of payment protection and control, this defense system should natively connect the banking portal with the fraud engine.**

REVEAL suspicious activity. Data may get criminals into the system, but data can also keep them from being successful in executing their intended fraud. **Technology that uses Artificial Intelligence (AI) and Machine Learning (ML)—especially when deployed with an eye on a wider view than just serving as a payment rail**—can spot anomalous payments such as a change in where funds are typically being sent or an unusual payment amount. These technologies can also reveal suspicious patterns, which can be key to catching bad actors within a bank's own system. Human intelligence also has a role here: a bank's fraud team must be able to see the entire picture and have the ability to play things back. That way, if fraud does occur, it's possible to determine what happened and the steps taken throughout the incident, then use that information to develop stronger fraud-prevention strategies.

REPEL fraudsters. Financial institutions are the last line of defense in BEC because their corporate customer has already fallen victim to a scam. Simply employing "last mile-protection" that watches for changes between the channel and settlement can stop criminals in their tracks. In fact, this type of defense mechanism could have prevented attacks like the infamous Bangladesh heist on SWIFT and the others that followed. **Even more exciting is a new tool: payee verification that mines 3rd-party sources to collect additional intelligence on potential payees.** By analyzing this data, banks can quickly confirm (or reject) legitimacy before payment is released.

No matter what tools banks choose to use in these three areas, however, their methods must be quick—with high confidence and minimal false alerts to avoid transactional (and therefore customer) friction.

Stepping Up

There has never been a more necessary time for FIs to step up their fight against BEC. Due to the current global pandemic, more financial transactions than ever are being conducted online— and with that rise has come the startling increase in fraud mentioned earlier. Yet commercial customers, strained by the virus's economic impact, are in no position to absorb more losses. Whether or not their bank is technically liable, the strain that a BEC fraud incident can put on the bank-customer relationship makes addressing commercial fraud prevention more urgent than ever.

Even if a financial institution has fraud detection and prevention technology, it is not necessarily safe. First, the organized crime rings that perpetrate these scams are always adapting—both in terms of context (such as the recent PPE supply scams) and technology (new forms of malware). In addition, banks must add new features on a regular basis to maintain their competitive positioning—and new offerings mean new vulnerabilities. Every time there is a change, protection must evolve as well. When your fraud defense begins inside the commercial payments portal, fraud prevention experts have the knowledge and agility to respond quickly as new threats appear or new features roll out.

The more familiar a fraud prevention technology provider is with the "big picture" of commercial payment portals and activities, the more accurately their tools can be connected and calibrated for success. Bottomline Technologies has been at the forefront of making complex business payments simple, smart and secure since 1989. With Cyber Fraud and Risk Management (CFRM) implementations in tier 1 to tier 4 banks, our best-in-class fraud prevention tools and expertise are available worldwide. Any bank that is seeking a flexible, agile fraud management system with unique capabilities to fight BEC should consult with Bottomline.

New European regulations that require FIs to perform payee verification before a payment goes out have led to the deployment of new features for Bottomline Technologies' customers in the region. By leveraging rapid but sophisticated 3rd party data mining, banks can spot a fraudulent payee by checking for details such as a valid tax id. While there is no equivalent in the United States yet, this technology represents an exciting advance in secure payments that has the potential to deliver value to US banks and their customers.

Learn how Bottomline's Fraud and Financial Crime solutions can help you spot the threat from business email compromise and provide you with unparalleled protection, while helping you secure your digital channel and comply with regulations.

CONTACT US

1. https://www.ic3.gov/Media/Y2022/PSA220504

2,3. https://www.ic3.gov/media/2020/200406.aspx

4. https://www.tripwire.com/state-of-security/security-data-protection/43-billion-stolen-through-business-email-compromise-since-2016-reports-fbi

5. https://www.proofpoint.com/uk/blog/email-and-cloud-threats/fbis-ic3-report-financial-losses-due-email-fraud-hit-record-high-2021

6.https://www.ic3.gov/Media/Y2016/PSA160614

7. https://www.infosecurity-magazine.com/news/nikkei-hit-in-29-million-bec-scam/

Bottomline

Connect with us

About Bottomline

Bottomline (NASDAQ: EPAY) makes complex business payments simple, smart and secure. Corporations and banks rely on Bottomline for domestic and international payments, efficient cash management, automated workflows for payment processing and bill review, and state of the art fraud detection, behavioral analytics and regulatory compliance solutions. Thousands of corporations around the world benefit from Bottomline solutions. Headquartered in Portsmouth, NH, Bottomline delights customers through offices across the U.S., Europe, and Asia-Pacific.

For more information, visit **www.bottomline.com**

Corporate Headquarters
325 Corporate Drive
Portsmouth, NH 03801
United States of America

Phone: +1-603-436-0700
Toll-free: +1-800-243-2528
Fax: +1-603-436-0300
info@bottomline.com

Europe, Middle East, Africa Headquarters
1600 Arlington Business Park
Theale, Reading, Berkshire RG7 4SA
United Kingdom

Tel (Local): 0870-081-8250
Tel (Int): +44-118-925-8250
Fax: +44-118-982-2253
emea-info@bottomline.com

Asia Pacific Headquarters
Level 3, 69-71 Edward Street
Pyrmont, Sydney NSW 2009
Australia

Tel: +61-2-8047-3700
Fax: +61-3-9824-6866
ap_info@bottomline.com